IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

Artificial Intelligence and the Erosion of Women's Digital Security

Syeda Asna Fatima Nahri
BA LLB (Hons), 5th year
Hindustan Institute of Technology and Science, School of Law, Chennai

Abstract: *Artificial Intelligence (AI) is fundamentally altering the nature of digital identity, privacy, and personal autonomy, while simultaneously enabling sophisticated forms of technology-facilitated violence against women. AI-generated deepfakes, identity cloning, impersonation, and non-consensual synthetic intimate content permit the unauthorised appropriation and manipulation of a woman's face, voice, body, and personal identity at unprecedented scale. Such practices constitute more than conventional forms of online abuse; they raise fundamental questions concerning dignity, bodily autonomy, equality, reputation, privacy, and the security of individual identity within digital environments. This paper critically examines the adequacy of existing legal frameworks in addressing AI-enabled violations of women's digital security, with particular attention to the challenges of consent, attribution, evidentiary authentication, intermediary responsibility, jurisdiction, and effective access to remedies. Adopting a rights-based and comparative legal methodology, the study analyses the intersection of criminal law, constitutional protections, privacy and data protection regimes, intermediary liability, platform governance, and emerging AI regulation. It assesses whether legal doctrines developed around conventional forms of publication, impersonation, privacy infringement, and reputational injury can effectively respond to synthetic forms of identity-based harm that are instantaneous, scalable, persistent, and capable of transnational dissemination. The paper argues for recognition of digital identity as an integral dimension of human dignity and autonomy, requiring gender-responsive legal protection. It proposes an integrated regulatory framework incorporating meaningful consent standards, clear civil and criminal liability, strengthened intermediary due diligence, expedited removal and redress mechanisms, digital evidence preservation, victim-centred remedies, transparency obligations, and cross-border regulatory cooperation. The study ultimately positions women's digital security as a critical legal imperative for preserving autonomy, equality, and dignity within an increasingly AI-mediated society.*

Keywords: Artificial Intelligence; Deepfakes; Women's digital security; Synthetic identity; Consent; Intimate-image abuse; Platform liability; Privacy; Digital evidence

I. INTRODUCTION

The rapid expansion of the digital sphere has transformed the way individuals construct, communicate and experience their identities, but it has also created new forms of vulnerability, particularly for women. Artificial Intelligence (AI) has intensified this vulnerability by making it possible to reproduce and manipulate a person's face, voice, body and mannerisms with remarkable accuracy, often without the person's knowledge or consent. Generative AI, deepfake technology, voice cloning and other synthetic-media tools can create representations that appear authentic while depicting an individual in situations, conversations or contexts that never existed. The resulting harm is not confined to the circulation of false information; it concerns the erosion of an individual's control over her own digital identity. In this environment, a woman may retain control over her devices, accounts and personal information and yet lose meaningful control over how her likeness, voice or identity is represented and used online. This development marks an important shift in the understanding of digital security. Protection can no longer be limited to confidentiality,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

cybersecurity or prevention of unauthorised access. It must also address the integrity of digital identity and the ability of individuals to determine the contexts in which their identity-bearing representations are created, altered and disseminated. The gendered character of this problem is particularly significant as women are disproportionately exposed to AI-enabled sexual harassment, non-consensual synthetic intimate imagery, impersonation, fabricated endorsements, online stalking, blackmail and reputational attacks. The capacity of AI tools to generate realistic material at low cost and distribute it instantaneously enables such abuse to be produced, replicated and circulated on a scale that conventional forms of manipulation could not achieve. What was previously dependent upon specialised technical skills can increasingly be accomplished through widely accessible technologies, thereby lowering the barriers to identity-based abuse. The consequences may extend beyond the digital environment, affecting dignity, privacy, bodily and sexual autonomy, employment, social relationships, psychological well-being and physical safety. The distinctive legal problem lies in the fact that AI-enabled identity abuse does not necessarily depend upon the unlawful acquisition of the original material. A photograph or video may have been voluntarily and lawfully shared online, yet that does not imply consent to its transformation into sexualised, defamatory, deceptive or otherwise harmful synthetic content. The availability of information in one context cannot therefore be treated as unrestricted permission for its subsequent manipulation or dissemination. This raises the broader question of contextual integrity: whether the use of identity-bearing material remains legitimate when its purpose, context, audience or meaning has been fundamentally altered. Existing legal frameworks are not fully equipped to answer this question. Privacy and data-protection law, criminal law, defamation, copyright, personality rights and intermediary regulation each address particular dimensions of digital harm, but synthetic identity abuse frequently operates across these legal categories without fitting neatly within any single one. The inadequacy becomes especially apparent where the representation is demonstrably false but nevertheless produces genuine and substantial harm. Traditional legal concepts centred on unauthorised access, ownership, publication or falsity may therefore fail to capture the central injury the unauthorised creation or manipulation of a person's identity and its deployment in a harmful context. A more effective legal approach must consequently examine the relationship between the individual, the representation, the purpose for which it is used, the absence or presence of consent and the foreseeable consequences of its dissemination. At the same time, protection of women from AI-enabled abuse must be reconciled with constitutionally protected freedom of expression. Not every manipulated or synthetic representation should attract legal prohibition, particularly where it constitutes legitimate journalism, criticism, satire, political commentary or artistic expression. The challenge is to establish clear thresholds that distinguish protected expression from conduct that unjustifiably infringes privacy, dignity, autonomy or security. Interim protection may therefore be justified where an identifiable woman has been represented without meaningful consent and the dissemination presents a serious and immediate risk of harm, while final civil or criminal liability should remain subject to appropriate standards of proof concerning attribution, fault and causation. In India, the constitutional foundation for protecting these interests is strengthened by *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which recognised privacy as a fundamental right closely connected with dignity, autonomy and personal choice. *Shreya Singhal v. Union of India* (2015), meanwhile, provides an important constitutional framework for assessing restrictions on online expression. The Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and intermediary-related regulations provide additional mechanisms for addressing aspects of digital abuse, but they do not yet constitute a comprehensive framework specifically designed to address AI-generated identity manipulation. The emerging challenge is not whether AI should be permitted to develop, but how its transformative capacity can be reconciled with the rights and security of individuals whose identities can be reproduced without their participation. A meaningful framework for women's digital security must move beyond the narrow protection of data and accounts and recognise digital identity itself as an important site of privacy, dignity, autonomy and personal security. Such a framework should establish clear standards for non-consensual synthetic representations, impose proportionate responsibility on perpetrators and relevant intermediaries, facilitate rapid intervention where serious harm is threatened, preserve digital evidence for subsequent proceedings and provide effective civil, criminal and regulatory remedies. The erosion of women's digital security through AI thus represents not simply a technological

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

problem, but a contemporary legal and rights-based challenge in which the capacity to reproduce identity is advancing faster than the mechanisms available to protect individuals from its misuse.

Conceptual and Technological Dimensions of AI-Enabled Digital Identity Abuse

Artificial intelligence, deepfakes, digital identity, and non-consensual synthetic content must be understood through a common legal framework that focuses not merely on technological novelty but on the effects of transforming identity-bearing material. For this inquiry, artificial intelligence is understood functionally as a computational system capable of generating or materially transforming outputs that viewers associate with an identifiable person. The legal inquiry therefore remains technology-neutral and does not depend upon whether the underlying architecture is a generative adversarial network, diffusion model, or subsequent technique. This approach is significant because conventional legal protection has historically been structured around access, ownership, publication, or falsity, while synthetic identity abuse may arise even where the underlying source material was lawfully accessible. Contextual integrity accordingly provides a more appropriate organising principle: material associated with an individual may be available for one purpose without becoming available for every transformation, audience, or commercial use. A rights-based assessment must consequently consider the relationship between the person, the representation, the purpose of processing, and the foreseeable consequences of dissemination. Within this framework, technology-neutral drafting should be accompanied by capability-based regulation that avoids both technological obsolescence and unrestricted suppression of contested expression. Such regulation must be translated into defined elements, evidentiary thresholds, and proportionate remedies. Interim restrictions may appropriately rest upon a prima facie showing of identifiability, absence of consent, and serious risk, whereas final civil liability, damages, or criminal conviction should require fuller proof of fault, causation, and attribution. This distinction permits timely protection while preserving procedural fairness and due process. Institutional fit is equally important. Courts are positioned to grant injunctions and determine contested rights; police authorities may investigate serious offences; data-protection authorities may examine unlawful processing; and digital platforms may respond rapidly to hosted or indexed material. These functions should operate complementarily rather than as substitutes. A coherent framework should allocate responsibilities, establish referral mechanisms, and prevent complainants from repeatedly presenting the same factual account before institutions. Evidence preservation must operate alongside restriction or removal so that urgent intervention does not destroy material necessary for later judicial adjudication. The relevant legal foundation includes the TAKE IT DOWN Act definition of digital forgery as these sources should be applied narrowly and accurately: constitutional decisions establish governing principles, statutes confer defined powers and offences, and institutional reports document patterns or recommend reforms. They should not be treated as automatically creating a freestanding remedy for every injury caused by synthetic media. Nevertheless, openly stated analogical reasoning remains legitimate. Privacy doctrine may illuminate control over identity; personality-rights jurisprudence may inform questions of appropriation; and electronic-evidence principles may assist in determining authenticity. Where recurring deficiencies cannot be resolved consistently through case-specific orders, however, legislative intervention remains necessary. Deepfakes constitute a subset of synthetic media because they create the appearance that a real person said, did, or participated in something that did not occur. Their legal significance lies principally in identifiability, materiality, attribution, and consent rather than technical novelty. Harmful appropriation and contextual falsity therefore require carefully bounded expression safeguards, ensuring that protective measures do not become an unlimited mechanism for suppressing legitimate commentary, criticism, or contested material. The same evidentiary distinctions between interim protection and final liability remain relevant, as do questions of institutional coordination and preservation of evidence. United Kingdom wording concerning images that show or appear to show a person provides a further comparative legal foundation, but must similarly be interpreted according to its statutory scope. Digital identity extends beyond a single photograph and may encompass a person's face, voice, name, signature, biometric characteristics, gestures, professional role, and combinations of attributes through which recognition occurs. Misuse arises where such attributes are appropriated to attribute speech, conduct, endorsement, presence, or participation without authority. This conception supports an understanding of identity

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

integrity that protects ordinary persons as well as public figures. In the Indian context, the Information Technology Act, 2000, including sections 66C and 66D, and Delhi High Court personality-rights decisions provide relevant references, subject to their statutory and doctrinal limits. Finally, non-consensual synthetic content requires a rigorous conception of consent. Consent should be free, specific, informed, unambiguous, and limited to the purpose for which it was given. Permission to be photographed, to publish an image, or to license a particular use does not, without more, authorise model training, replica generation, or deployment in a different context. The legal inquiry must therefore distinguish the lifecycle stages of creation, solicitation, threats, and distribution, because harm and responsibility may arise differently at each stage. The TAKE IT DOWN Act's consent language and United Kingdom reforms concerning intimate images offer comparative foundations for this analysis. Across these categories, the central principle remains that lawful access to identity-bearing material does not constitute unrestricted authority to transform, attribute, or disseminate it. A publishable framework must consequently reconcile identity integrity, privacy, expression, consent, evidentiary reliability, institutional competence, and effective remedies while maintaining proportionality and due process. Such an approach preserves the core objective of addressing AI-enabled identity abuse without treating technological capability itself as the legal wrong, thereby providing a principled basis for both immediate protection and sustainable and effective legislative development.

AI-Enabled Threats to Women's Digital Security.

Artificial Intelligence (AI) enabled identity abuse operates within existing inequalities and can produce particularly severe consequences for women, including fabricated intimate media, impersonation, reputational attacks, harassment and other forms of identity-based abuse. Such harms can exploit gendered stigma and impose disproportionate costs on women who participate in professional, political, journalistic or civic life. Synthetic identity abuse can therefore generate dignitary, reputational, economic, relational, safety and civic harms simultaneously, while traditional legal categories often separate these consequences and leave victims to pursue several proceedings for one course of conduct. This shift matters because legal protection has historically been organised around access, ownership, publication or falsity, whereas synthetic identity abuse can occur even when source material was lawfully visible. The better organising concept is contextual integrity: identity-bearing material may be available for one purpose without becoming available for every transformation, audience or commercial use. A rights-based analysis must therefore examine the relationship between the subject, the representation, the purpose of processing and the foreseeable consequences of dissemination. The first normative consideration is substantive equality, intersectionality and accessible remedies, alongside harm-flexible civil relief and offence-specific criminal responsibility. These considerations should not operate as slogans or as an unlimited power to suppress contested material. They must instead be translated into defined elements, evidence thresholds and remedies proportionate to the stage of harm. Interim restriction may properly depend on a prima facie showing of identifiability, lack of consent and serious risk, while final damages or criminal conviction require fuller proof of fault, causation and attribution. This separation enables fast protection without diluting due process. The gendered nature of AI abuse also requires recognition that the impact of synthetic media may extend beyond the immediate publication of false or manipulated material. Women may face reputational damage, professional exclusion, social stigma, relational consequences, threats to physical safety and reduced participation in public or civic life. A framework based on substantive equality must therefore account for the unequal social consequences of technologically facilitated abuse and ensure that remedies remain accessible to persons who may lack financial, technological or institutional resources. At the same time, the legal framework must distinguish between legitimate expression and harmful appropriation, contextual falsity and non-consensual synthetic representation, thereby preserving carefully bounded expression safeguards. Digital distribution further changes the scale and duration of injury because synthetic material can be copied, indexed, edited, translated and re-uploaded before ordinary legal proceedings begin. Removal from an originating account does not necessarily eliminate mirrors, caches or materially equivalent variants, making virality and permanence central considerations in assessing harm. The appropriate normative response is therefore rapid containment combined with preservation, review and appeal. Urgent

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

restriction may be justified where identifiability, lack of consent and serious risk are established on a prima facie basis, but such measures should remain subject to defined standards, procedural safeguards and opportunities for review. Evidence preservation must operate alongside restriction so that urgent removal does not destroy material required for subsequent adjudication. The problem of attribution is equally significant because false accounts, overseas services, privacy tools, stripped metadata and open models can make it difficult to identify the creator or distributor of synthetic content. Detection technologies can support triage and establish whether material is likely to be synthetic, but a probability that media is artificial does not, by itself, prove who created, altered or distributed it. The legal framework must therefore separate interim protection from final criminal proof. This distinction is particularly important where rapid action is necessary to prevent continuing dissemination, but criminal liability requires fuller proof of fault, causation and attribution. Courts, police, data-protection authorities and platforms consequently have complementary institutional roles. Courts can issue injunctions and determine contested rights; police can investigate serious offences; data-protection authorities can examine unlawful processing; and platforms can act rapidly on hosted or indexed material. None of these institutions should be treated as a complete substitute for the others. A coherent framework should allocate functions, establish referral channels and prevent a complainant from repeatedly presenting the same factual account before every institution. Institutional coordination is especially important in cases involving cross-platform dissemination, where the speed of technological replication may exceed the speed of conventional legal processes. The relevant legal foundation includes OHCHR and UNESCO institutional materials concerning the gendered and human-rights dimensions of technology, United States notice-and-removal models, United Kingdom online-safety models, and constitutional privacy principles and general remedial doctrine. These sources should be read narrowly and accurately: constitutional cases supply principles, statutes provide defined powers and offences, and institutional reports document patterns or propose reform. They do not automatically create a freestanding remedy for every synthetic-media injury. Analogical reasoning is nevertheless legitimate where the analogy is stated openly. Privacy doctrine can illuminate control over identity, personality-rights cases can illuminate appropriation, and electronic-evidence cases can illuminate authenticity, yet legislation remains necessary where recurring gaps cannot be resolved consistently through case-specific orders. In relation to evidentiary questions, Anvar P.V. and Arjun Panditrao, together with the Bharatiya Sakshya Adhiniyam 2023, provide relevant foundations for understanding the treatment and authentication of electronic evidence. Their significance in the context of synthetic identity abuse lies not in automatically resolving questions of responsibility, but in establishing a framework through which digital material can be presented, authenticated and assessed in legal proceedings. Accordingly, evidence relating to the creation, alteration, transmission, metadata, account activity and dissemination of synthetic content should be preserved carefully, while technological detection should be treated as an evidentiary aid rather than an infallible substitute for proof. Ultimately, AI-enabled threats to women's digital security require a framework that recognises the gendered nature of harm while remaining technology-neutral, evidence-based and proportionate. Substantive equality, contextual integrity, meaningful consent, rapid containment, evidence preservation, attribution standards and institutional coordination must operate together rather than as isolated legal responses. The objective should not be an unlimited power to suppress synthetic or controversial expression, but a carefully structured system capable of responding effectively where artificial intelligence is used to appropriate identity, fabricate conduct, intensify gendered abuse or produce foreseeable and serious harm to women's dignity, privacy, reputation, security and participation in digital and public life.

Constitutional and Statutory Framework for Women's Digital Protection.

India's legal framework addressing AI-enabled synthetic identity abuse remains dispersed across constitutional principles, information technology law, data-protection regulation, criminal law, intellectual property and personality-rights jurisprudence. This fragmentation is particularly significant for women because AI-generated or manipulated images, videos and voices can facilitate impersonation, sexualised representation, harassment, reputational injury and extortion. The constitutional framework therefore provides the normative foundation for protecting women's digital identity, while statutory and judicial mechanisms address specific forms of misuse. At the constitutional level, Articles

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

14, 19 and 21 provide the principal architecture for addressing synthetic identity abuse. Article 14 guarantees equality and protection against arbitrary State action, Article 19 protects freedom of expression subject to constitutionally permissible restrictions, and Article 21 encompasses privacy, dignity, autonomy and personal liberty. Conventional legal protection has historically been organised around access, ownership, publication or falsity, whereas synthetic identity abuse may occur even where identity-bearing material was lawfully available. Lawful availability for one purpose should not authorise its transformation, redistribution, commercial exploitation or deployment in another context. The constitutional principles of privacy, dignity and autonomy were significantly strengthened by *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, while *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, provides important principles concerning freedom of expression and permissible restrictions in the digital environment. These authorities should not be construed as creating a freestanding remedy for every form of synthetic-media injury. Regulation must remain rights-protective without becoming vague. Restrictions should therefore be based on defined legal elements, appropriate evidentiary thresholds and proportionate remedies. Interim restrictions may depend upon a prima facie showing of identifiability, absence of consent and serious or continuing risk, whereas final damages or criminal conviction should require fuller proof of fault, causation and attribution. The Information Technology Act, 2000 provides another important layer through provisions concerning offences, blocking powers and conditional intermediary protection. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, together with subsequent governmental measures, further address grievance handling, due diligence, impersonation and synthetic or misleading information. These mechanisms can facilitate removal and regulatory intervention but do not independently create a comprehensive private remedy for synthetic identity abuse. Platform obligations should therefore operate alongside lawful orders, evidence preservation and transparent review. Platforms should respond promptly to harmful hosted or indexed material within clearly defined legal standards. Courts, police authorities, data-protection institutions and platforms perform distinct functions: courts determine contested rights and issue injunctions; police investigate criminal conduct; data-protection authorities examine unlawful processing; and platforms facilitate rapid restriction of harmful material. A coherent system should establish referral channels and standardised complaint procedures. Evidence preservation should accompany restriction so that removal does not destroy material necessary for investigation or adjudication. The Digital Personal Data Protection Act, 2023 is relevant where facial images, voice recordings or other identity-bearing information constitute digital personal data linked to an identifiable individual. Its principles concerning processing and governance can contribute to regulating collection, reuse and continued processing. Synthetic identity abuse extends beyond conventional data governance because manipulated material can be rapidly copied, transformed and redistributed. Data-protection principles should therefore complement mechanisms for rapid restriction, investigation and redress. The Act and its official rules provide a defined data-governance framework but do not automatically establish a comprehensive remedy for every synthetic identity injury. The Bharatiya Nyaya Sanhita, 2023 provides criminal provisions capable of addressing conduct involving personation, cheating, stalking, intimidation, extortion, voyeuristic conduct, forgery-related behaviour and defamation. These provisions can address particular consequences of AI-enabled identity abuse where statutory elements are established. The BNS does not create a unified offence of synthetic identity abuse. Criminalisation should therefore remain narrow and fault-based, while aggravated forms of serious abuse may warrant stronger consequences. The principles developed in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, together with the Bharatiya Sakshya Adhiniyam, 2023, provide an important foundation for establishing the authenticity and admissibility of electronic material. Proving that content is AI-generated does not establish who created, commissioned, uploaded or disseminated it. Detection establishes the synthetic character of material, whereas attribution requires additional evidence connecting it to a particular actor. Intellectual property and personality-rights doctrines provide another significant but incomplete layer of protection. Copyright primarily protects authorship rather than the identity of the person depicted, while trademark and passing-off principles generally address commercial misrepresentation. Personality-rights jurisprudence has increasingly recognised interests in identifiable aspects of an individual's persona. Recent decisions involving public figures,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

including *Anil Kapoor v. Simply Life India & Ors.* (2023), *Shroff v. The Peppy Store & Ors.* (2024) and *Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors.* (2025), demonstrate growing judicial willingness to protect aspects of personality against unauthorised exploitation. Such protection supports recognition of a dignity-based interest distinct from transferable commercial publicity rights, while preserving safeguards for legitimate criticism, parody and commentary. Overall, India's existing framework can address several manifestations of AI-enabled identity abuse, but its fragmented character creates gaps concerning definitional clarity, consent, attribution, rapid removal, platform responsibility, evidence preservation and victim-centred remedies. Constitutional principles provide the normative foundation; technology law facilitates digital enforcement; data-protection law addresses personal-data processing; criminal law addresses specific harmful conduct; and evidentiary law supports authenticity and admissibility. A comprehensive framework should build upon these principles through technology-neutral definitions, clear consent and attribution standards, differentiated civil and criminal remedies, coordinated institutional procedures, evidence-preservation duties and safeguards for legitimate expression. Such an approach would strengthen protection of women's privacy, dignity, autonomy, reputation and identity while ensuring that regulation remains precise, proportionate and consistent with constitutional freedom of expression.

Comparative Legal Approaches to AI-Enabled Threats Against Women.

The regulation of AI-enabled threats against women demonstrates three distinct but complementary approaches in India, the United States and the United Kingdom, each attempting to reconcile individual protection, platform responsibility, technological innovation and freedom of expression. The United States adopts a comparatively decentralised model combining federal legislation, state criminal laws, tort principles, privacy protections and publicity rights, while constitutional protection of speech places significant limits on governmental regulation. A significant recent development is the TAKE IT DOWN Act, which establishes a federal framework addressing the publication of non-consensual intimate visual depictions, including covered digitally manipulated or AI-generated content, and introduces notice-and-removal obligations for covered platforms. Its significance lies in recognising that digitally fabricated intimate material can cause serious harm even where the underlying photograph or other source material was originally obtained lawfully. The U.S. approach therefore offers India useful lessons concerning precise statutory definitions, consent-based protection and rapid platform procedures, although its federal-state division may create variations in enforcement and available remedies. The United Kingdom has adopted a more integrated statutory and regulatory model. The criminal-law framework addresses the sharing, creation and requesting of intimate images without consent, including certain forms of purported intimate imagery, while the Online Safety Act 2023 places broader systems and process obligations on regulated online services. The United Kingdom therefore moves beyond a purely victim-versus-perpetrator model by recognising the role of platforms in preventing, detecting and responding to harmful content. The Online Safety Act 2023 and also Data (Use and Access) Act 2025 further demonstrates the continuing development of the United Kingdom's digital regulatory architecture. The principal comparative advantage of the UK model is its combination of offence-specific criminalisation with platform-level regulatory duties, although effective implementation continues to depend upon clear statutory thresholds and proportionate enforcement. India, by comparison, presently relies on a fragmented framework consisting of constitutional rights, information-technology regulation, data-protection law, criminal provisions, electronic-evidence rules and personality-rights jurisprudence. Articles 14, 19 and 21 provide the constitutional foundation by protecting equality, expression, privacy, dignity and personal autonomy, while the Information Technology Act, 2000, the Information Technology Rules, 2021, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023 provide different forms of statutory protection. Indian courts can also employ injunctions and personality-rights principles to restrain unauthorised use of an individual's name, image, voice or persona. However, unlike the more specific U.S. and UK responses, India does not yet possess a comprehensive statutory regime specifically directed at AI-generated identity abuse. The comparison consequently reveals important lessons for Indian law. From the United States, India may adopt clearly defined concepts of non-consensual digital forgery, consent-based liability and expedited notice-and-removal procedures; from

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

the United Kingdom, it may draw upon integrated platform obligations, criminal regulation of purported intimate imagery and systems-based online safety duties. At the same time, India should preserve its own constitutional emphasis on dignity, privacy, equality and proportionality rather than mechanically importing foreign models. Across all three jurisdictions, the principle of contextual integrity provides a useful analytical foundation: lawful access to identity-bearing material for one purpose should not automatically imply consent to its AI transformation, commercial exploitation or dissemination to a different audience. A balanced framework should distinguish interim protection from final liability, permitting rapid restriction where identifiability, lack of consent and serious risk are prima facie established, while requiring stronger proof of fault, causation and attribution for criminal conviction or substantial damages. Ultimately, the comparative experience supports a layered regulatory model for India combining individual rights, targeted criminal offences, platform accountability, data governance, evidence preservation, accessible civil remedies and procedural safeguards. Such an approach would provide stronger protection for women against AI-enabled digital abuse while maintaining due process, legitimate expression and technological innovation.

Towards a Comprehensive Legal Framework.

A comprehensive legal framework for AI-enabled identity abuse must move beyond the fragmented regulation of privacy, defamation, intellectual property, intermediary liability and cybercrime. Synthetic identity abuse cannot be adequately addressed through laws designed primarily around unauthorised access, publication, ownership or conventional forms of falsity, because the underlying harm may arise even where the original image, voice or personal information was lawfully available. The principal legal challenge is therefore to establish a framework that protects an individual's control over identity without unduly restricting legitimate expression, technological innovation or public-interest uses of synthetic media. Such a framework should be rights-based, consent-centred and proportionate to the degree of risk and harm involved. A model law should define synthetic identity content broadly to include audio, visual, audiovisual and functionally equivalent digital material that represents, appears to represent, or is reasonably attributable to an identifiable person. Regulation should be based on the context and consequences of use rather than technological novelty alone. The principle of contextual integrity provides an appropriate foundation: material made available for one legitimate purpose should not automatically be treated as consent for its transformation, replication, commercialisation or dissemination in another context. Legal assessment should accordingly consider the relationship between the individual, the representation, the purpose of processing, the existence and scope of consent, and the foreseeable consequences of dissemination. Consent should be evaluated independently at each stage of the data and content lifecycle, including collection, training, generation, editing, retention, publication, monetisation and onward transfer. Consent obtained through deception, coercion, bundled contractual terms or significant power imbalances should not legitimise high-risk identity replication. The framework should also establish clearly defined legal elements and evidentiary thresholds so that urgent protection can coexist with procedural fairness. Interim restrictions may be appropriate where there is a prima facie showing of identifiability, lack of consent and serious risk, while final civil liability or criminal responsibility should require appropriate proof of fault, causation and attribution. Liability should further be distributed according to the role, knowledge, control, benefit and capacity of each participant. Creators and those who intentionally commission or disseminate harmful synthetic content should bear primary responsibility, while platforms should assume proportionate duties relating to notice, review, evidence preservation and systemic failures. AI providers should undertake reasonable safety-by-design obligations corresponding to the foreseeable risks and scale of their systems, without being subjected to indiscriminate strict liability or unrealistic general monitoring requirements. Institutional coordination is equally necessary. Courts should determine contested rights and grant appropriate injunctions; law-enforcement agencies should investigate serious offences; data-protection authorities should address unlawful processing; and platforms should provide rapid mechanisms for restricting harmful hosted or indexed material. Clear referral mechanisms should prevent victims from repeatedly presenting the same factual circumstances before different institutions. An effective emergency-remedy system should therefore provide a single and accessible complaint mechanism, confidential handling, trained human review, secure evidence preservation and prompt access to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

an independent decision-maker. Restrictions should remain narrowly tailored and subject to meaningful review and appeal so that protection against abuse does not become a mechanism for suppressing legitimate speech. AI providers should additionally conduct risk assessments before deployment and after material system changes, particularly where their products enable identity replication. Appropriate safeguards may include access controls, rate limits, abuse-reporting mechanisms, secure logging, provenance measures and the rapid disabling of compromised functionalities. Privacy by design should operate throughout the system lifecycle through data minimisation, lawful processing, restrictions on identity-data extraction, meaningful consent verification for high-risk cloning and proportionate retention and deletion controls. Finally, the framework must remain victim-centred. Individuals affected by synthetic identity abuse should not be required to identify the precise technical model, legal offence or responsible intermediary before obtaining urgent protection. Remedies should include injunctions, removal and de-indexing, disclosure where necessary for attribution, compensation, correction and appropriate legal support, while procedures should minimise repeated exposure to harmful material and secondary victimisation. Existing constitutional principles, privacy doctrine, personality rights, intermediary regulation and electronic-evidence rules can provide important foundations, but they cannot substitute for legislation where recurring forms of synthetic identity abuse remain inadequately addressed. A comprehensive framework should therefore integrate substantive rights, meaningful consent, graduated liability, coordinated enforcement, emergency remedies, privacy-by-design obligations and accessible victim-centred relief while maintaining proportionality, freedom of expression, evidentiary fairness and judicial oversight.

II. CONCLUSION

Artificial Intelligence has fundamentally transformed the nature of digital identity and exposed significant weaknesses in existing mechanisms for protecting women's digital security. Generative AI, deepfakes, voice cloning and other forms of synthetic media now make it possible to reproduce, manipulate and redistribute a woman's face, voice, body and identity with unprecedented speed, scale and realism. The resulting harm extends beyond the creation of false information as it involves the unauthorised appropriation of identity and the imposition of fabricated conduct, statements or circumstances upon an identifiable individual. Digital security must therefore be understood more broadly than the protection of devices, accounts or personal data. It encompasses privacy, dignity, autonomy, reputation, bodily and sexual integrity, personal safety and meaningful control over one's digital identity. Existing legal protections can address particular forms of AI-enabled abuse, but remain fragmented across privacy and data protection, criminal law, defamation, personality rights, intermediary regulation and constitutional principles. India's regulatory framework is also evolving in response to these emerging risks, as reflected in the February 2026 amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which introduce specific regulatory measures concerning Synthetically Generated Information (SGI), thereby strengthening the legal response to AI-generated and manipulated digital content. This fragmentation creates uncertainty regarding applicable remedies, liability and institutional responsibility, particularly where synthetic content is false but nevertheless causes substantial personal, professional or social harm. A coherent response must recognise the distinctive nature of synthetic identity abuse while avoiding disproportionate restrictions on legitimate expression. The principle of contextual integrity is important in this regard because the lawful availability of an image, recording or other identity bearing material in one context cannot automatically constitute consent to its alteration, sexualisation, commercial exploitation or dissemination in another. Future regulation should therefore adopt a rights-based, consent-centred and technologically neutral framework that clearly defines synthetic identity content, digital replicas and meaningful consent, while distinguishing civil wrongs from narrowly defined criminal conduct. It should provide accessible and proportionate remedies, including urgent interim measures where there is a credible and serious risk of harm, while preserving procedural safeguards, freedom of expression and the right to contest allegations. Evidence preservation must operate alongside removal or restriction so that immediate protective action does not destroy material necessary for investigation and adjudication. Institutional coordination is equally essential. Courts, police authorities, data-protection institutions and intermediary grievance mechanisms should operate through clearly defined responsibilities and referral

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

procedures rather than requiring victims to repeatedly present the same complaint and evidence. A coordinated system should facilitate rapid platform notification, evidence preservation, investigation and referral while protecting victims through appropriate confidentiality measures. Responsibility must also extend across the technological ecosystem. AI developers should incorporate safeguards against foreseeable misuse, while platforms and search services should maintain effective mechanisms for reporting, reviewing, restricting and, where legally justified, removing or de-indexing harmful synthetic content. At the same time, journalism, research, public-interest communication, satire, parody, artistic expression and other legitimate activities must remain protected through clear safeguards and proportionality requirements. Ultimately, legal effectiveness should be assessed not merely by the existence of legislation, but by whether affected women can obtain timely, meaningful and accessible protection. The speed of provisional containment, preservation of evidence, effectiveness of de-indexing, availability of compensation, prevention of repeated dissemination and accessibility of remedies should constitute important measures of regulatory success. The erosion of women's digital security through AI is therefore not merely a technological problem but a broader challenge to privacy, dignity, equality and individual autonomy. As AI increasingly enables the reproduction and manipulation of human identity, legal protection must evolve beyond safeguarding information and access towards meaningful control over digital identity. Regulation should foster technological innovation without permitting it to undermine women's dignity, autonomy, or participation in digital society. A balanced legal framework must therefore place human autonomy at its core, ensuring effective protection through proportionality, due process, accountability, and respect for legitimate expression.

BIBLIOGRAPHY

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India). https://indiankanoon.org/doc/127517806/
2. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India). https://indiankanoon.org/doc/110813550/
3. Information Technology Act, 2000, No. 21 of 2000, India Code. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/static/uploads/2026/03/0b576f2071694b52e4cd6bb1b6dfab1e.pdf
5. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
6. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code. https://www.indiacode.nic.in/bitstream/123456789/20062/1/a202345.pdf
7. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, India Code. https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf
8. Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-12, 139 Stat. 55 (2025). https://www.govinfo.gov/content/pkg/PLAW-119publ12/pdf/PLAW-119publ12.pdf
9. Online Safety Act 2023, c. 50 (U.K.). https://www.legislation.gov.uk/ukpga/2023/50
10. UN Women - How AI is Exacerbating Technology-Facilitated Violence Against Women and Girls (2025). https://digitallibrary.un.org/record/4099277?v=pdf