

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DEEPFAKES AND HUMAN RIGHTS: PROTECTING PRIVACY AND DIGNITY IN THE DIGITAL AGE

AUTHORED BY - MANISHA BRAHMA¹

ABSTRACT

The swift evolution of generative artificial intelligence has shifted deepfakes from a mere technological novelties into a global serious human rights concern. By allowing artificial replication of human faces, voices, and appearance, synthetic media can threaten privacy, dignity, and individual's identity. This paper evaluates these challenges through the lens of Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, that both protect individuals from arbitrary interference of privacy and reputation. It focuses on three emerging harms: non-consensual creation of sexually explicit deepfakes that targets women, manipulated audio, video use to intimidate or mute political dissidents and the rise of liar's dividend, an issue where existence of deepfake technology lets people dismiss authentic evidence as fake. It compares the European Union Artificial Intelligence Act with India's developing digital regulatory framework to see if the existing legal responses can effectively address such harms or not. Even the traditional defamation laws fail to fully capture the distinctive harms caused by unauthorized synthetic version of actual people. so, it tried to proposes for "Likeness Sovereignty" as a possible human rights framework. This model aims to protect individuals by providing them strong legal control over the unauthorized digital reproduction and manipulation of their face, voice, and identifying characteristics. The goal of this proposal seeks to strengthen protection for human dignity and personal independence while still leaving room for the growth in technological innovation.

KEYWORDS

Deepfakes, Human Dignity, Privacy, Synthetic Media, Likeness Sovereignty.

¹ Cooch Behar Panchanan Barma University, Cooch Behar.

1. INTRODUCTION

In current digital landscape, our faces and voices are no longer just physical features, they now works as our unique biometric signatures. For generations, society and global legal systems operated on unwritten theory- “seeing is believing.” A photo or a video recording was use to be treated as solid evidence that an event took place or a particular words were uttered. Yet, the sudden aggressive rise of consumer-facing generative artificial intelligence has completely broken this foundational trust. Today, the easy access to advanced machine learning algorithms allows virtually anyone with basic net connections to copy a person’s voice print or map out facial geometry in mere seconds without their consent. This technological shift has turned deepfakes from interesting coding curiosity into an active, weaponized threat for global human rights. When an individual’s identity can be duplicated and synthetically altered, it violates the core of an individual’s autonomy. Such malicious alterations directly damages the basic human rights to privacy, personal honour, and individual dignity-protections that are explicitly guaranteed to all human beings under international treaties like Article 12 of the Universal Declaration of Human Rights² and Article 17 of the International Covenant on Civil and Political Rights.³ The internet functions across borderless networks, domestic legal structures are proving to be physically incapable to stop the viral spread of synthetic abuse before it inflicts permanent psychological and trauma on any individual.

It argues that isolated state-centric laws are poorly equipped to handle a decentralized identity crisis. While advanced region like the European Union have brought systemic regulations via the landmark EU AI Act⁴ to enforce technical watermarking, and nations like India align with strict Information Technology Rules⁵ to pressure social media platforms into fast content removal. These fragmented approaches create major gaps in enforcement. To safeguard human dignity in this digital age, international human rights law must needs an active paradigm shift. Even, this paper will step-by-step analyze the limitations of current global treaties, in details outline the three-parted threat of contemporary deepfake harms. Evaluation on the structural differences between the European and Indian regulatory laws, and final goal towards a new international legal norm “Likeness Sovereignty.”

² Universal Declaration of Human Rights art. 12, G. A. Res. 217 (III), U. N. Doc. A/RES/217 (III) (Dec. 10, 1948).

³ International Covenant on Civil and Political Rights (ICCPR) art. 17, Dec 16, 1966, 999 U. N.T. S. 171.

⁴ European Union (2024) ‘Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)’, Official Journal of the European Union, L Series, 12 July.

⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended by Amendment Rules, 2023), Ministry of Electronics and Information Technology, Gazette of India, Extra., pt. II sec. 3(i) (6 April 2023).

2. THE NORMATIVE FOUNDATIONS OF DIGNITY

Arrival of high-realistic synthetic media demands for a complete reassessment of digital harms under contemporary legal frameworks. We no longer treat deepfakes as mere online jokes, minor data leaks, or data privacy issues. Instead, the unapproved duplication and alteration of an individual's face or voice print recognizes as a direct, systemic violation of human rights. Entire international legal structure is based on a fundamental, non-negotiable promise. That every single person has an absolute right to personal autonomy, privacy, and control over their own identity. If generative artificial intelligence is weaponized to hijack these biometric traits of an individual without explicit consent, it shatters the moral foundation of our global treaties. Technological disruption changes the actual meaning of privacy, turning it from protecting physical property into a shield for human personhood itself.

If we look for the main international anchor for protecting personal identity from digital abuse, we find inside Article 12 of the Universal Declaration of Human Rights.⁶ This classic text states that no individual shall face arbitrary interference with their privacy, family, home, or correspondence. It blocks targeted attacks on person's honour and reputation. The people who drafted this declaration did not restrict privacy rights only to physical borders, bank records, or tangible property they openly recognized a person's honour and reputation as core human rights that requires active legal protection. In our contemporary digital era, deepfakes have become the ultimate weapon against individual honour. When attacker maps the victim's face to explicit material or clones their voice to spread lies, they execute a brutal character assassination. This instantly destroy person's social status, livelihood, and mental well-being.

Moral protection turns into a binding, positive legal obligation under Article 17 of the International Covenant on Civil and Political Rights.⁷ It mirrors the protective language of UDHR, placing strict duty on signatory countries to pass strong domestic laws that actively protect citizens from such illegal interferences. Under the global human rights system, governments cannot stay neutral or act indifferent towards technological changes. They are legally bound to step in when unregulated digital actors or commercial platforms expose individuals to identity abuse. Deepfakes completely broke the social contract built by the covenant. Because generative tools let attackers to launch borderless, untraceable identity violations, leaving victims to face massive public humiliation without any clear legal path to fix damage or reclaim their dignity.

⁶ Universal Declaration of Human Rights, Supra note 2.

⁷ International Covenant on Civil and Political Rights, Supra note 3.

Our traditional legal rules needs a deep structural evolution. Why? Because generative AI creates complete new category of harms that classic privacy laws were never designed to handle such. Old data protection rules only linked to regulate static information like-private paperwork, financial files, or stolen photos. Generative artificial intelligence, does not leak existing private data, it actively builds entire new, fake realities. When an unauthorized deepfake video or voice is made, it forces a living individual to speak words that they never chose to perform actions they never consented for. Recent international human rights studies emphasize that digital transformation must not erase human agency. They warns that automated systems risk wiping out the core value of human interaction if it left unchecked or unregulated.⁸ It makes deep unsettling reality where a person can lose ownership over their own visual and vocal presence in the world.

So, the global legal community must realize that passive data protection rules and slow, reactive laws are no longer enough to defend human personhood. To protects individual's privacy and dignity in this digital arena, international law must make a proactive transition. The world requires a recognized legal norm rooted in "Likeness Sovereignty"- principle that every human being has an absolute, inalienable right to legal ownership over their own biometric data and digital reflection. Global human rights assessments indicate that the legitimacy of new systems should be judged by how well they uphold human dignity rather than their technological sophistication alone.⁹ Without this critical legal shift, our foundational rights to honour, privacy, and basic human dignity will be rendered entirely meaningless in an environment ruled by unchecked synthetic manipulation.

3. THE TRAIID OF CONTEMPORARY HARMS

The abstract dangers of generative artificial intelligence become devastatingly clear when we examine how synthetic media is deployed in the real world. Deepfakes are not merely futuristic software concepts or innocent technical novelties they are current, active weapons used to violate human dignity, disrupt democratic discourse, and silence targeted individuals. To understand the full scale of this human rights crisis, the practical damage caused by synthetic manipulation must be evaluated across three distinct operational categories: the creation of non-consensual intimate imagery, the execution of transnational repression against journalists,

⁸ Farida Shaheed, Special Rapporteur on the Right to Education, Impact of Digitalization and Artificial Intelligence on the Right to Education, 4 -6, U.N. Doc. A/79/520 (Oct. 16, 2024).

⁹ United Nations Educational Scientific and Cultural Organization, AI and Education: Protecting the Rights of Learners, 12-15, (Paris, UNESCO Publishing, 2025).

and the systemic rise of the political “liar’s dividend.”

A. Non -Consensual Intimate Imagery (NCII) as Gender-Based Violence

The primary and most widespread deployment of malicious deepfake technology is overwhelmingly gendered. Current empirical tracking indicates that a vast majority of synthetic videos circulating online involve the unauthorized superimposition of women’s faces onto explicit adult content. This practice represents a severe breach of bodily autonomy and a direct violation of individual dignity. Framework of the United Nations Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), states to protect women from systematic digital violence that limits their equal enjoyment of human rights.¹⁰ Standard system frequently view these violations through a narrow scope of property copyright laws or public obscenity statutes. Yet, this traditional perspective completely misses the main problem: maps down person’s physical appearance into explicit media without permission is a direct violent attack on their mental stability and dignity.

A real-world example of this harm occurred in widely publicized case of Indian actress Rashmika Mandanna.¹¹ A viral clip spread online showing the actress’s face digitally superimposed into the body of another individual through advanced deep learning tool. Although law enforcement authorities reacted by filing a First Information Report (FIR) under Sections 66D and 66E of the Information Technology Act, 2000-punishes cheating by personation and violations of bodily privacy-the digital humiliation was instant and massive.¹² The case highlights why reactive, country-specific laws simply fall short. By the time a local police cyber-unit manages to track a digital footprint and register a complaint, the victim’s reputation has already been damaged on a global level. This situations demonstrates that unauthorized synthetic media functions as a direct tool for gender-based harassment, reducing person’s biological identity into an unapproved public commodity.

B. Transnational Repression and the Silencing of Dissidents

Closely mirroring this targeted, gender-based violence, deepfakes have quickly evolved into modified instruments for political conflicts and borderless repression. Authoritarian government and corrupt political groups are no longer restricted by physical borders when

¹⁰ Convention on the Elimination of All Forms of Discrimination against Women art. 1, Dec. 18, 1979, 1249 U.N.T.S. 13.

¹¹ Ministry of Electronics & Information Technology, Government of India, “Advisory to Significant Social Media Intermediaries on Deepfakes,” (Press Information Bureau, November 7, 2023), pib.gov.in.

¹² The Information Technology Act, 2000, §§ 66D-66E, No. 21, Acts of Parliament, 2000 (India).

trying to intimidate their critics. Taking the advantage of high-quality voice cloning and automated facial editing, bad actors can manufacture realistic fake videos of investigating journalists, human rights activists, and opposition leaders. Those fabrications are intentionally created to destroy their professional standing, isolate them from their communities, and scare them into complete silence. This targeted usage hits at heart of Article 19 of the International Covenant on Civil and Political Rights (ICCPR)-guarantees the fundamental right to hold opinions without interference and to freely share, receive information.¹³

A major example of this political weaponization is the severe harassment campaign aimed at the globally recognized investigative journalist Rana Ayyub.¹⁴ Ayyub, known for her sharp reporting on structural corruption and human rights abuses, faced organized digital assault that featured realistic, non-consensual deepfake clips. The explicit synthetic content was shared across mainstream social platforms with clear intent to ruin her professional reputation and erase her journalistic works. This case shows a terrifying development in the deepfakes allowing political actors to carryout borderless character assassination. When an activist or journalist can have their actual face and voice stolen to mimic compromising things, the digital space becomes completely toxic to free speech, converting generative AI into an efficient tool for cross-border human rights violations.

C. The Liar's Dividend and the Destruction of Democratic Truth

The third dimension of contemporary harm moves beyond the direct victimization of individuals and threatens the stability of public truth itself. This trend is known as the “Liar’s Dividend.” More the person gets aware that audio and video can be faked using basic AI software, a dark legal paradox emerges. Corrupt politician, human rights offenders, and corporate criminals can take merit from this widespread digital skepticism to escape accountability. When authentic video evidence of their crimes or corruption surfaces, they simply brush the evidence by falsely claiming that the video is just an AI-generated deepfake. This effectively ruins the value of objective visual evidence within courtroom trials and public debates.

Such well-structural organized manipulation of truth was clearly observed in the Venezuelan State Propaganda Campaign.¹⁵ State-backed media networks deployed hyper-realistic,

¹³ International Covenant on Civil and Political Rights, Supra note 3, art. 19.

¹⁴ Irene Khan, Mandates of the Special Rapporteur on Freedom of Opinion and Expression and the Special Rapporteur on the Situation of Human Rights Defenders, 2 -4, U.N. Doc. AL IND 3/2020, (February 10, 2020).

¹⁵ ProBox Digital Observatory, Report on Transnational Information Manipulation (2023): Synthesized Propaganda: How the Venezuelan Government Uses AI News Anchors to Spread Misinformation, 2023, 8-10.

synthetic news anchors-built by AI platforms that named Noah and Daria to read false news stories that minimizes the nation's economic crises while praising government policies. It was a deliberate move to blur the line between real journalism and automated propaganda. The danger of the liar's dividend is that it slowly effects the public's core human right in order to find authentic facts and hold power accountable. When people no longer tell the difference between a real human being and an algorithmic product, trust in democratic institutions collapses undoubtedly. Giving actual human rights abusers to hide behind the excuse of digital simulation.

4. COMPARATIVE DOMESTIC JURISPRUDENCE

International treaties offers a vital ethical shield for human value, these protections remain abstract ideas until enforced by actual national laws. To know how states deal with the deepfake crisis today, we have to look into world's digital legal models: European Union and India. They both tackle identity protection from completely opposite angles. The European Union relies on a proactive, preventive approach that targets the tech supply chain itself. In contrast, India uses reactive framework that focuses directly on the digital content delivery pipeline. Looking at the strengths and gaps of both models reveals how hard it is to protect human rights in borderless digital world.

A. The European Union Model: Proactive Supply-Chain Transparency

The European Union has established the world's most comprehensive regulatory framework for artificial intelligence by passing the landmark European Union Artificial Intelligence Act.¹⁶ Instead of waiting for a malicious deepfake to go viral and then trying to track down an anonymous internet user, the European framework halts the harm from its source. The fundamental design of the EU AI Act rests on a strict risk-classification system. Under this, generative AI tools capable of creating or twisting high-fidelity synthetic sound, video, or imagery are categorized as carrying specific transparency risks. Legal classification forces tech developers and software providers to follow demanding safety protocols before their can launch or sell products inside the European market. The core of this European blueprint is a strict transparency mandate. Under Article 50 of the EU AI Act, developers of generative AI systems must design their software outputs to be technically identifiable.¹⁷ Meaning any AI-

¹⁶ European Union Artificial Intelligence Act, supra note 4.

¹⁷ European Union Artificial Intelligence Act, Supra note 4, art. 50.

generated video, photo, or audio file must automatically include invisible, machine-readable cryptographic watermarks directly within its digital metadata. These technical markers relate with global data tracking protocols, allows websites and security software to directly identify content as artificial.¹⁸ On top of that, the legislation places direct legal duty on ordinary users who generate deepfakes to explicitly disclose their work. If someone uses AI to replicate a video that realistically resembles like real person or event, they are required to feature a clear disclosure on the screen declaring that file has been artificially altered. Shifting the burden of safety on developers and creators, the EU aims to protect the public from being deceived, preserving individual reputation and shared truth as well.

B. The Indian Framework: Intermediary Liability and Urgent Takedowns

In contrast to the European Union's focus on tech developers, India crafted rapid - response model that zeroes in on the distribution pipeline. One of the largest consumer-internet landscape, India faces immediate, viral threat from synthetic media. Because of this urgency, the government avoids long-term supply-chain watermarking to take effect. Instead, relies on strict intermediary liability laws to force social media platforms like Meta, X, and Instagram to monitor and wipe out malicious content from their networks instantly.

The main legal tool for this approach is in Section 79 of the Information Technology Act, 2000, grants platforms "safe harbour" immunity, shields from being legally responsible for the content uploaded by ordinary users.¹⁹ However, this immunity is conditional. Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, if an internet company receives a complaint about harmful deepfake, it has to move very fast.²⁰ Following multiple high-profile deepfake incidents involves celebrities, India's Ministry of Electronics and Information Technology stepped in with directives to tighten these rules.²¹ Under the current framework, platforms have a strict legal obligation to remove non-consensual explicit deepfakes within 24-36 hours of a report. If a platform fails to execute this rapid content takedown, it instantly loses its safe harbour protection and its executives can face criminal prosecution as co-conspirators to the crime. This urgent approach prioritizes protecting the victim's dignity by containing the digital wildfire before it can spread completely across the population.

¹⁸ Coalition for Content Provenance and Authenticity, C2PA Technical Specifications for Media Provenance Tracking, 44–48, (C2PA Standards Organisation, 2023).

¹⁹ The Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Supra note 5.

²¹ MeitY Deepfake Advisory, Supra note 11.

C. The Enforcement Blindspot of Territorially Bound Laws

Analyzing both systems shows structural conflict between the borderless nature of generative AI and the physical limit of national laws. The European Union's model is highly excellent, but it suffers technical loopholes. Cryptographic watermarking and metadata tags are fundamentally fragile can be stripped away by taking simple screenshot of video, screen-recording an audio track, open-source code etc. Once metadata watermark removed, the EU AI Act loses ability to track the fake. Otherside, India's reactive framework puts pressure on social media networks, but only operates after the crime has occurred. Despite the direct removal of explicit deepfake successfully deleted within 24 hours, but the viral nature of modern internet-means thousands of users already viewed, downloaded, and shared their file across encrypted, private messaging applications like WhatsApp. Because both frameworks works within their territorial jurisdictions, they are helpless against international attackers. An anonymous bad actor sitting outside European or Indian territory uses unregulated open-source AI tools to attack victim's face, host the file on decentralized server, and distribute it globally. Jurisdictional friction shows that independent domestic laws are unequipped to handle borderless identity theft, proves that local enforcement may not fully shield individual human dignity in digital era.

5. ENFORCEMENT VULNERABILITIES AND STURCTURAL GAPS

Differences between digital advancement and rule of law clears up why our current laws fail to protect individuals from synthetic exploitation. Even with European Union's technical watermarking rules, India's intermediary takedown timelines, the structural design of modern internet provides a safe haven for malicious actors. Traditional legal system works around the concept of physical borders, identifiable perpetrators, and tangible property harms. However, generative AI works upon decentralized networks, automation, and intangible harms. This mismatch lead to enforcement vulnerabilities, making existing civil and criminal remedies essentially useless. The first obstacle is anonymity loophole interconnected with open-source software. While commercial platforms sets strict safety filters which block users from generating explicit material or cloning, machine learning source code is out of the bottle. Malicious actors not uses corporate interface to commit crimes, they download unregulated, open-source diffusion models in their private computers.²² Because such model runs locally without linking to a corporate server, doesn't include safety guardrails, cryptographic

²² European Union Artificial Intelligence Act, Supra note 4, art. 50.

watermarking tracking, or checks user identity. Any one can generate high-fidelity deepfakes without leaving a trace, making supply-chain regulations ineffective. When files are uploaded via virtual private networks (VPNs) and distributed across decentralized platforms, tracing of real identity becomes hurdlesome for local law enforcement authorities.²³ This anonymity is further protected by end -to-end encrypted messaging channels and decentralized file hosting networks. When any harmful video involves individual's likeness shared inside the private chat groups like Telegram or WhatsApp, such encrypted protocols block platforms and police forces from monitoring or filtering the content. Leading to severe legal blindspot. India's Information Technology Rules requires public platforms to remove reported deepfakes within 24-hour window, but cannot stop any file from spreading across millions of private, encrypted chat loops. The damage to individual's mental equilibrium and personal dignity occurred in private digital spaces, legal and technical barriers leaves the state powerless to intervene legal consequences. Even reactive distribution controls cannot stop a viral digital wildfire.

Classical civil and tort remedies-defamation and copyright infringement are unequipped to address synthetic identity theft. Defamation law requires victim to prove that an absolute, false statement of fact was made about them to a third party. Here, deepfakes not just communicates false statement, it makes a false visual experience of reality. When victim's face is mapped to an explicit video, the harm extends beyond criticism, it is direct assault on physical personhood where bodily autonomy is digitally hijacked. Handling this harms as minor reputational injury or property copyright issue it entirely, misses out the point. A person's face and voice are not commercial properties they are the literal expressions of their human dignity.

It brings up to view the vulnerability of contemporary legal systems, jurisdiction hopping. Why so? Because the internet is borderless, bad actor sitting in one country targets a citizen living in another country, hosts malicious file on a server located in third country, distribute through an app registered in other country. Local cyber-crime cell has no legal authority to issue warrants cross-borders or force foreign web host to take down an illegal file. Conventional international legal assistance treaties works at slowpace, takes months or years to execute a single digital data request. In the digital age, the deepfake can destroy person's life and reputation within hours, our territorial bounded legal laws leaves victim exposed fully, establishes we cannot protect human dignity with fragmented national laws.

²³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Supra note 5.

6. CONCLUSION

The high-speed growth in generative artificial intelligence fundamentally altered the relationship between human personhood and the digital landscape. As stated throughout, deepfakes can no longer only counted as novelties or minor privacy breaches. It represents interlinked weaponized assault on human worth, privacy, and individual autonomy. Turning an individual's unique biological signatures-face, voice print into manipulative digital products, synthetic media strips away victims control over their personal identity. Old legal frameworks, roots with state-sovereignty, restricted territorial boundaries, are structurally incapable to deal this borderless viral threat. Neither proactive supply-chain watermarking mandates of European Union AI Act nor reactive distribution takedowns of India's Information Technology Rules can completely safeguard individual human dignity from decentralized, cross-border exploitation.

To settle such systemic crisis, global legal community must let go of reactive, fragmented regulatory plans and accepts profound paradigm shift. This essay proposes the new international human rights norm "Likeness Sovereignty." Likeness Sovereignty-defined as absolute, inalienable legal ownership of every human being over their own biometric data, voice prints, and digital reflection across all global networks. This framework moves beyond passive data protection rules, establishes an individual's likeness as extension of their bodily integrity. Under a global convention on synthetic media, any unauthorized extraction or manipulation of a person's biometric signatures must be treated as a direct violation of their fundamental rights to honour and reputation as promised under long-standing global treaties. This framework would legally obligate states to recognize cross-border biometric identity theft as a severe, extraditable offense, rendering the current strategy of jurisdiction hopping completely ineffective.

Furthermore, implementing Likeness Sovereignty requires a unified integration of international policy and tech engineering standards. True digital safety cannot rely on localized enforcement, it requires a global digital architecture where zero-trust provenance systems are embedded into the very fabric of the internet. Software providers and online platforms must be held globally accountable under international standard-setting bodies to implement unstrippable verification standards. Ultimately, the true success of the digital age must never be measured by the visual perfection or processing speed of generative machine learning models. Instead, it must be judged by how securely an ordinary human being can navigate the digital space without fear of having their identity hijacked and their dignity destroyed. By shifting the global focus from technological convenience to human-centered sovereignty, international law can ensure that

artificial intelligence serves to augment human progress rather than diminish the sacred value of human personhood.

AUTHORITIES

1. Universal Declaration of Human Rights art. 12, G. A. Res. 217 (III), U. N. Doc. A/RES/217(III) (Dec. 10, 1948).
2. International Covenant on Civil and Political Rights (ICCPR) art. 17, Dec 16, 1966, 999 U. N.T. S. 171.
3. European Union (2024) 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)', Official Journal of the European Union, L Series, 12 July.
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended by Amendment Rules, 2023), Ministry of Electronics and Information Technology, Gazette of India, Extra., pt. II sec. 3(i) (6 April 2023).
5. Farida Shaheed, Special Rapporteur on the Right to Education, Impact of Digitalization and Artificial Intelligence on the Right to Education, 4-6, U.N. Doc. A/79/520 (Oct. 16, 2024).
6. United Nations Educational Scientific and Cultural Organization, AI and Education: Protecting the Rights of Learners, 12-15, (Paris, UNESCO Publishing, 2025).
7. Convention on the Elimination of All Forms of Discrimination against Women art. 1, Dec. 18, 1979, 1249 U.N.T.S. 13.
8. Ministry of Electronics & Information Technology, Government of India, "Advisory to Significant Social Media Intermediaries on Deepfakes," (Press Information Bureau, November 7, 2023), pib.gov.in.
9. The Information Technology Act, 2000, §§. 66D-66E, No. 21, Acts of Parliament, 2000, India.
10. International Covenant on Civil and Political Rights (ICCPR) art. 19, Dec 16, 1966, 999 U. N.T. S. 171.
11. Irene Khan, Mandates of the Special Rapporteur on Freedom of Opinion and Expression and the Special Rapporteur on the Situation of Human Rights Defenders, 2-4, U.N. Doc. AL IND 3/2020, (February 10, 2020).
12. ProBox Digital Observatory, Report on Transnational Information Manipulation (2023): Synthesized Propaganda: How the Venezuelan Government Uses AI News Anchors to Spread Misinformation, 2023, 8-10.

13. Coalition for Content Provenance and Authenticity, C2PA Technical Specifications for Media Provenance Tracking, 44-48, (C2PA Standards Organisation, 2023).
14. The Information Technology Act, 2000, §. 79, No. 21, Acts of Parliament, 2000, India.

