VOLUME 7 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

AI-GENERATED DEEPFAKES AND CROSS-BORDER CYBERCRIME: AN ANALYSIS OF INDIA'S LEGAL FRAMEWORK AND EMERGING NORMS OF CUSTOMARY INTERNATIONAL LAW

- Nitansha Bhatia[1] & Ishita[2]

Abstract

Generative artificial intelligence has made it cheap to fabricate convincing audio and video of real people, and offenders use that capability for fraud, extortion, intimate imagery and political deception across borders. This paper asks whether India's legal framework can answer deepfakes that are made in one country, hosted in another and aimed at victims in India, and whether emerging international practice is hardening into customary international law. Using doctrinal, comparative and international legal analysis, it examines the Information Technology Act, 2000, the 2026 amendment to the Intermediary Rules, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023, and compares them with the approaches of the European Union, the United States and the United Kingdom. It then tests proposed international norms against state practice and opinio juris. The paper finds that Indian law is technology-neutral and partly adequate but fragmented, and weakest on attribution, evidence and foreign enforcement. Cooperation, due diligence and labelling are best described as treaty-based, contested or emerging standards, while sovereignty and non-intervention are the only established rules that can reach deepfake operations.

Keywords: Artificial intelligence; deepfakes; cybercrime; cross-border jurisdiction; Indian cyber law; customary international law; electronic evidence; intermediary liability.

I. Introduction

[1] LL.M. (Cyber Law & Cyber Security), Amity University, Noida
[2] LL.M. (Cyber Law & Cyber Security), Amity University, Noida
For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

© 2026 International Journal of Advanced Legal Research

Generative artificial intelligence has changed the look of a fabricated recording. Now, with generative adversarial networks, diffusion models and voice-cloning tools,[3] a person with a laptop and a few seconds of audio can create a video or a call that most listeners will think is real.

Deepfakes were new. Now they are used to impersonate company directors, to create sexual images of people who never gave their consent, to extort, to defame and to deceive voters.

Three characteristics distinguish deepfakes from older cybercrime. They create evidence so a victim has to prove the opposite of what looks like a recorded fact.[4] They make perpetrators harder to find, because generation, hosting and distribution can be split across services and masked behind anonymizing tools. They can be in different countries in minutes but investigation is still linked to national police, national courts and slow channels of assistance.[5] There is nothing inherently illegal about synthetic media creation. It's all about consent, purpose and consequence, so any sort of blanket ban is the wrong approach.

India is worthy of attention as one of the biggest digital societies, with so much of its users' stuff owned and hosted abroad. After Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, deepfakes impinge on Article 21 which protects privacy and dignity, and Article 19(1)(a) which protects speech including satire, subject to Article 19(2).[6]

The paper employs a single recurring example. A person in Country A uses an AI service hosted in Country B to create a fake video of an Indian public figure, which is then uploaded on a platform incorporated in Country C and viewed in India. The hypothesis is that India's technology-neutral framework provides a workable foundation but is fragmented and insufficient in respect of transnational deepfake offenses. International practice is moving toward shared expectations but has not yet crystallized into custom. Research cut-off date: 31 October 2026.

1.1. Review of Literature

[3] Ian Goodfellow et al., "Generative Adversarial Nets", 27 *Advances in Neural Information Processing Systems* 2672 (2014); Jonathan Ho, Ajay Jain and Pieter Abbeel, "Denoising Diffusion Probabilistic Models", 33 *Advances in Neural Information Processing Systems* 6840 (2020).

[4] Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", 107 *Cal. L. Rev.* 1753 (2019).

[5] The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ch. VIII.

[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

© 2026 International Journal of Advanced Legal Research

1. **Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.**

   In their study, the researchers analyze the dangers caused by deepfake technologies for people's privacy, honor, democracy, and national safety. The authors reveal the concept of 'liar's dividend' and explain how fake material can stop people's perception of the authentic videos. This research formed the basis of understanding the legal and social impact of deepfakes and created the foundation for analyzing the flaws of current legal measures in dealing with relevant cases, particularly where international aspects are involved.

2. **Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017).**

   The study is dedicated to assessing the application of already existing notions of international law regarding cyber operations, including non-intervention. This paper forms the basis of understanding the international legal effects of cyber operations originating from other countries. This paper helped to answer the question of whether the cyber actions can be considered breaches of state responsibility.

3. **United Nations Group of Governmental Experts, Report on Developments in the Field of Information and Telecommunications in the Context of International Security (2015 and 2021).**

   These documents cover ethical actions of States in cyberspace, as well as voluntary standards which aim to promote cooperation, safety and stability in cyberspace. They underline the necessity to consider the State responsibility, peaceful behaviours and cooperation in order to resolve issues connected with cyber activities. They have allowed the research to trace the evolution of international expectations about the conduct of States in cyberspace and to determine whether these practices have signified the start of the formation of customary international law. In particular, the reports were useful for find the difference between voluntary commitment and obligations which are legally binding.

1.2 Statement of Problem

© 2026 International Journal of Advanced Legal Research

The problem is one of mismatch. Deepfake-enabled crime is transnational in its commission, hosting and dissemination. Criminal law is territorial in its creation and enforcement. In the example, the creator, the generating service, the account records and the host may all be abroad and Indian law may cover the conduct but still be unenforceable.

The problem is in four parts. The first is substantive: existing offenses were drafted for cheating, forgery and obscenity, and each has elements that a given deepfake may or may not fulfil.The second is procedural: attribution is difficult, electronic evidence must be authenticated and data held abroad can only be accessed through cooperation.The third is concerning intermediaries, where the conditional immunity of intermediaries under section 79 of the Information Technology Act, 2000 has to be balanced against timely take-down and freedom of expression. The fourth is international: it is not clear whether any binding rule, as opposed to treaty or policy, requires states to stop, investigate or cooperate on cross-border synthetic media harms.

1.3 Research Questions

1. To what extent does Indian law adequately regulate the creation, dissemination and malicious use of AI-generated deepfakes?
2. How do territorial jurisdiction, attribution and access to electronic evidence affect the prosecution of cross-border deepfake offences?
3. How do the EU, US and UK regulate deepfakes, and which elements could be adapted to India?
4. What evidence exists of emerging customary international law governing state cooperation, attribution, prevention and remedies for AI-enabled cybercrime?
5. How can India reconcile effective deepfake regulation with freedom of speech, privacy, artistic expression and procedural safeguards?

1.4 Hypothesis

1. Indian law provides a variety of remedies, but fragmentation results in gaps in enforcement and victim protection.

© 2026 International Journal of Advanced Legal Research

2. Divergent national laws, jurisdictional obstacles and delays in obtaining electronic evidence are the main obstacles to cross-border enforcement.
3. International practice converges on shared expectations but does not create a customary prohibition on deepfakes.

1.6 Study Methodology

1. Doctrinal Research: This type of research is done to analyze the existing statutes, rules, regulation and decisions of the Indian judiciary in relation to deepfakes, their applicability, regulatory challenges faced, and the necessity of reforms.
2. Comparative Research: Focuses on the examination of laws related to deepfakes from the perspectives of the EU, US, and UK to draw a comparative analysis amongst the different approaches taken by these demarcated countries.
3. International Law Analysis: Analyzes whether international obligations related to deepfakes can be identified by virtue of customary international law by applying the two-pronged test of state practice and opinio juris under Article 38 (1)(b) of the ICJ statute.
4. Case Law Analysis: Reviews those cases that have dealt with AI-generated misuse of identity and other constitutional cases helping to derive the legality of the concepts of privacy, free speech, and intermediary liability.
5. Sources of Research: The research is grounded predominantly on the primary sources of law namely, legislation, treaties, judgments, and official documents with references to secondary sources of literature like books, journal papers, and academic writings.

II. Legal and Regulatory Analysis of Deepfakes: National and International Perspectives

2.1 India's Legal Framework

Privacy, dignity, and autonomy are considered to be part of Article 21 by Puttaswamy and any deepfake violates all these aspects. Article 19(1)(a) on the other hand protects parody, satire, and political criticism and Article 19(2) only allows for such restrictions that conform to its provisions.[7]

[7] *Puttaswamy*, *supra* note 4; The Constitution of India, arts. 19(1)(a), 19(2) and 21.

© 2026 International Journal of Advanced Legal Research

Shreya Singhal invalidated Section 66A and interpreted Section 79(3)(b) in such a way that it mandates the receipt of information about the occurrence by a court or an authority. Although these decisions do not deal with synthetic media directly, they set a benchmark for testing a law against the principle of proportionality.[8]

The main law is the Information Technology Act, 2000. Voice-clone and video-impersonation fraud is best described as cheating by personation using a computer resource, which is Section 66D. Section 66C is a little less comfortable. It deals with fraudulent use of another person's electronic signature, password or other unique identification feature. It should not be assumed that all facial or voice imitation comes within its ambit.[9] Section 66E only applies to images of a private area so a synthetic nude might get around it. Sections 67 and 67A deal with obscene and sexually explicit content and are the usual route against intimate deepfakes, but the content must fit their definitions.[10] Section 75 brings within the purview of the Act any offense committed outside India by any person if the act involves a computer, computer system or network located in India which gives India an arguable basis for jurisdiction in the example.[11] Paper reach isn't enforcement.

The main tool to deal with platforms is the Intermediary Rules, 2021. Intermediaries have been guided by advisories issued in December 2023 and March 2024, but these are not binding law. This changed with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which were notified on 10 February 2026 and came into force from 20 February 2026. They describe synthetically generated information as audio, visual or audio-visual content created or altered by computer means so that it appears real, and references to unlawful information in the due-diligence rules as including it. Intermediaries facilitating creation of such content shall obtain declaration from users, technical verification of such declaration and mark prominently. The amendment also reduces the takedown timelines for certain unlawful content and provides that the removal of compliant content does not result in an intermediary losing section 79(2) protection. It is India's first binding step toward the transparency model but it is implemented through

[8] *Shreya Singhal, supra* note 15; The Information Technology Act, 2000, ss. 66A and 79(3)(b).
[9] The Information Technology Act, 2000, ss. 66D and 66C.
[10] The Information Technology Act, 2000, ss. 66E, 67 and 67A.
[11] The Information Technology Act, 2000, s. 75.

© 2026 International Journal of Advanced Legal Research

intermediaries. However, a foreign platform without an Indian presence can be blocked under section 69A, but it cannot be easily forced to adhere or reveal user data.[12]

The Bharatiya Nyaya Sanhita, 2023 provides for general offenses. Sections 318 and 319 address the usual voice cloning fraud in relation to cheating and cheating by personation.[13]Where a fabricated recording is a false electronic record made or used to cause harm, sections 336 and 340, on forgery and use of a forged document or electronic record as genuine, apply. Section 353, on statements conducing to public mischief, can catch some political deepfakes but has its own ingredients and does not criminalize misinformation as such. Section 111 for organized crime is about syndicates not about a person who makes one fake.[14] None deals with synthetic media, so courts must extend concepts like document and personation that strict construction of penal law renders uncertain.

Deepfakes test evidence law in both ways : a fake can be presented as real and a real recording can be disavowed as fake . Electronic records are treated as documents under Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023 and further the certificate requirement evolved in Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.[15] A certificate is about who created a record, not whether the record shows something that happened. Forensic analysis, hash values and metadata are needed, but none is conclusive on its own. The Bharatiya Nagarik Suraksha Sanhita, 2023 has search, seizure and reciprocal-assistance powers, but they are contingent on foreign cooperation.

The Digital Personal Data Protection Act, 2023, identifies a face or voice used to power a generator as personal data, and imposes consent and fiduciary obligations on those who process it. But it's a data protection statute, not a penal law on deepfakes. It doesn't include personal data that the individual has made public, and that might describe images taken from social media.[16]

---

[12] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026; The Information Technology Act, 2000, s. 69A.

[13] The Bharatiya Nyaya Sanhita, 2023, ss. 318 and 319.

[14] The Bharatiya Nyaya Sanhita, 2023, ss. 336, 340, 353 and 111.

[15] The Bharatiya Sakshya Adhiniyam, 2023, ss. 61-63; *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

[16] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(t), 3(c)(ii), 6 and 8.

© 2026 International Journal of Advanced Legal Research

Civil relief has plugged the holes in the courts. Anil Kapoor v. Simply Life India (Delhi High Court, 2023), Amitabh Bachchan v. Rajat Nagi (Delhi High Court, 2022), Jaikishan Kakubhai Saraf v. The Peppy Store (Delhi High Court, 2024), and Arijit Singh v. Codible Ventures LLP (Bombay High Court, 2024) are some instances where injunctions protected name, image, voice and persona against AI-based imitation.[17] Later cases involving Shilpa Shetty Kundra and Sudhir Chaudhary took the approach further to intimate and political content.[18] The limits are clear. These are civil and interim orders, the claimants are mostly well known and there is nothing in them which settles foreign evidence, criminal attribution or the duties of foreign states.

2.2 Comparative Analysis

The United States has opted for targeted federal action. The TAKE IT DOWN Act, Public Law 119-12, enacted on May 19, 2025, criminalizes the knowing publication of nonconsensual intimate depictions, including qualifying digital forgeries, and requires covered platforms to remove reported material within 48 hours of a valid request and to make reasonable efforts to remove copies. The Federal Trade Commission started enforcing the platform duties in May 2026. Elsewhere, platforms continue to benefit from Section 230 of the Communications Decency Act, and broader regulation is limited by the First Amendment.[19] The Court rejected this approach in United States v. Alvarez, 567 U.S. 709, 717-19 (2012), and struck down an overbroad prohibition on virtual images in Ashcroft v. Free Speech Coalition, 535 U.S. 234, 251-56 (2002). The Eighth Circuit in Kohls v. Ellison, 166 F.4th 728 (8th Cir. 2026), declined to issue a preliminary injunction against Minnesota's election deepfake law, leaving the law's constitutionality open and rejecting the challenge on standing and laches grounds.[20]

The UK has rules around both conduct and platforms. The Online Safety Act 2023 places illegal-content duties on regulated services under Ofcom. The Data (Use and Access) Act 2025 introduced new offenses under the Sexual Offenses Act 2003 to criminalize the

[17] *Anil Kapoor v. Simply Life India*, CS (COMM) 652/2023 (Del HC); *Amitabh Bachchan v. Rajat Nagi*, CS (COMM) 819/2022 (Del HC); *Jaikishan Kakubhai Saraf v. The Peppy Store*, CS (COMM) 389/2024 (Del HC); *Arijit Singh v. Codible Ventures LLP* (Bom HC, 2024).

[18] *Shilpa Shetty Kundra v. Getoutlive.in* (Bom HC, 2025); *Sudhir Chaudhary v. Meta Platforms Inc.* (Del HC, 2025).

[19] TAKE IT DOWN Act, Pub. L. No. 119-12 (2025), ss. 2-3; 47 U.S.C. s. 230; U.S. Const. amend. I.

[20] *United States v. Alvarez*, 567 U.S. 709 (2012); *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002); *Kohls v. Ellison*, 166 F.4th 728 (8th Cir. 2026).

© 2026 International Journal of Advanced Legal Research

intentional creation or request for creation of a purported intimate image of an adult without consent. Liability therefore attaches pre-publication. R v. Sheppard [2010] EWCA Crim 65 and Monroe v. Hopkins [2017] EWHC 433 (QB) deal with online publication and reputational damage, not deepfakes.[21]

The European Union believes in prevention by transparency and systematic obligations. Under Article 50 of the AI Act, Regulation (EU) 2024/1689, providers of systems that generate synthetic audio, image, video or text must label outputs in a machine-readable way and deployers of deepfake systems must indicate that content has been artificially generated or manipulated, with modified obligations for obviously artistic or satirical works. Regulation (EU) 2022/2065 – the Digital Services Act – introduces notice-and-action and risk-assessment obligations for large platforms.[22] "The GDPR applies where faces and voices are processed and biometric rules only apply where the processing uniquely identifies a person. Google Spain (C-131/12) and Lindqvist (C-101/01) provide general privacy principles, not rulings on synthetic media.[23]

The four jurisdictions differ on the following when compared on the same parameters. India has the 2026 Intermediary Rules for dedicated legislation, but no single statute; the US has the TAKE IT DOWN Act; the UK has intimate-image offenses; and the EU has Article 50 of the AI Act. In India, intimate deepfakes are covered under the IT Act and BNS. In the US, it is a federal offense and must be removed within 48 hours. In the UK, the creation and request of such material is criminalized. In the EU, it is a matter of national criminal law. India requires labelling, the US has no general regime, the UK is sectoral and the EU requires marking and disclosure on transparency. The platform duties are in section 79 and the Intermediary Rules, section 230, the Online Safety Act and the Digital Services Act respectively. The limiting rights are Articles 19 and 21, the First Amendment, expression and privacy, and the EU Charter.[24]

[21] The Online Safety Act 2023 (UK), c. 50; The Data (Use and Access) Act 2025 (UK); The Sexual Offences Act 2003 (UK), c. 42; *R v. Sheppard*, [2010] EWCA Crim 65; *Monroe v. Hopkins*, [2017] EWHC 433 (QB).
[22] Regulation (EU) 2024/1689 (Artificial Intelligence Act), art. 50; Regulation (EU) 2022/2065 (Digital Services Act), arts. 16 and 34.
[23] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 4(14) and 9; *Google Spain SL v. AEPD*, Case C-131/12 (2014); *Bodil Lindqvist*, Case C-101/01 (2003).
[24] Charter of Fundamental Rights of the European Union, arts. 7, 8 and 11.

© 2026 International Journal of Advanced Legal Research

India already has labelling like the EU, takedown like the US and general offenses like the UK but no offense aimed at creation or commissioning, and no statutory victim procedure with safeguards against abusive complaints. The most transferable direction is combining the victim focus of the US and UK with the transparency model of the EU, with exceptions for satire and journalism.

2.3 Cross-Border Enforcement

In this example, India may exercise jurisdiction under Section 75 of the IT Act and the extraterritorial provisions of the BNS but the BNS stipulates that the Central Government gives approval for trying the crimes committed in other countries.[25] The real difficult questions arise later.

The first challenge that arises is attribution. Investigators notice accounts, IP address and files but not people. VPNs and shared devices as well as bogus personalities break the connection. A watermark or IP address can indicate the origin of the content without indicating the criminal.

The second is evidence. Original files and logs, account records sits in Countries B and C.. Content travels in hours and logs can be deleted; mutual legal assistance can take months. The third is choice of law. If Country A treats the act as speech or does not criminalize it, dual criminality can prevent both extradition and assistance.[26]

The treaty framework includes only part of India. It is not a party to the Budapest Convention on Cybercrime (2001) with the most developed procedures for expedited preservation and cross-border cooperation and a Second Additional Protocol on disclosure of electronic evidence.[27] The United Nations Convention against Cybercrime was adopted by the General Assembly on 24 December 2024 and signed by India on 25 September 2026. It includes crimes such as non-consensual sharing of intimate images and provides for cooperation, preservation and sharing of evidence, and a 24/7 contact network, with human rights safeguards. It is not yet in force, as this requires forty instruments of ratification, and

[25] The Information Technology Act, 2000, s. 75; The Bharatiya Nyaya Sanhita, 2023, s. 1(4)-(5); BNSS, *supra* note 3, s. 208.
[26] The Extradition Act, 1962 (Act 34 of 1962), s. 2(c).
[27] Convention on Cybercrime, 2001, ETS No. 185, arts. 16 and 29; Second Additional Protocol to the Convention on Cybercrime, 2022, CETS No. 224.

© 2026 International Journal of Advanced Legal Research

signature does not create its substantive obligations. Till such time India has to depend on bilateral treaties, letters rogatory and voluntary platform contact, none of which has any power to compel anyone.[28]

2.4 Customary International Law in the Making

Under Article 38(1)(b) of the ICJ Statute, custom is defined as a general practice accepted as law. The 2018 Draft Conclusions require both elements, examined separately: practice that is general and consistent and acceptance that the practice is required or permitted by law and is not merely convenient or desirable.[29] Policy convergence is driven by the enactment of an increasing number of national deepfake laws. It does not demonstrate opinio juris.

Two rules of international law in general may be applicable. Sovereignty safeguards a state's power to govern its territory. The prohibition of intervention, acknowledged as customary in Nicaragua v. United States (ICJ Reports 1986), forbids coercive interference in areas a state is free to determine such as its electoral system.[30] Such rules could pull in a foreign state's deepfake campaign to coerce an election result. It could not be a common voice clone fraud by private criminals.

The Articles on Responsibility of States for Internationally Wrongful Acts (2001) govern attribution. A State may be responsible for the conduct of State organs (Article 4), of entities exercising elements of governmental authority (Article 5), of persons acting under the direction or control of a State (Article 8) and for conduct which a State acknowledges and adopts as its own (Article 11).[31] Nicaragua implemented an effective control test. In the case of Bosnia and Herzegovina v. Serbia and Montenegro (ICJ Reports 2007) it was confirmed for Article 8, while considering the duty to prevent as an obligation of conduct, requiring a state to use the means that are reasonably available to it.[32] That is the closest judicial analogue

[28] United Nations Convention against Cybercrime, GA Res. 79/243 (24 December 2024); BNSS, *supra* note 3, ch. VIII.
[29] Statute of the International Court of Justice, *supra* note 14, art. 38(1)(b); ILC, *Draft Conclusions*, *supra* note 12, conclusions 2, 8 and 9.
[30] The Charter of the United Nations, 1945, art. 2(1); Schmitt, *supra* note 6, r. 1; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, ICJ Reports 1986, p. 14, paras 202 and 205.
[31] International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, annex (2001), arts. 4, 5, 8 and 11.
[32] *Nicaragua*, *supra* note 39, para 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, ICJ Reports 2007, p. 43, paras 400 and 430.

© 2026 International Journal of Advanced Legal Research

to due diligence." Authority: Corfu Channel Case (ICJ Reports 1949) A State must not knowingly allow its territory to be used for acts that are contrary to the rights of other States. The 2015 report of the Group of Governmental Experts recommends the same as a voluntary norm. States are divided as to whether a general cyber due-diligence rule exists. Some have accepted it as law, but others, including the United Kingdom, have refused.[33] The fact that a deepfake is produced in the territory of a state does not make the state responsible.

Human rights law offers another basis. Article 17 of the International Covenant on Civil and Political Rights protects against arbitrary or unlawful interference with privacy, and against attacks on honor and reputation; Article 19 protects expression, subject to necessary and proportionate limits; and Article 20 requires the prohibition of advocacy of hatred that incites violence.[34] These help regulate deepfakes. They also restrict it.

This basis allows evaluating six proposed norms. The UN Charter, Nicaragua and state positions show that sovereignty and non-intervention are established and apply to cyber operations, but their application to deepfakes requires state involvement and coercion. Cross-border investigation cooperation is treaty-based (Budapest Convention, UN Convention, mutual legal assistance treaties) and evolving, custom is unproven. Due diligence is contested and emerging and based on Corfu Channel, the 2015 GGE report and divided positions. The preservation and exchange of electronic evidence is a developing practice and mainly a treaty obligation. Labelling of AI content, as in the EU AI Act and India's 2026 Rules, is both a regulatory trend and aspirational as custom. There is no basis for a blanket prohibition on making deepfakes, because national laws vary and legitimate uses are everyplace.

An advocate of customary law would underline the worldwide rejection of unauthorized explicit visuals, and the ubiquity of cooperation provisions. The problem is that when it comes to these areas states operate via treaties, whose binding effect only extends to the parties, and they convey ideas about what actions are preferable instead of what should be done. Moreover, there is no clarity on how to implement those norms: there are many definitions, and the meaning of the principle of freedom of expression differs depending on the location, and there are no specific legislations regulating deepfakes in most countries.

[33] *Corfu Channel Case (United Kingdom v. Albania)*, Merits, ICJ Reports 1949, p. 4 at 22; UN Doc. A/70/174, *supra* note 7, para 13(c); Jeremy Wright, Attorney General, "Cyber and International Law in the 21st Century" (Chatham House, 23 May 2018).

[34] International Covenant on Civil and Political Rights, 1966, 999 UNTS 171, arts. 17, 19 and 20.

© 2026 International Journal of Advanced Legal Research

2.5. Observations

Four observations have been made in the process of the study:

First, Hypothesis 1 is supported, first. India boasts an abundance of law because of the several legal frameworks existing across different contexts of the IT Act, Intermediary Rules, BNS, BSA, and DPDP Act and how these different laws exist independently. It is up to the victim to decide which route to take between criminal complaint, platform grievance, civil suit, or data protection claim as no law exists for the creation of hazardous synthetic image. The 2026 amendment increases duties for platforms but does not fill the loophole.

On the other hand, Hypothesis 2 is affirmed. It is not a lack of legislation, but a lack of access to foreign people and information. While para 75 provides jurisdiction on paper, the question of whether the case can go forward is determined by an evidence, attribution, and dual criminality requirement.[35] Personality-rights injunctions demonstrate how civil courts are much faster than the criminal system but they still protect only celebrities and do not apply to foreign infrastructure.[36]

Finally, Hypothesis 3 is supported, but with a qualification. Cooperation, diligence, evidence preservation, and labelling show great advancement in practice.

However, each is treaty-based, contested or regulatory. The only laid-down rules are sovereignty and non-intervention in cases where a state is behind the operation or forces a matter which is within the domestic jurisdiction of another state. The rest is overstatement to call it custom. Fourth, there are the safeguards. Overbroad removal duties risk censoring satire and journalism, and the American litigation shows how quickly such laws are challenged.[37]

The paper therefore suggests six reforms:

- A harm-based, technology-neutral offense covering creation, commission and dissemination of non-consensual synthetic intimate imagery and fraudulent impersonation, with defences for satire, journalism and consensual work.

[35] The Information Technology Act, 2000, s. 75.
[36] *Anil Kapoor*, *supra* note 26.
[37] *Shreya Singhal*, *supra* note 15; *Kohls*, *supra* note 29.

© 2026 International Journal of Advanced Legal Research

- A legal protocol for fast removal of undesired content including a notification of a user, an avenue for an appeal, and measures against re-uploads and processes for seeking compensation for erroneous removals of content.
- Common protocols for securing original files, metadata, hashes, and logs from platforms in order to maintain chain of custody of evidence.[38]
- Technical capacities of investigative agencies and courts.
- Adoption of the UN convention and bilateral treaties for evidence sharing.[39]
- At the international level, a definition of malicious deepfakes and standards of evidence protection proposed but not yet in force.

III. Conclusion

The situation of a video that was created in one country, shared via a platform in a second, and watched in India indicate that domestic criminal law cannot argue against crimes committed through deepfake technology, as different jurisdictions are involved including the actors, infrastructure, victims, and evidence. In order for the domestic laws to be effective, they should amend and govern every stage of deepfake creation.

India has a solid base of rules due to its systems. However, in the case of the Amendments to the Intermediary Rules in 2026, it switched from regulatory guidelines to mandatory obligations.[40] Nevertheless, Indian law avails itself of being fragmented and devoid of any clarification on the aspects of the deepfake creation and commissioning stages. In addition to that, India does have to depend on outside cooperation to help in the matters of course of action.

International law can be beneficial, but it is not an easy and straightforward solution. There is no customary prohibition on deepfakes. Customary status requires proof of state practice and opinio juris, not just the assumption that a policy is sensible.[41]

India thus requires a rights-based, technology-neutral but harm-specific framework,[42] supported by forensic capacity, workable procedures for foreign evidence[43] and active

[38] Convention on Cybercrime, *supra* note 36, art. 16.
[39] GA Res. 79/243, *supra* note 37.
[40] Intermediary Rules, 2021, *supra* note 21.
[41] ILC, *Draft Conclusions*, *supra* note 12, conclusion 9; *North Sea Continental Shelf Cases*, ICJ Reports 1969, p. 3, para 77.

© 2026 International Journal of Advanced Legal Research

participation in treaty-making.[44] If it does build that it will be in better position to protect victims at home and to contribute the state practice and legal positions from which any customary rule would have to be built.

References

Statutes, Rules and Notifications

- Information Technology Act, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (notified 10 February 2026).
- Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023.
- Digital Personal Data Protection Act, 2023.
- TAKE IT DOWN Act, Pub. L. No. 119-12 (2025) (United States).
- Online Safety Act 2023; Data (Use and Access) Act 2025; Sexual Offences Act 2003 (United Kingdom).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act); Regulation (EU) 2022/2065 (Digital Services Act); Regulation (EU) 2016/679 (General Data Protection Regulation).

Cases

- Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
- Shreya Singhal v. Union of India (2015) 5 SCC 1.
- Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
- Anil Kapoor v. Simply Life India (Delhi High Court, 2023); Amitabh Bachchan v. Rajat Nagi (Delhi High Court, 2022); Jaikishan Kakubhai Saraf v. The Peppy Store (Delhi High Court, 2024); Arijit Singh v. Codible Ventures LLP (Bombay High Court, 2024).

---

[42] *Puttaswamy*, *supra* note 4; The Constitution of India, arts. 19(1)(a) and 21.
[43] BNSS, *supra* note 3, ch. VIII.
[44] GA Res. 79/243, *supra* note 37.

© 2026 International Journal of Advanced Legal Research

- United States v. Alvarez, 567 U.S. 709 (2012); Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002); Kohls v. Ellison, 166 F.4th 728 (8th Cir. 2026).
- R v. Sheppard [2010] EWCA Crim 65; Monroe v. Hopkins [2017] EWHC 433 (QB).
- Google Spain SL v. AEPD and Mario Costeja Gonzalez, Case C-131/12 (2014); Bodil Lindqvist, Case C-101/01 (2003).
- Corfu Channel Case (United Kingdom v. Albania), ICJ Reports 1949; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), ICJ Reports 1986; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), ICJ Reports 2007.

International Instruments and Materials

- Statute of the International Court of Justice, Article 38(1)(b).
- International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts (2001).
- International Law Commission, Draft Conclusions on Identification of Customary International Law (2018).
- Convention on Cybercrime (Budapest, 2001) and Second Additional Protocol (2022).
- United Nations Convention against Cybercrime, adopted by General Assembly resolution 79/243 (24 December 2024).
- International Covenant on Civil and Political Rights, Articles 17, 19 and 20.
- Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015); Open-ended Working Group final report (2021).

Secondary Sources

- Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.
- Michael N. Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017).
- Tech Law Forum, NALSAR University of Law, commentary on deepfake takedown litigation and Article 21-based relief against nudifying websites (2026).

© 2026 International Journal of Advanced Legal Research