PROTECTING IDENTITY IN THE AGE OF AI: A MEDIA LAW ANALYSIS OF DEEPFAKE SCAMS AND DIGITAL IMPERSONATION

Deepraj Bagate[1] & Harsha Rajani[2]

ABSTRACT

Artificial Intelligence's quick progress has changed the nature of media production, making "deepfakes," or synthetic highly realistic productions, possible. While such technologies have a transformative potential for entertainment, education, and innovation, their misuse has emerged to pose a serious risk for individual identity, privacy, and societal trust. Deepfake scams and digital impersonation facilitate fraud, reputational harm, and misinformation beyond legal recourse. This paper critically analyses the adequacy of media law in combating the challenges of identity manipulation by artificial intelligence, using India's media law as a reference.

Using doctrinal and comparative methodology, the paper examines constitutional safeguards, statutory provisions under Information Technology Act, 2000, and changing jurisprudence related to personality rights in India. It argues that legal responses remain piecemeal, reactionary, and poorly suited to address the scale, speed, and complexity of deepfake-enabled harms. The study also undertakes a comparative assessment of regulatory strategies in the United States, and European Union, and identifies competing considerations of free speech, data protection, and platform liability.

Through an exploration of emerging case studies, the paper highlights significant regulatory gaps, encompassing the lack of legislation specifically addressing deepfakes, difficulties in attribution and enforcement, and the limited effectiveness of intermediary liability regimes. Its argument is that laws that rely on action after damage has been caused are no longer sufficient in times when synthetic videos can cause instant and unrecoverable harm.

In response, the paper proposes a multi-layered regulatory framework that incorporates legal reform with technological and institutional interventions. This includes recognising deepfakes as a unique form of legal harm, establishing personality rights in law, enforcing transparency and due

[1] Deepraj Bagate, LL.M. (Human Rights), Symbiosis Law School, Pune
[2] Harsha Rajani, V BBA LL.B. (Hons.), Dr. Vishwanath Karad MIT-World Peace University

diligence requirements on digital platforms, and adopting technological measures like watermarking and detection technologies. The paper ultimately advocates for a balanced approach which protects individual identity and dignity without infringing freedom of expression, and encourages responsible innovation within the digital ecosystem.

Keywords: Artificial Intelligence, Deepfakes, Digital Impersonation, DPDP, Identity Protection, Intermediary Liability, Media Law, Personality Rights, Synthetic Media.

1. INTRODUCTION

AI-powered content generation has led to significant changes in the digital information ecosystem. One of the most unsettling innovations has been deepfakes, which can mimic a person's face, voice, or behaviour in highly realistic videos or audio recordings. Photographic manipulation has advanced from a simple procedure to a level of digital impersonation so sophisticated that it is capable of deceiving not only human beings but also institutional organisations and financial markets.[3] This leap in technology has somewhat destabilised the inextricable link between visual evidence and truth, thus compromise the reliability of the media as a source of authenticity.

While the deepfake technology has legitimate applications in entertainment, education, and accessibility, the misuse of this technology has led to many new forms of harm that cut across privacy, reputation, and even financial security. They range from non-consensual lewd deepfake videos targeting women to voice scams with cloned voices defrauding corporations. There is a new category of identity theft that uses deepfake technology that is different from conventional forms of identity theft, as the deepfake-enabled impersonation can be done at scale with minimal costs, with greater precision that aggravates the reach and impact of fraudulent activities.[4] These harms are not just reputational and economic but also include psychological harm and the violation of human dignity.

However, the legal system has not been able to keep up with this change in technology. The existing legal frameworks, particularly in India, tackle elements of identity misusing in disparate provisions of privacy, cheating, defamation, and obscenity. The Information Technology Act, 2000, and the Intermediary Guidelines and the Digital Media Ethics Code

[3] Chowdhary, K.R., 2020. Fundamentals of Artificial Intelligence.
[4] Divate and Puri, 2021. Relevance of Artificial Intelligence in Today's Time, at p.7.

Rules, 2021, provide certain mechanisms to deal with online harms but continue to be a reactive and ill-suited approach against the unique challenges of synthetic media.[5] Lastly, the absence of a codified regime related to personality rights makes it harder to protect the digital identity of a person. The issues of jurisdiction, attribution, and enforcement in a borderless digital environment aggravate this regulatory lag.

At the same time, the rise of deepfakes brings up complex normative questions about the balance between freedom of expression and the protection of identity. Media law, which has for long focused on regulation of speech and ensuring accountability in dissemination, is now faced with technologies that diffuse expression and deception. The role of intermediaries, particularly social media platforms, has also evolved from passive conduits to active amplifiers of content, with a corresponding reappraisal of liability regimes and due diligence requirements.[6]

Against this backdrop, this paper performs a critical analysis of the adequacy of extant legal mechanisms in dealing with deepfake scams and digital impersonation. It considers the issue within a legal context of media law and identity protection, using a comparative analysis of legal precedents from the United States, and the European Union. This paper argues that current legal approaches are ill-equipped to address the scale and complexity of AI-driven harms, necessitating a "coherent multi-layered" regulatory approach that involves legal, technological, and institutional accountability reforms.

1.1. PROBLEM STATEMENT

The rise of deepfake technology and AI-powered impersonation has created a kind of harm that our current media laws are not equipped to handle. Our traditional laws that protect identity, such as defamation law and intellectual property rights were made in a time when creating an image of someone required a lot of human effort and was easily detectable. With generative AI these assumptions no longer apply.

Today fake media can be made quickly spread across the globe and seen by millions before anyone can correct it or take legal action. The harm caused by deepfakes is many, complex and severe. For individuals it means their reputation is destroyed they suffer trauma they are

[5] Mohanty, A. and Sahu, S., 2024. India's Advance on AI Regulation. Carnegie India, November, 21, p.2024.
[6] *Supra* note 3.

financially scammed and they lose control over their own story and identity. For society the unchecked spread of AI-generated information threatens the integrity of elections erodes trust in institutions and undermines the foundation of public discussion.

At the level the lack of a clear, enforceable and rights-respecting legal framework creates a governance gap that bad actors are taking advantage of. This problem is made worse by the fact that deepfakes can be made and spread across countries. A fake video can be made using a model hosted in one country uploaded to a platform in another and seen by a victim in a third.

This makes it hard for any one country to respond effectively. It also raises questions about platform and intermediary liability.

1.2. RESEARCH OBJECTIVES

As a medium of this research paper, the authors aim to achieve the following objectives:

(a) To understand the technology behind deepfake generation and digital impersonation and how fake media is made and used so decisions can be made about the law.

(b) To look at the laws about media, including defamation, privacy and liability and see if they are good enough to deal with the problems caused by AI-generated impersonation and deepfake scams.

(c) To compare how different countries, like the United States, the European Union, India and some Asian countries are dealing with deepfakes and find out what works best and what does not.

(d) To take a look at the laws in India and see how well they protect people from harm caused by deepfakes and if the proposed changes to the laws are enough.

(e) To examine if the companies that run platforms are doing enough to stop deepfakes and if the current laws are good enough to deal with this problem.

(f) To suggest a framework for laws that takes into account the technology respects people's rights and can be used in different countries to protect people from deepfake threats.

1.3. RESEARCH QUESTIONS

This paper attempts to answer questions about how well the current media laws can deal with the deepfake crisis. The main question is whether the laws as they are now can protect people whose identities are being used made up or hurt through AI-generated media and if not what a better legal framework would look like.

From this question, more specific questions arise. The authors aim to understand how the laws about defamation work when it comes to AI-generated content, where no human made a statement on purpose and the person in the content never actually said the words that are being attributed to them. Additionally, a question is posed on the laws about privacy deal with the harm caused by identity appropriation and if the idea of "reasonable expectation of privacy" still makes sense when someone's likeness can be copied without invading their private space.

What also needs to be studied is how to balance the right to free expression with the need to protect peoples identities and how to decide what is use of synthetic media like satire or parody and what is harmful impersonation that takes away people's control over their own story. It should be known how the laws about platform liability should be changed in an environment where AI-generated content is not just hosted, but created by tools that are part of the platform. Finally, this study aims to know what a good legal framework, for regulating deepfakes would look like what principles it would be based on what institutions would be needed and what compromises would have to be made.

2. FOUNDATION OF DEEPFAKES AND DIGITAL IMPERSONATION

The rise of videos and digital copying is changing how we create media and show who we are. Unlike ways of manipulating media fake media uses artificial intelligence to make very realistic content that can copy how humans look, talk and act. This tech change has made it hard to tell what is real and what is not and that makes the general audience question if we can trust digital content.[7] Understanding how fake videos work how they are. How they can be misused is crucial to dealing with the legal and regulatory issues they bring.

2.1. ARCHITECTURE OF SYNTHETIC MEDIA

At the heart of video tech are advanced machine learning models like Generative Adversarial

[7] Reuters, *AI Deepfakes Blur Reality in 2026 US Midterm Campaigns* (Mar. 28, 2026).

Networks (GANs) and diffusion-based models. GANs work with two networks: one creates content and the other checks if its real. Through training the creator network gets better at making content that is hard to tell from data.[8]

Besides GANs other models like autoencoders and transformer-based models help with mapping, voice copying and real-time manipulation. These systems use lots of images, videos or audio recordings to learn patterns, tone and movement.[9] Once trained they can make convincing copies of people without their permission or knowledge.

It has also become easier for people to access these technologies. Open-source tools and simple apps have made it possible for individuals with tech knowledge to create fake videos. This has made it easier for more people to use the tech. It also means there's more potential, for misuse.

Importantly fake media tech is not inherently bad, the legal and ethical implications depend on how it is used and what its used for.[10] However, the same features that make it creative. Like realism, scalability and automation. Also make fake videos very dangerous when used to deceive people.

2.2. TECHNOLOGIES OF DEEPFAKE BASED IMPERSONATION

Deepfake technologies work in different ways. They can make it seem like someone's face is on another person's body. They can also make it sound like someone's voice is coming from someone. This is called voice cloning. Sometimes they use both of these things together to make it seem real.

Deepfake technologies are used for things. For example, people can use someone's voice to trick others into doing something they should not do. This can happen on the phone or in messages. It is a problem for people who want to keep their money safe.

There was a case in the UK, namely **R v. Foster**[11] wherein synthetic audio technology was used to impersonate an executive of a company, to authorise fraudulent transactions. This case

[8] Bau, D., Zhu, J.Y., Strobelt, H., Zhou, B., Tenenbaum, J.B., Freeman, W.T. and Torralba, A., 2018. GAN dissection: Visualizing and Understanding Generative Adversarial Networks.
[9] Micheal Lanham, Generating a New Reality: From Autoencoders and Adversarial Networks to Deepfakes (Apress 2021).
[10] Nie, W. and Patel, A.B., 2020, August. Towards a better understanding and regularization of GAN Training Dynamics. In Uncertainty in Artificial Intelligence (pp. 281-291). PMLR.
[11] R v. Foster 2021 UK Crown Court, EWCA Crim 952

showed that deepfake technologies can be used to trick people without using a fake face. They only used this voice to get money sent to the place where it clearly did not belong and was indeed a bad thing to do making it one of the worst possible uses of AI.

It is getting harder to tell when someone is using Deepfake technologies. The old ways of telling if something is fake do not work anymore.[12] This is because the technology is getting better and better but for the worse, it is making it harder for people to know what is real and what is not.

2.3. UNDERSTANDING THE MISUSE SPECTRUM

People use deepfake technologies for different things, it can be understood as a broad spectrum. At one end there are comical or satirical uses such as parody and entertainment and at the other end deepfake technology can also be used to trick people deceive them and cause intensive hurt to them either financial, reputational or both.[13]

One of the things people do with Deepfakes is use them to spread false information about important people. They can make it seem like someone said or did something they did not. This can be very bad for the person and for the country.

In the case of **United States v. Baugh,**[14] manipulated digital content was used as part of a broader scheme to mislead and defraud individuals online. While not exclusively a deepfake case, it demonstrates how digitally altered media can so easily be integrated into complex fraudulent ecosystems, thereby painting a picture of the actual intensity of the issue.

2.3.1. THE LINE BETWEEN ENTERTAINMENT AND EXPLOITATION

The problem with Deepfake technologies is that they can be used for both bad and good things, but are most often used for the worse. Someone can make a fun video using Deepfakes but then someone else can use the same technology to hurt people.

For example, people can use face-swapping to make videos. They can also use it to make videos that hurt people. This is a problem because it is hard to stop people from using the technology

[12] Devagiri, J.S., Paheding, S., Niyaz, Q., Yang, X. and Smith, S., 2022. Augmented Reality and Artificial Intelligence in industry: Trends, tools, and future challenges. Expert Systems with Applications, 207, p.118002.
[13] Anderljung, M., Hazell, J. and von Knebel, M., 2025. Protecting society from AI misuse, pp.3841-3857.
[14] United States v. Baugh 2022, 1:22-CR-00313

for bad things that clearly cross lines and boundaries without also stopping them from using it for good things.[15] A blanket ban would result in it being ultra vires due to the freedom of expression guaranteed under the constitution, restrictions can easily be classified as unreasonable. The actual issue lies within the recognition of the severity of the issue at hand, along with the clear legislative gap.

2.4. HARM BEYOND POLICY VIOLATIONS

The harm that Deepfakes can cause, is different for people, in different ways. Deepfakes and digital impersonation can hurt someone's feelings, their reputation and even their money. This kind of harm affects the mental health of an individual and it stays with them for a long time even if the world forgets about it, they always have a lingering fear that no matter how much the content gets deleted, it will always be available in some deep dark corner of the internet.

One of the things about Deepfakes is that they can be used to make fake videos of people without their permission and even their knowledge, this is obviously very hurtful. Even when the fake videos come to light and gain traction, the main issue is not even the deepfake video anymore, it is the struggle to prove that it is not real.

The case of **Subramaniam Swamy v. Union of India,**[16] is not a case regarding deepfake technology or digital impersonation. It was a landmark case that 'recognised the right to reputation' as a fundamental right within the scope of Article 21 of the Indian Constitution. The principles articulated by the court are directly applicable, as synthetic media can inflict reputational damage on a scale far exceeding conventional defamation.

3. THE FRAGMENTED INDIAN LEGAL FRAMEWORK

The Indian law about deepfake scams and digital impersonation currently exists in bits and pieces, it uses a mix of rules from the constitution, laws and court decisions that were not made to deal with problems caused by intelligence. These laws together give some protection against people misusing identities.[17] They are mostly reactive and do not fully address the complexities of fake media. Because there is no law for deepfakes there are gaps in regulation

[15] Lundberg, E. and Mozelius, P., 2025. The Potential Effects of Deepfakes on Society, 40(4), pp.2159-2170.
[16] Subramaniam Swamy v. Union of India, AIR 2016 SC 2728
[17] Kalyanakrishnan, S., Panicker, R.A., Natarajan, S. and Rao, S., 2018, December. Opportunities and Challenges for Artificial Intelligence in India. In Proceedings of the 2018 AAAI/ACM conference on AI, Ethics, and Society (pp. 164-170).

especially when it comes to saying who is responsible holding people accountable and stopping these problems before they happen. This part of the discussion looks at the legal system and points out its limitations in dealing with new technological threats.

3.1. THE CONSTITUTION OF INDIA, 1950

The Constitution of India is the basis for protecting rights like privacy, dignity and freedom of expression. However, when it comes to deepfakes the Constitution does not directly address these issues. We have to rely on the judiciary to interpret the laws.

3.1.1. ARTICLE 21[18]

Article 21 of the Constitution provides that everyone has the right to life and personal freedom. Judges have broadly interpreted this to include the right to privacy, dignity and autonomy. In one court case **Justice K.S. Puttaswamy v. Union of India,**[19] the Supreme Court stated that people have the right to control their personal information, which helps protect individuals from unauthorised use of their data and likeness.

Deepfakes are those that use someone's face or voice without permission directly affect this right. Making and sharing content without consent violates a person's right to control their own information and dignity. In cases where deepfakes involve consensual explicit content the harm goes beyond privacy and affects a person's body and mental well-being.

However, Article 21 mostly helps after the harm has already been done and it does not give a way to prevent these problems. It also does not directly tell companies like digital platforms what they must do. This limits how well Article 21 can deal with the widespread nature of deepfakes.

3.1.2. ARTICLE 19(1)(a)[20]

Article 19(1)(a) of the Constitution says that people have the right to freedom of speech and expression which includes creating and sharing content. Deepfake technology can be used for satire, parody or art and in these cases, it is protected by this right.

[18] INDIA CONST. art. 19(1).
[19] Justice K.S. Puttaswamy v. Union of India AIR 2017 SC 4161
[20] INDIA CONST. art. 19(1)(a).

This right is not absolute and can be limited by reasonable restrictions[21], such as laws against defamation, public order and decency. Deepfakes that are meant to deceive, cheat or harm someone's reputation can be restricted under these laws.

The main challenge is to tell the difference between expression and harmful impersonation. If the rules are too broad, they might stop people from speaking but if they are too narrow, they might allow abuse. Because there are no laws to make this distinction it is confusing for both content creators and regulators which makes it hard to enforce the laws. Deepfakes and the laws about deepfakes are issues that need to be addressed. Deepfakes and their impact, on society are topics that require careful consideration of deepfakes and their effects.

3.2. THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 is the law that deals with cybercrimes in India. It has some rules that can be used for deepfake-related misconduct. Considering the act is more than a quarter of a decade old, these rules were not made with AI-generated content in mind. This makes it hard to understand and enforce them.

3.2.1. SECTIONS 66C & 66D[22]

Section 66C makes it a crime to steal someone's identity like using their signature, password or unique ID, whereas, Section 66D is about cheating by pretending to be someone using computers.

These rules are important for deepfake scams where someone pretends to be someone to get money, like voice-cloned CEO scams or phishing schemes. Using media to trick people can be seen as "digital impersonation."

A big problem is that these rules are only about traditional IDs, like passwords or digital signatures. Deepfakes use visual replication so they do not always fit these definitions. This makes it unclear how to apply these rules especially when no direct financial fraud happens but it is crystal clear that someone's reputation is getting hurt and thereby tarnished.

[21] INDIA CONST. art. 19(2).
[22] Information Technology Act, 2000, § 66C, § 66D, No. 21, Acts of Parliament, 2000 (India).

3.2.2. SECTION 67[23]

Section 67 of the IT Act makes it a crime to publish or send material electronically. This rule is often used in cases of non-consensual deepfake pornography, which mostly targets women.

While Section 67 helps punish behavior it only deals with obscenity-based harm. It doesn't address forms of deepfake misuse like political misinformation or financial fraud. Also relying on obscenity standards can be subjective which may make it hard to enforce consistently.

3.2.3. SECTION 79[24]

Section 79 says that intermediaries, like media platforms are not liable for content from third parties if they follow certain rules and do not know about unlawful activity.

In the case of deepfakes this rule affects how platforms are held accountable. Social media platforms often spread media but their liability is limited. The "notice-and-takedown" framework under Section 79 is reactive meaning victims have to report content before anything is done. Given how fast deepfakes can spread this approach is often not enough to prevent harm. Also, the standard of "knowledge" has been interpreted by courts, which further limits proactive content moderation.

3.2.4. INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE RULES, 2021

The Intermediary Guidelines and Digital Media Ethics Code Rules 2021 were introduced to make digital platforms more accountable. These rules require intermediaries to remove content within certain timelines and establish grievance redressal mechanisms.

Importantly the rules require identifying the "originator" of information in certain cases which can help trace the source of deepfake content.[25] However, the rules have been criticised for being too burdensome and not specifically addressing AI-related harms. They do not explicitly address deepfakes or synthetic media. Do they require proactive detection mechanisms. Moreover concerns, about privacy and encryption make it hard to implement traceability

[23] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[24] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
[25] Manazir, S., 2025. Personal Impersonation and Role of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025. Available at SSRN 5663270.

requirements.

3.3. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act of 2023 also known as the DPDP Act is a step forward for India in terms of protecting peoples personal information online. This law is important because it says that companies need to get peoples permission before they can use their data. The Digital Personal Data Protection Act of 2023 is relevant when we talk about deepfakes which are fake videos or audio recordings that use real peoples faces or voices without their permission.

Lately there have been some policies that recognise the dangers of deepfakes. For example some people want to create a definition for "media" or "deepfake content".[26] However, these policies are still new. Do not have the full support of the law, which makes it hard to enforce them. The Digital Personal Data Protection Act of 2023 is important. It has some limitations. It only applies to personal data, which means it does not cover situations where deepfakes are made without using any identifiable information.

The Digital Personal Data Protection Act of 2023 also focuses on getting peoples permission before using their data. This does not work well when it comes to deepfakes that are made with bad intentions.[27] The law mostly puts the responsibility on companies that handle peoples data and gives them fines if they do not follow the rules of providing immediate help to the victims. There are also some exceptions in the law that might create protection for different groups of people. For instance the law might protect people who work for the government. It might not protect people who are not in those positions. This means that some people might be left vulnerable to deepfakes in spaces that are not regulated.

3.4. CRIMINAL LAW PERSPECTIVE

Deepfake scams and digital impersonation can be dealt with under the Bharatiya Nyaya Sanhita of 2023 which is a law that says what is considered a crime in India. The Bharatiya Nyaya Sanhita of 2023 includes crimes such as cheating, personation, defamation and forgery. If

[26] Press Information Bureau, Govt. of India, India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes; Government to Parliament (Aug. 8, 2025)
[27] Press Information Bureau, Govt. of India, DPDP Rules wrt. Impact of Artificial Intelligence on Individual Rights (Nov. 17, 2025).

someone uses deepfakes to cheat people or harm their reputation they can be charged with these crimes. For example, if someone uses voice cloning to scam people they can be charged with cheating. If a deepfake harms someone's reputation it amounts to defamation. The Bharatiya Nyaya Sanhita of 2023 also has laws, against content, which can be used to charge people who make deepfakes that target women.[28]

However, it is hard to apply these laws to deepfake cases because they involve technology and many different people. It is difficult to figure out who is responsible and prove that they did it on purpose. The Bharatiya Nyaya Sanhita of 2023 is mostly focused on punishing people after they have committed a crime than preventing the crime from happening in the first place.

The concepts of "personation" and "forgery" were created a time ago before the internet existed and they do not fully capture the complexity of deepfakes.[29] Therefore while the Bharatiya Nyaya Sanhita of 2023 provides some rules for dealing with deepfakes it is not enough to fully address the problems they cause. We need to create laws that are specifically designed to deal with deepfakes and the harm they can cause.

4. CROSS-JURISDICTIONAL COMPARISON

The regulation of deepfakes and digital impersonation varies significantly across countries. This is because different countries prioritise things, such as free speech, data protection and platform accountability. A comparative analysis is provided below.

4.1. THE UNITED STATES

In the US the approach to regulating deepfakes and impersonation is focused on speech and is not uniform across the country. The right of publicity allows individuals to control how their name, image or likeness is used for purposes. However, this right is handled at the state level resulting in protection.

The First Amendment limits the scope of regulation particularly when deepfakes are considered content, such as satire or parody. This creates a tension between protecting individuals from

[28] Press Information Bureau, Govt. of India, India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes; Government to Parliament (Aug. 8, 2025)
[29] Begum, A.D., AYYUB, M.S. and KIRTHY, M.K., 2016. Journal of Recent Research and Applied Studies.

harm and preserving freedom of expression.[30]

A key case in this context is **Haelan Laboratories, Inc. v. Topps Chewing Gum Inc.,**[31] where the court recognised the "right of publicity" as a legal interest. This decision acknowledged an individual's interest in their identity laying the groundwork for subsequent claims involving unauthorised use of likeness.

In years some states like California and Texas have introduced laws specifically targeting deepfakes especially those related to election interference and non-consensual explicit content.[32]

However, the lack of a federal framework means that enforcement is inconsistent and often dependent on the nature of harm and jurisdiction involved. The US framework provides protection for speech but struggles to address the harms posed by deepfakes uniformly.

4.2. THE EUROPEAN UNION

In contrast the European Union takes a rights-based and regulatory approach, with an emphasis on data protection and individual autonomy. The General Data Protection Regulation (GDPR) is the cornerstone of this framework governing the processing of data.

Deepfakes often involve the manipulation of data, such as facial images and voice which fall within the scope of "personal data" and in many cases "special category data" under the GDPR.

Unauthorised creation or dissemination of content can constitute a violation of principles such as lawfulness, fairness, transparency and purpose limitation.[33]

A key case illustrating the breadth of data protection under EU law is **Google Spain SL v. Agencia Española de Protección de Datos.**[34] In this case the Court of Justice of the European Union recognised the "right to be forgotten," enabling individuals to request the removal of data from search engine results. The EU has taken steps through instruments such as the Digital

[30] Shanor, A., 2018. First Amendment Coverage. NYUL Rev., 93, p.318.
[31] Haelan Laboratories, Inc. v. Topps Chewing Gum Inc. 202 F.2d 866
[32] Rodriguez, X., 2023. Artificial intelligence (AI) and the practice of law in Texas. S. Tex. L. Rev., 63, p.1.
[33] Grundstrom, C., Väyrynen, K., Iivari, N. and Isomursu, M., 2019, January. Making sense of the general data protection regulation: four categories of personal data access challenges. In Proceedings of the 52nd Hawaii International Conference on System Sciences, January 8-11 2019, Grand Wailea, Maui. IEEE Computer Society.
[34] Google Spain SL v. Agencia Española de Protección de Datos 2024, C-131/12

Services Act (DSA) and the proposed AI Act, which adopt a risk-based approach to regulating AI systems, including transparency obligations for synthetic content.[35]

Compared to the US the EU framework is more comprehensive and preventive. Nevertheless, its emphasis, on consent, accountability and platform responsibility offers lessons.

5. MAJOR INDIAN DEEPFAKE AND DIGITAL IMPERSONATION CASES

Technology is inevitably a double-edged sword, with its enhancements comes heaps of misuse and exploitation. It is no surprise that India has witnessed a rapid rise in deepfake-enabled frauds and digital impersonation, reflecting the growing accessibility of synthetic media technologies. These incidents illustrate the transition from isolated cyber offences to organised, technology-driven deception, although these are four independent incidents, the root cause remains the same, the target remains the same, money, emotions, reputation, mental agony and suffering, often exploiting trust, urgency, and emotional vulnerability. While judicial responses remain limited, emerging cases highlight both the scale of harm and the inadequacy of existing legal frameworks in addressing AI-enabled impersonation.

5.1. MICROSOFT PHISHING SCAM (2026)[36]

The 2026 "Microsoft Phishing Scam" represents an evolution of digital impersonation, combining elements of traditional phishing with AI-enabled deception. In this scam, perpetrators impersonated representatives of Microsoft, contacting victims through emails, calls, and pop-up alerts claiming that their systems had been compromised.

There were no fake logos, no legally existing persons, no authorised representatives. The scam was simply that meeting links were being sent to higher level employees at different locations of Microsoft's offices through an email id that looked exceptionally similar to the real one. In these email ids, the word Microsoft was spelt using a lower-case 'n' and a lower-case 'r' to replace the letter 'm' in Microsoft. Through these links, transactions that weren't even supposed to exist were being set up through deepfake video technology, scammers were posing as top management and key managerial persons through voice and face cloning mediums.

[35] Pathak, M., 2024. Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. European Data Protection Law Review (EDPL), 10(1).
[36] Correya, R.D. and Sagathia, T.A., 2026. Microsoft 365 Phishing case. In Information Technology Security and Risk Management (pp. 107-117). CRC Press.

What distinguished this scam from earlier phishing attempts was the use of AI-generated voice modulation and scripted interaction patterns, which made the impersonation highly convincing. Victims were often guided through step-by-step instructions to "secure" their systems, during which they unknowingly granted remote access or transferred funds under the pretext of resolving fabricated security threats.

The scam exploited two critical vulnerabilities: institutional trust and technological illiteracy. By invoking a globally recognised entity such as Microsoft, perpetrators leveraged perceived legitimacy, while the use of technical jargon created a sense of urgency and dependency. In several instances, victims reported hearing convincing human-like voices, suggesting the use of voice synthesis tools to enhance credibility.

From a legal perspective, such conduct falls within offences of cheating and personation under cyber and criminal law frameworks. However, the scale and sophistication of the scam expose significant enforcement challenges. The perpetrators often operated across jurisdictions, used anonymised communication channels, and frequently altered their digital footprints, making attribution difficult.

5.2. DIGITAL ARREST SCAMS (2025-2026)[37]

One of the most alarming developments in India's cybercrime landscape is the emergence of so-called "digital arrest scams," reported widely between 2025 and 2026. These scams involve perpetrators impersonating law enforcement officials who contact victims via video calls often on platforms like WhatsApp claiming that a close family member has been detained in connection with serious criminal activity.

The way in which they operate is both psychologically manipulative and technologically sophisticated. Victims are told that their child, spouse, or relative has been implicated in offences such as drug trafficking or financial fraud. To heighten credibility, the perpetrators conduct video calls where individuals dressed as police officers appear in what resembles an official setting. In many cases, victims are made to hear the voice of their alleged family member AI-generated to mimic tone and distress pleading for help.

[37] Robert, S.J., Singh, V., Pandey, R.P. and Bhuyan, B., 2026. Digital Arrest in the Cyber Age: A Psychological Perspective on fear, Authority, and Consciousness. Frontiers in Psychology, 17, p.1726740.

The scammers then demand an immediate transfer of money, threatening severe consequences such as custodial violence, prolonged detention, or failure to produce the individual before a magistrate if payment is not made. The urgency and emotional distress induced by these threats often override rational judgment, leading victims to comply without verification.[38]

A variation of this scam involves impersonation of family members or trusted acquaintances, where the perpetrator directly requests urgent financial assistance. The use of AI-generated voices significantly enhances the credibility of such requests.

Legally, these acts constitute offences of cheating, criminal intimidation, and impersonation, potentially attracting liability under both cyber and penal laws. However, the effectiveness of legal recourse is limited by several factors. The use of encrypted communication platforms, anonymised accounts, and cross-border networks complicates investigation and prosecution. Additionally, scams are executed speedily and leave little scope for preventive intervention.[39]

Beyond financial loss, these scams have profound psychological consequences, including trauma, guilt, and loss of trust in communication systems. As such, they underscore the urgent need for integrated responses combining legal reform, platform accountability, and public awareness to effectively counter emerging forms of deepfake-enabled fraud.

5.3. ARIJIT SINGH V. CODIBLE VENTURES LLP (2024)[40]

This case represents a significant development in the recognition of personality rights in the context of digital impersonation. The dispute arose from the unauthorised use of the singer's name, voice, and likeness in connection with digital content and commercial activities, raising concerns about identity misappropriation in the age of AI.

The plaintiff, a well-known public figure, argued that the defendants had exploited his personality without consent, thereby violating his right to publicity and commercial identity. This case is is highly relevant in illustrating how digital technologies enable the unauthorised replication of identity, blurring the line between endorsement and impersonation.

The court recognised the importance of protecting an individual's personality, particularly in

[38] RBI Notification: Digital Frauds – Classification and Reporting RBI/2025-26
[39] *Ibid.*
[40] Arijit Singh v. Codible Ventures LLP, 2024, SCC OnLine Bom 2445

the case of celebrities whose identity holds significant commercial value. It emphasised that unauthorised use of such identity elements could result in both economic harm and reputational dilution, thereby warranting legal protection.

This case highlights a key gap in Indian law, the absence of a codified personality rights regime. Protection currently relies on a combination of constitutional principles, tort law, and judicial interpretation, leading to uncertainty and inconsistency. This gap lays out the foundation for another identified gap in the context of deepfakes, where identity replication can be automated and scaled, this gap becomes even more pronounced.

Importantly, the case underscores the need to move beyond traditional notions of identity misuse toward a framework that recognises digital likeness as a protected legal interest. It also reinforces the argument that deepfake harms are not limited to fraud or obscenity but extend to commercial exploitation and unauthorised association.

5.4. KARTI P. CHIDAMBARAM V. UNION OF INDIA (2021)[41]

This case is directly centred on deepfakes, it provides important insights into the intersection of digital content, reputation, and political discourse. The matter involved allegations relating to the circulation and use of digital material in a manner that raised concerns about misinformation and reputational harm.

The petitioner being a well-known politician, campaigns, actively engages in public speaking, has an established public presence and as a politician, her prized possession would be her reputation. The perpetrator in this case, circulated a deepfake generated video online, wherein it is depicted that she is involved in illegal activities including defrauding the public and being engaged in all sorts of extortion and money laundering.

In the context of deepfakes, this case is significant for understanding how digital manipulation can influence public perception, particularly in politically sensitive environments. The increasing use of synthetic media to create fabricated statements or visuals of public figures poses a direct threat to democratic processes, including elections and public debate.[42]

The case also reflects the judiciary's cautious approach in balancing free speech with

[41] Karti Chidambaram v. Union of India (2020) SCC OnLine Mad 605
[42] Nadia Naffi, *Deepfakes and the Crisis of Knowing*, UNESCO (Oct. 1, 2025).

reputational protection, especially where political actors are involved. Courts have traditionally afforded a higher threshold for restricting speech in political contexts, recognizing the importance of open discourse. However, deepfakes complicate this balance by introducing deliberate falsification disguised as authentic expression.

6. REGULATORY GAPS AND STRUCTURAL CHALLENGES

The law in India does not do a job of dealing with deepfakes and digital impersonation. This is because there are gaps in the system. These gaps are not just because the laws are not good enough but because digital technology is very hard to control. It can be used from anywhere. It is hard to say who is doing what.

6.1. ABSENCE OF DEEPFAKE-SPECIFIC LEGISLATION

One problem is that India does not have any laws that are just for deepfakes. The laws we have now like the Information Technology Act, 2000 and other criminal laws only deal with parts of the problem. They talk about things like cheating, obscenity or defamation. They do not really understand what deepfakes are.[43]

This means that the law is not clear and it is hard to say what is allowed and what is not. Deepfakes are not just someone using someone Information they are completely made up. This makes it hard to say who is responsible and what they did wrong. It is like trying to use rules for something that is completely new.

6.2. IDENTIFICATION OF THE PERPETRATOR

It is very hard to find the person who makes and shares deepfakes. They can use names, special servers and secret platforms to hide who they are. This makes it very hard for the police to catch them. VPNs can also be used to fabricate and falsify IP addresses. Anyone sitting on one side of the world can make it look like they are in a completely different location.[44]

Unlike crimes deepfakes can involve many people who are in different places and use different technology. This makes it hard to say who did what and why. It is like trying to solve a puzzle

[43] Vig, S., 2024. Regulating Deepfakes. Journal of Strategic Security, 17(3), pp.70-93.
[44] Prayudi, Y. and Ashari, A., 2015. A Study on Secure Communication regarding Virtual Private Networks. Int. J. Sci. Eng. Res, 6(1), pp.1036-1043.

with missing pieces.

6.3. JURISDICTIONAL COMPLEXITIES IN CROSS-BORDER DIGITAL CRIMES

Deepfakes can be made in one country shared in another and seen around the world. This makes it hard to say which laws should be used and who should enforce them.

Indias laws are mostly based on what happens in the country. Digital crimes can happen anywhere.[45] This means that it is hard to work with countries to stop these crimes. It is like trying to catch a guy who is running away.

6.4. FREE SPEECH CONCERNS

We also need to think about freedom of speech when we talk about deepfakes. Some people use media to make jokes or to talk about politics or to make art. We do not want to stop people from expressing themselves. At the same time, we do not want perpetrators to use this freedom to hurt others. We need to find a way to say what is okay. What is not. If we do not have rules, it can be confusing for everyone. It is like trying to find a balance, between being free and being safe.[46]

7. THE POLITICS OF INTERMEDIARIES AND PLATFORM GOVERNANCE

The rise of deepfakes and digital impersonation clarifies that social media platforms play a role in shaping the way we get our information. These platforms are active gatekeepers that decide what content to show us what to amplify and sometimes even make money from what we post. This has implications for who is accountable especially when it comes to synthetic media, where platforms are often the main way this content gets out.[47]

Laws like the safe harbour regime say that platforms are not responsible for what other people post long as they follow some basic rules. The way these platforms are designed, with algorithms that prioritise engagement and virality means they are not really neutral. Deepfake

[45] Oladele, O.K., 2025. Secure Distributed AI Systems for Cross-Border Financial Crime Prevention.
[46] Bearman, M., Ryan, J. and Ajjawi, R., 2023. Restrictions of Artificial Intelligence in Higher Education: A Critical Literature Review. Higher Education, 86(2), pp.369-385.
[47] Press Information Bureau, Govt. of India, Advisory on Countering Misinformation and Deepfakes under IT Rules, 2021 (Mar. 15, 2024).

content is often easy to share so it can spread quickly through recommendation systems.

This raises concerns about whether platforms are inadvertently helping to spread harmful content. The problem is made worse by how hard it's to moderate this content. Detecting deepfakes requires technology and even then, it can be hard to tell the difference between malicious impersonation and legitimate expression like satire or parody.[48] As a result, platforms often go back and forth between not doing enough to stop content and doing too much which can mean suppressing lawful speech.

The way we govern these platforms is also deeply political with governments, private companies and users all having competing interests. Governments want to impose rules on platforms including making them track who posts what and take down harmful content quickly. While these measures aim to stop misuse, they also raise concerns about privacy and state overreach. On the hand platforms often resist regulation saying it is too hard to comply with and could stifle user expression.

This dynamic has led to a debate about how to regulate these platforms. Some say they should self-regulate, with community guidelines and voluntary disclosure practices. This approach often fails to address systemic risks. Others say the state should regulate them. This risks being too intrusive and could be used to control dissent. A co-regulatory model, where platforms operate under enforceable standards but still have flexibility might be a better approach but it requires strong oversight and transparency.

When it comes to deepfakes it is clear that our current system is not working. The way we deal with content now is reactive and it is not suited to content that can spread quickly. We need to move towards a proactive approach with detection technologies, transparency in algorithmic processes and accountability for when platforms amplify harmful content.

Any effective response to deepfake harms must reimagine platform governance in a way that balances innovation, free expression and the protection of identity. Social media platforms must be held accountable, for deepfakes and digital impersonation. We must find a way to regulate them that works for everyone. Deepfakes and digital impersonation are a problem and

[48] Chatterjee, S., 2020. AI strategy of India: policy framework, adoption challenges and actions for government. Transforming Government: People, Process and Policy, 14(5), pp.757-775.

social media platforms are a big part of the solution.

8. REFORMS AND RECOMMENDATIONS

The regulatory challenges posed by deepfakes and digital impersonation require a shift from reactive responses to a coherent forward-looking legal framework. Given the limitations identified in the existing regime reforms must combine legal precision, technological integration and institutional accountability while carefully balancing competing constitutional values.

8.1. ENACTING A DEDICATED DEEPFAKE REGULATION IN INDIA[49]

A primary reform imperative is the enactment of deepfake- legislation that recognises synthetic media as a distinct category of legal harm. Such a framework should clearly define deepfakes. Differentiate between malicious impersonation, non-consensual use and legitimate expression such as satire or parody.

The law must provide for both liability and civil remedies including injunctive relief, damages and expedited takedown mechanisms. Importantly it should incorporate a harm-based approach targeting intent to deceive, defraud or harm reputation than broadly criminalising all deepfakes. This would ensure clarity while avoiding overbreadth.

8.2. RECALIBERATING INTERMEDIARY LIABILITY FRAMEWORK[50]

The existing safe harbour regime under Section 79 of the Information Technology Act, 2000 requires recalibration to reflect the role of intermediaries in "deepfake" content dissemination. A reactive "notice-and-takedown" model is insufficient in the context of rapidly spreading deepfakes.

Reform should move toward a safe harbour, where immunity is linked to demonstrable compliance with proactive due diligence obligations, such as deploying deepfake detection tools, flagging suspicious content and limiting algorithmic amplification of identified harms.

[49] Srivastava, S.K., 2018. Artificial Intelligence: Way Forward for India. JISTEM-Journal of Information Systems and Technology Management, p.15.
[50] Kalyanakrishnan, S., Panicker, R.A., Natarajan, S. and Rao, S., 2018, December. Opportunities and Challenges for Artificial Intelligence in India. In Proceedings of the 2018 AAAI/ACM conference on AI, Ethics, and Society (pp. 164-170).

At the time safeguards must ensure that intermediaries are not compelled into over-censorship preserving the balance with free expression.

8.3. TRANSPARENCY AND DISCLOSURE OBLIGATIONS[51]

A critical regulatory intervention lies in mandating transparency in deepfake content creation and dissemination. Platforms and AI developers should be required to implement watermarking or labelling mechanisms for AI-generated deepfake content enabling users to distinguish between synthetic media.

Additionally, intermediaries should be obligated to disclose content moderation practices, algorithmic criteria and risk assessments in relation to high-risk deepfake content. Such transparency enhances accountability. Allows for independent scrutiny reducing the opacity that currently characterises platform governance.

8.4. BALANCING REGULATION WITH FREEDOM OF EXPRESSION[52]

Any regulatory framework must carefully navigate the tension between identity protection and freedom of speech. Overbroad restrictions risk chilling forms of expression including satire, parody, artistic works and political commentary involving deepfakes.

Therefore, legal reforms should incorporate exceptions and safeguards ensuring that only deepfake content involving intent to mislead, harm or exploit is subject to regulation. Judicial oversight and tailored restrictions are essential to prevent misuse of deepfake laws as tools for censorship or suppression of dissent.

8.5. PROMOTING DIGITAL LITERACY AND PUBLIC AWARENESS[53]

Legal and technological measures alone are insufficient, without a user base. There is a pressing need to promote literacy and public awareness regarding the existence, risks and detection of deepfakes.

State institutions, educational bodies and digital platforms should collaborate to develop

[51] *Ibid.*
[52] Vempati, S.S., 2016. India and the Artificial Intelligence Revolution (Vol. 1). Washington, DC: Carnegie Endowment for International Peace.
[53] *Supra* note 49.

awareness campaigns, verification tools and user education programs on deepfakes. Empowering individuals to evaluate digital content serves as a preventive safeguard reducing susceptibility to deception and limiting the societal impact of "deepfake-driven misinformation."

9. CONCLUSION

The rise of deepfakes and AI-driven digital impersonation is changing the way we think about identity, evidence and trust in the world. What we used to consider proof is now easy to manipulate in ways that were not possible before. This change is causing problems for people's rights like privacy, dignity and reputation. It is also affecting the way our society works including how we get information keep our money safe and have discussions.

This paper shows that the laws we have in India are not really helping to deal with the problems caused by deepfakes. The laws we have now are not working well together and are not really thinking about the future. We have some protection under the Constitution like Articles 21 and 19(1)(a). Some laws like the Information Technology Act, 2000. These laws are not enough to deal with the problems caused by deepfakes. We do not have laws that are specifically made to deal with deepfakes. This is a big gap in our laws.

When we look at what other countries like the United States and the European Union are doing we see that they are trying different things. Some are focusing on protecting speech while others are looking at how to regulate data. They all know that they need to change their laws to deal with the new risks that come with new technology. This shows us that we need to think about how to change our laws in a way that makes sense for our country.

The problem of regulating deepfakes is not about technology or law. It is about finding a balance between letting people be creative and holding them accountable for what they do. It is about protecting people's right to express themselves while also protecting their identity. This paper suggests that we need to have a plan that includes making laws making companies that help spread information more responsible and making sure people know what is going on.

Now that we cannot always trust what we see our laws need to change to help us know what is real and what is not. Protecting people's identity in a world where computers can make things is not just about stopping bad things from happening. It is about keeping people safe and

making sure they can be themselves, in a world that is becoming more and more fake. Deepfakes are a problem and we need to deal with deepfakes in a way that works for everyone.