Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

AI-Generated Likeness and The Law: Protecting Personality Rights in The Age of Deepfakes and Social Media Exploitation

Anmol Arora[1]* , Dr Superna Venaik[2], Deigo Gomez Baya[3]
[1]* Research Scholar, School of Law, Manav Rachna University, Faridabad, Haryana, India.
[2]Associate Professor, School of Law, Manav Rachna University, Faridabad, Haryana, India.
[3]Associate Professor, Department of Social, Developmental and Educational Psychology, University of Huelva: Huelva, Andalucía, ES
*Corresponding Author: aroraa1208@gmail.com

ABSTRACT

The proliferation of artificial intelligence (AI) technologies—particularly deepfakes—has given rise to complex legal and ethical challenges concerning the unauthorised use of an individual's likeness. With AI-generated content becoming increasingly indistinguishable from reality, questions surrounding the protection of personality rights have taken centre stage. Celebrities, politicians, and even private individuals are now at risk of having their images, voices, and behaviours manipulated and disseminated without consent. The law, however, has not evolved at the same pace as technology, resulting in gaps in legal protection across jurisdictions. This paper explores the legal dimensions of AI-generated likenesses, focusing on personality rights, privacy laws, intellectual property, and the ethical implications of digital exploitation on social media platforms. By examining case law, statutory frameworks, and comparative legal approaches, the paper underscores the urgent need for updated legislation and proactive regulation. Furthermore, it explores the implications for content creators, platforms, and victims and outlines proposed strategies for ensuring accountability and protecting individual dignity in the digital age.

Keywords: *Deepfakes, Personality Rights, AI-generated Content, Digital Privacy, Social Media Exploitation*

INTRODUCTION

In the modern digital landscape, artificial intelligence (AI) is no longer a futuristic concept but a deeply embedded facet of our daily lives. From virtual assistants to predictive analytics and personalised advertising, AI continues to reshape the way we interact with technology. One of the most controversial advancements within this domain is the emergence of AI-generated likeness, particularly in the form of deepfakes—highly realistic synthetic media that manipulate or fabricate audio-visual content to depict individuals saying or doing things they never actually said or did. Initially perceived as novel or humorous content, deepfakes have now evolved into powerful tools that blur the lines between reality and fabrication, raising critical legal, ethical, and societal concerns.

At the heart of this discussion lies the concept of *personality rights*, a set of legal principles that safeguard an individual's identity from unauthorized commercial or public exploitation. Personality rights typically encompass the right to control the use of one's name, image, voice, and other unique attributes. Traditionally, these rights were invoked in situations involving celebrities or public figures who wished to prevent the unauthorized use of their persona for advertising or merchandising. However, with the democratization of AI tools and the explosion of social media usage, these rights have become relevant to virtually anyone with an online presence.

The digital age has introduced a paradox: while individuals now have unprecedented access to platforms that allow them to express, share, and promote themselves, the same platforms have become breeding grounds for exploitation. Deepfakes, in particular, pose a threat not only to the privacy and dignity of individuals but also to the integrity of information and the trustworthiness of digital content. Cases involving non-consensual pornography, political misinformation, financial scams, and reputational sabotage have highlighted the dangers of synthetic media in the hands of malicious actors. Furthermore, the victims of such exploitation often find themselves with limited

recourse, as legal systems struggle to keep pace with technological innovation.

What complicates the issue further is the lack of a coherent global legal framework to address the misuse of AI-generated likeness. Jurisdictions around the world vary in their recognition and enforcement of personality rights. For example, the United States relies heavily on state-level right of publicity laws, which are inconsistently applied and often limited in scope. Some states provide strong protection, while others offer minimal or no statutory support. On the other hand, the European Union, through the General Data Protection Regulation (GDPR), emphasizes the individual's right to control personal data, which may include biometric data and identifiable features used in AI-generated content. However, even these protections were not designed with deepfakes in mind and often fall short when tested against the nuances of synthetic media.

Social media platforms play a pivotal role in this ecosystem. They act not only as distributors of deepfake content but also as facilitators of viral dissemination. The structure of these platforms—designed to prioritize engagement and shareability—makes them particularly vulnerable to the spread of false or harmful AI-generated content. While some platforms have taken steps to address the issue by introducing content labeling, takedown mechanisms, and AI detection tools, enforcement remains patchy and reactive rather than preventative. Moreover, platform policies often lack transparency and consistency, leaving users uncertain about their rights and options when targeted by synthetic content.

The economic incentives behind the proliferation of deepfakes and AI-generated likeness cannot be ignored. As generative AI becomes more accessible, content creators and marketers are increasingly using synthetic personas and voice clones for entertainment, advertising, and influencer campaigns. While this creates new business opportunities and creative possibilities, it also raises concerns about consent, attribution, and compensation. Can an AI-generated version of a deceased celebrity endorse a product without violating ethical norms? Can a company use a digital twin of an employee in training simulations without their express permission? These questions strike at the core of evolving personality rights in the age of AI.

Adding to the complexity is the role of anonymity and jurisdictional challenges in enforcing legal remedies. Deepfake creators often operate from locations where legal enforcement is weak or nonexistent. The global nature of the internet means that harmful content can be created in one country, hosted in another, and consumed worldwide—creating a tangled web of cross-border legal issues. Traditional legal mechanisms like defamation suits, copyright claims, and privacy violations may not always be effective or applicable in these cases. Victims are frequently left to navigate a confusing patchwork of laws, often without sufficient resources or legal support.

From a philosophical and ethical standpoint, the rise of AI-generated likeness challenges our understanding of identity, consent, and authenticity. In societies that value autonomy and individual dignity, the unauthorized manipulation of one's likeness can be seen as a profound violation. It raises fundamental questions about what it means to be "real" in a digital world, and whether individuals should have the right to control how they are digitally represented. These concerns are particularly salient in a world where misinformation and digital manipulation can have real-world consequences, from inciting violence to undermining democratic processes.

Recognizing the urgency of the issue, some jurisdictions have begun to take legislative steps. Laws targeting non-consensual deepfake pornography, electoral manipulation, and fraudulent impersonation are emerging in places like California, China, and the United Kingdom. However, these laws are often narrow in scope and reactive in nature. A broader, more proactive legal approach is needed—one that encompasses personality rights, digital consent, ethical AI use, and platform accountability.

This paper aims to explore the multifaceted legal challenges posed by AI-generated likeness, focusing specifically on personality rights and social media

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

exploitation. It will analyze existing legal frameworks, highlight their limitations, and propose potential pathways for reform. The discussion will also consider the roles of technology developers, policymakers, and social media platforms in creating a more ethical and legally sound environment. Ultimately, the goal is to provide a comprehensive understanding of how society can protect individual identity and dignity in an era where digital representations are increasingly indistinguishable from the real thing.

THE RISE OF DEEPFAKES AND AI-GENERATED LIKENESS

The rapid progression of artificial intelligence in the 21st century has led to unprecedented developments in how content is created, shared, and consumed. Among the most transformative—and controversial—of these innovations is the emergence of deepfakes: synthetic media that use deep learning techniques to produce hyper-realistic but fabricated representations of individuals. Whether it's generating videos, images, or voices, AI-generated likenesses are now capable of closely mimicking real people, blurring the boundaries between authentic and artificial content.

Deepfakes are primarily produced using a branch of machine learning known as generative adversarial networks (GANs). In a GAN system, two neural networks—the generator and the discriminator—are trained simultaneously. The generator creates synthetic data, while the discriminator evaluates its authenticity against real data. Over time, the generator learns to produce increasingly realistic outputs that can deceive the discriminator. This adversarial training process is what allows GANs to craft convincing visual and auditory representations of individuals, even if the subjects never performed the depicted actions or uttered the generated speech.

Initially, the use of deepfake technology was largely confined to academic research and niche internet communities. It was often viewed as a technical curiosity—a demonstration of what AI could achieve. However, in just a few years, the technology transitioned from novelty to mainstream, propelled by increasingly user-friendly applications and open-source codebases. Today, even those with limited technical knowledge can access tools to create deepfakes using just a standard laptop and publicly available videos or images. This democratization of deepfake technology has led to an explosion of synthetic content online, some used creatively and ethically, but much of it crossing legal and moral boundaries.

One of the most troubling uses of deepfakes is in the realm of non-consensual pornography. Numerous high-profile cases have emerged where individuals—mostly women—have had their faces digitally superimposed onto explicit content without their consent. These violations have not only caused profound emotional distress but also damaged reputations, careers, and personal relationships. Unlike traditional forms of image-based abuse, deepfakes are uniquely difficult to detect and often appear indistinguishable from reality, making it hard for victims to prove their authenticity or seek redress.

Beyond adult content, deepfakes are increasingly being used for political manipulation. Fabricated videos have been created showing politicians making inflammatory statements or engaging in scandalous behavior. These clips, if widely believed, have the potential to sway public opinion, influence elections, and fuel disinformation campaigns. In a world already grappling with the consequences of fake news, the threat posed by deepfakes to democratic institutions and public trust is substantial. Their ability to manufacture controversy or create false narratives undermines journalistic integrity and complicates efforts to maintain informed public discourse.

Financial fraud and impersonation are also on the rise due to the capabilities of AI-generated likeness. Voice cloning, for instance, has been used in sophisticated scams where fraudsters impersonate CEOs or family members to extract money or confidential information. A widely reported case involved cybercriminals using AI to mimic the voice of a company executive, leading to a fraudulent transfer of hundreds of thousands of dollars. These incidents reveal how deepfake technology can be weaponized for economic exploitation and erode trust in traditional modes of communication.

While much attention has been focused on the negative uses of deepfakes, it's important to acknowledge their legitimate applications. In film and entertainment, AI-generated likenesses are used to de-age actors, resurrect deceased performers, or produce realistic CGI sequences. In education, healthcare, and marketing, synthetic avatars and voices offer cost-effective ways to personalize content and improve user engagement. For instance, language learning platforms may use AI to generate native-like pronunciation models, while virtual therapists can simulate empathetic interactions using emotionally intelligent avatars. These beneficial uses demonstrate the dual nature of the technology—it is neither inherently good nor bad, but rather dependent on the intent behind its use.

The commodification of likeness is not a new phenomenon. However, AI has changed the scale and scope at which it can be done. In earlier decades, unauthorized use of a person's image or voice for commercial gain required extensive resources and was relatively easy to trace. Today, a realistic video or audio clip can be generated in hours using content scraped from social media profiles. Celebrities, influencers, and everyday users alike are at risk of having their digital personas exploited without consent. This presents serious challenges for existing legal frameworks, which are often ill-equipped to handle issues of authorship, consent, and accountability in AI-generated media.

Another dimension of concern is the psychological and societal impact of deepfakes. The technology feeds into a broader trend of post-truth culture, where objective facts are increasingly devalued in favor of emotionally compelling narratives. As deepfakes become more pervasive, they threaten to erode the public's ability to trust visual evidence. A future in which seeing is no longer believing can have far-reaching implications—from legal proceedings relying on video evidence to public responses during emergencies. The concept of "reality" becomes increasingly negotiable, and with it, the ability to maintain a shared understanding of truth and authenticity.

Social media platforms have been instrumental in the viral spread of deepfakes. Their algorithms prioritize engagement, often amplifying sensational or controversial content. This creates an environment where fake videos can reach millions of users before fact-checkers or moderators can intervene. While major platforms like Facebook, Twitter (X), and YouTube have introduced policies to ban or label manipulated media, enforcement is inconsistent and often reactive. Furthermore, AI-generated content can be subtly altered to evade detection algorithms, making it a moving target for content moderation efforts.

As the sophistication of AI tools increases, so does the concern that deepfakes will become indistinguishable from genuine media in real time. Live video manipulation, real-time face swapping, and AI-powered speech synthesis are already in development stages. This convergence of technologies could lead to scenarios where impersonation occurs during video calls or livestreams—events that previously relied on visual presence for credibility. The implications for journalism, law enforcement, and personal communication are profound, raising urgent questions about verification, identity, and trust.

The rise of deepfakes also highlights the broader issue of data privacy. To create realistic AI-generated likenesses, algorithms require vast amounts of training data, often sourced from publicly available photos, videos, and voice recordings. In many cases, individuals are unaware that their data is being used to train generative models. This exploitation of personal data without explicit consent underscores the importance of data protection laws and ethical AI governance. It also calls for increased transparency from AI developers and data collectors about how and why this information is being utilized.

LEGAL FOUNDATIONS OF PERSONALITY RIGHTS

In a world increasingly governed by digital interactions, the concept of personality rights has gained critical importance. Personality rights, sometimes referred to as the "right to personality," protect an individual's personal attributes and ensure that their identity—comprising their name, image, voice, likeness, and other defining characteristics—is not exploited without consent. While these rights

have long been recognized in the context of celebrities and public figures, they are becoming more relevant as digital technologies, particularly artificial intelligence (AI) and deepfake technologies, increasingly threaten personal dignity, privacy, and autonomy. The legal foundations of personality rights are multifaceted, drawing on constitutional principles, common law, statutory laws, and evolving digital frameworks.

The core idea behind personality rights is that individuals have an inherent right to control the use of their identity in both public and private spheres. This right covers a range of aspects, including one's name, likeness, voice, and any other identifiable features that are uniquely associated with that person. Unlike other forms of intellectual property, personality rights do not require an individual to create something novel or tangible but instead protect an intrinsic part of one's identity that can be commercialized or exploited by others.

The need for legal protections around personality rights has become more pronounced with the rise of digital technology and the ability to replicate human likenesses through AI. The core of the legal struggle in this arena lies in determining how far personality rights extend, especially in the context of AI-generated likenesses and synthetic media such as deepfakes.

1. The Right of Publicity

One of the key legal concepts underpinning personality rights in common law jurisdictions, especially in the United States, is the **right of publicity**. The right of publicity allows individuals to control the commercial use of their identity, typically their name, image, voice, or likeness. Originally, the right of publicity was developed to protect individuals from the unauthorized exploitation of their identity for profit. However, its application has expanded over time, especially in the realms of advertising, entertainment, and media.

The right of publicity is not recognized universally across legal systems and tends to vary by jurisdiction. In the United States, the right of publicity is mostly governed by state law, meaning its scope and enforcement depend on where an individual resides. Some states, like California and New York, have developed robust laws that grant celebrities, athletes, and other public figures significant protection against unauthorized use of their likeness for commercial purposes. These protections extend to cases where an individual's image or voice is used in a way that suggests endorsement or affiliation without consent.

However, this right is not absolute and often includes exceptions. For instance, the right of publicity does not protect against all forms of non-consensual media use; it generally focuses on commercial exploitation rather than free speech. Additionally, the scope of the right of publicity can become murky when the individual's image or likeness is used for artistic, political, or non-commercial purposes. The balancing of these interests—commercial exploitation versus free expression—has led to complex case law and ongoing debate about where the line should be drawn.

With the advent of AI and deepfakes, the limitations of the right of publicity have become increasingly evident. For instance, a synthetic representation of a celebrity could easily be used to endorse a product without the celebrity's consent, but the law may only protect the celebrity's right of publicity in cases where there is clear commercial intent. However, the development of AI-generated likeness technologies complicates this analysis, as it's increasingly possible to create realistic depictions of individuals who have not given their consent for their likeness to be used in any capacity, commercial or otherwise.

2. Right to Privacy

Another legal foundation closely tied to personality rights is the **right to privacy**, which provides individuals with protection against the unauthorized invasion of their personal space, likeness, and personal information. While the right of publicity is focused on protecting the commercial use of one's identity, the right to privacy addresses broader concerns related to the personal exploitation of one's likeness, including non-consensual surveillance, the distribution of private information, and the use of one's image in a way that causes distress or harm.

The right to privacy was famously articulated by Justice Louis Brandeis and Samuel Warren in a 1890

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

article in the *Harvard Law Review*, where they argued for the recognition of privacy as an essential element of individual autonomy. The right to privacy encompasses several different interests, including the right to control one's image, to be left alone, and to maintain the confidentiality of personal information. In the modern era, the right to privacy has been expanded by various national laws, such as the European Union's **General Data Protection Regulation (GDPR)**, which protects individuals' privacy by granting them more control over their personal data and how it is used.

The intersection of the right to privacy and AI-generated likeness is particularly problematic in the digital age. AI tools like deepfakes make it possible to create highly realistic, fabricated representations of individuals that infringe on their privacy without their knowledge or consent. The proliferation of AI-generated likenesses raises fundamental questions about the right to control one's identity in the digital sphere. For instance, if an individual's image is manipulated and spread online without their consent, it may lead to significant harm, including reputational damage, emotional distress, and a loss of control over their own identity. In many cases, victims of such violations may not have a legal remedy under traditional privacy laws, as these laws were not designed to address digital manipulations or synthetic media.

3. The Role of Intellectual Property Law

In addition to privacy and publicity rights, intellectual property law also plays a crucial role in defining and protecting personality rights, particularly in the digital realm. For example, copyright law provides creators with the exclusive right to reproduce, distribute, and publicly perform their original works. While copyright does not directly protect an individual's name or likeness, it can offer indirect protection when a person's likeness is used as part of an artistic creation, such as in a photograph, film, or digital avatar. This becomes relevant in cases where AI-generated likenesses are created using an individual's image as part of a larger creative work. In some instances, creators of such works may claim ownership over the AI-generated likeness as part of their intellectual property rights.

However, the application of copyright in the context of AI-generated likeness is still an evolving area of law. For example, if an AI model generates a deepfake of a celebrity's likeness without any human input, it raises questions about authorship and ownership. Who owns the rights to the deepfake? The AI developer? The person whose likeness was used? The person who created the AI model? These unresolved issues indicate the gaps in current intellectual property frameworks and highlight the need for reform to adequately address the complexities of AI and digital likeness.

4. The Influence of International Law

International legal frameworks also play an important role in the protection of personality rights. For example, in the European Union, the **European Convention on Human Rights** and the **Charter of Fundamental Rights of the European Union** provide individuals with the right to privacy, which extends to the protection of their image and likeness. The **GDPR** has also set a global standard for data protection, placing emphasis on the individual's right to control their personal data, including biometric and facial recognition data, which are often used in AI-generated likenesses.

Similarly, in countries like Japan, South Korea, and China, legal protections are evolving to address new challenges posed by AI and digital technologies. China, for instance, has introduced regulations that mandate consent for the use of deepfake technology in specific contexts, while also working to balance innovation with individual rights.

5. Evolving Legal Frameworks for AI and Digital Likeness

Given the challenges posed by AI-generated likeness and deepfakes, there is a growing need for legal reform to address these new realities. Some jurisdictions have already begun to enact laws specifically targeting the misuse of deepfakes and AI-generated media. For example, California's **AB 730** addresses the creation and distribution of non-consensual deepfake videos, while the UK's **Online Safety Bill** seeks to tackle harmful online content, including AI-generated media. However, these laws are often reactive rather than proactive, addressing

the consequences of misuse rather than preventing it.

To protect individuals' personality rights in the digital age, it is essential for legal systems to evolve and incorporate new provisions that account for the capabilities of AI technologies. This may include extending privacy protections to cover digital likenesses, strengthening the right of publicity to address new forms of exploitation, and ensuring that intellectual property law adapts to the complexities of AI-generated content.

SOCIAL MEDIA EXPLOITATION AND PLATFORM LIABILITY

The rise of social media platforms has revolutionized communication, interaction, and content-sharing globally. These platforms, including Facebook, Instagram, Twitter (now X), TikTok, and YouTube, have created vast digital ecosystems where users can freely share personal experiences, thoughts, and creations. With billions of active users worldwide, social media has become an essential part of daily life, influencing everything from social relationships to political discourse. However, alongside these positive aspects, there has been an explosion of new issues, particularly surrounding privacy violations, misinformation, and the unauthorized use of individuals' images and likenesses.

The proliferation of AI-generated likenesses, including deepfakes, has significantly intensified the exploitation of personal identity on social media. These platforms, which often serve as the primary channels through which AI-generated content spreads, have found themselves at the center of the debate over privacy, consent, and digital rights. As deepfake technology advances, social media has become a fertile ground for unauthorized manipulations of individuals' likenesses, leaving users vulnerable to reputational harm, emotional distress, and even financial loss. The rapid pace at which AI-driven content spreads on social media raises the fundamental question: To what extent are social media platforms responsible for preventing or addressing the exploitation of personal likenesses? This section explores the intersection of social media exploitation and platform liability, focusing on the legal challenges platforms face when it comes to protecting users' personality rights. The role of these platforms in moderating AI-generated content, including deepfakes, will be examined in the context of current liability frameworks and potential legal reforms.

1. The Scope of Social Media Exploitation

Social media exploitation occurs when an individual’s image, likeness, or personal data is used without consent to create content that can harm their reputation, violate their privacy, or exploit their identity for financial gain. While traditional exploitation of identity has often involved commercial endorsements or unauthorized advertisements, social media has introduced a new dynamic: the mass dissemination of manipulated or fabricated content to a global audience in real-time. This includes the creation of deepfakes, which can convincingly depict individuals saying or doing things they never did. The viral nature of social media makes it all the more dangerous, as content can spread to millions of users within hours or days, even before victims can take action to remove it.

The range of social media exploitation is wide. For example, deepfake pornography is an increasingly prevalent issue, where an individual’s face is digitally inserted into explicit videos without consent. In other cases, individuals' images or voices are manipulated for political purposes, causing reputational damage or even political destabilization. Moreover, AI-generated likenesses are also used in scams and fraudulent activities, where voice mimicking tools impersonate individuals to trick others into giving away money or sensitive information.

The spread of such content on social media not only undermines individual privacy but also calls into question the ethical implications of using AI to manipulate identity in ways that were previously unimaginable. As digital content becomes more easily fabricated and distributed, individuals find themselves increasingly vulnerable to the unauthorized use of their likeness for malicious or exploitative purposes.

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

2. Platform Liability: The Current Legal Framework

Under existing laws, social media platforms often enjoy legal protections that shield them from liability for content posted by users. In the United States, for example, Section 230 of the **Communications Decency Act (CDA)** provides platforms with immunity from liability for third-party content, meaning platforms are not held responsible for user-generated content, including harmful or defamatory material. This law has been crucial in fostering the growth of platforms by allowing them to act as neutral intermediaries without the fear of being sued over the millions of posts their users share.

However, Section 230 immunity is not absolute. Courts have consistently ruled that platforms may lose their immunity when they become directly involved in creating or editing content, as in the case of recommending or promoting content through algorithms. Platforms may also be held liable if they fail to remove content that violates the law or infringes on individuals' rights when they have been notified of its existence.

In the context of deepfakes and AI-generated likeness, the application of Section 230 and similar legal protections is particularly controversial. These technologies often involve the creation and distribution of manipulated content that may infringe on an individual's personality rights or cause harm. However, under the current framework, social media platforms may argue that they are not responsible for the creation or spread of deepfakes because these tools are generally used by third-party users, and the platforms themselves do not directly create the content.

On the other hand, some legal experts argue that platforms should be held accountable when they knowingly host or promote harmful content. For example, if a platform uses an algorithm to prioritize sensational content, such as deepfakes, this could be seen as an active role in spreading harmful material. The argument here is that platforms are not merely passive distributors but play a central role in shaping what users see and interact with. When deepfakes or other forms of harmful AI-generated content go viral, platforms like Facebook, YouTube, and Twitter are seen by some as having an ethical and legal responsibility to prevent its spread.

3. The Role of Content Moderation and Platform Responsibility

Content moderation is central to the debate surrounding social media exploitation. Social media platforms are tasked with monitoring and removing harmful or illegal content, but the sheer volume of posts, videos, and images shared daily makes this an extraordinarily challenging task. In recent years, platforms have implemented measures to detect and remove deepfakes and other synthetic media, using AI tools and human moderators to identify and

4. The Ethics of AI-Generated Content and Social Media

The ethical considerations surrounding the use of AI-generated likenesses on social media are complex and multifaceted. On one hand, platforms provide a space for creative expression, political discourse, and social interaction, all of which can benefit from the innovative uses of AI technologies. On the other hand, the potential for harm is significant—individuals' rights to privacy, consent, and identity can be violated with devastating consequences.

One of the key ethical challenges is determining who is responsible when AI-generated content goes wrong. Is it the responsibility of the user who created the content? The platform hosting it? Or the developers of the AI tools used to create it? As AI becomes more sophisticated, it is likely that traditional models of liability will need to be reassessed. Lawmakers, platform owners, and tech developers must collaborate to ensure that users' rights are protected while preserving the creative potential of AI.

Additionally, platforms must address the broader social implications of the viral spread of harmful content. Given their immense reach, platforms have a significant role to play in shaping societal values and norms. The ethical responsibility to protect users from harm must extend beyond simply removing malicious content—it must also involve creating systems that educate users about the

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

potential dangers of synthetic media and promote digital literacy.

COMPARATIVE JURISDICTIONS AND LEGISLATIVE RESPONSES

As AI-generated likenesses and deepfakes become increasingly prevalent, countries around the world are grappling with how best to protect individuals from digital identity exploitation. Different legal systems have adopted varied approaches to address the challenges posed by synthetic media. A comparative analysis of how jurisdictions respond to AI-generated likenesses reveals a spectrum of strategies, ranging from comprehensive legislative reforms to targeted regulatory responses. These efforts reflect not only legal diversity but also cultural differences in the prioritization of privacy, free speech, and technological innovation.

United States: Balancing Innovation and Individual Rights

In the United States, the response to AI-generated likenesses and deepfakes has largely relied on state-level legislation and the common law right of publicity. States such as California and New York have expanded their statutory protections to include digital replicas of individuals' likenesses. For instance, California's **AB 602** prohibits the creation and distribution of sexually explicit deepfakes without the consent of the individual depicted, while **AB 730** restricts the use of deepfakes in political advertising within a defined time frame before elections. However, the federal legal framework remains fragmented. The U.S. Congress has introduced several bills, such as the **DEEPFAKES Accountability Act**, aimed at requiring disclosures and digital watermarks on AI-generated media, but these have not yet been enacted. Section 230 of the Communications Decency Act continues to shield social media platforms from liability, complicating enforcement. Overall, the U.S. legal landscape is evolving, with growing recognition of the need to protect identity rights without stifling free expression or innovation.

European Union: Emphasis on Data and Privacy Protection

The European Union takes a more holistic approach, emphasizing privacy and data protection through regulations like the **General Data Protection Regulation (GDPR)**. The GDPR grants individuals the right to control their personal data, including biometric and facial data, which are essential to creating AI-generated likenesses. Under this framework, using a person's likeness without consent can constitute a data protection violation.

Additionally, the EU's **Digital Services Act (DSA)** introduces obligations for online platforms to remove illegal content swiftly and implement robust risk mitigation measures against disinformation and harmful deepfakes. The **Artificial Intelligence Act**, still under development, aims to regulate high-risk AI systems, including those used in biometric identification and emotion recognition. Together, these regulations position the EU as a global leader in ensuring ethical AI use and protecting digital identity rights.

China: A Proactive Regulatory Approach

China has adopted a proactive stance toward synthetic media. In 2022, the **Cyberspace Administration of China (CAC)** introduced rules requiring AI-generated content to be clearly labeled and banning the use of deepfakes to endanger national security, disrupt the economy, or defame individuals. These rules mandate consent for using someone's likeness and impose strict compliance standards on content platforms and developers. This regulatory model reflects China's emphasis on state control, content governance, and societal stability, combining legal restrictions with real-time censorship mechanisms.

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

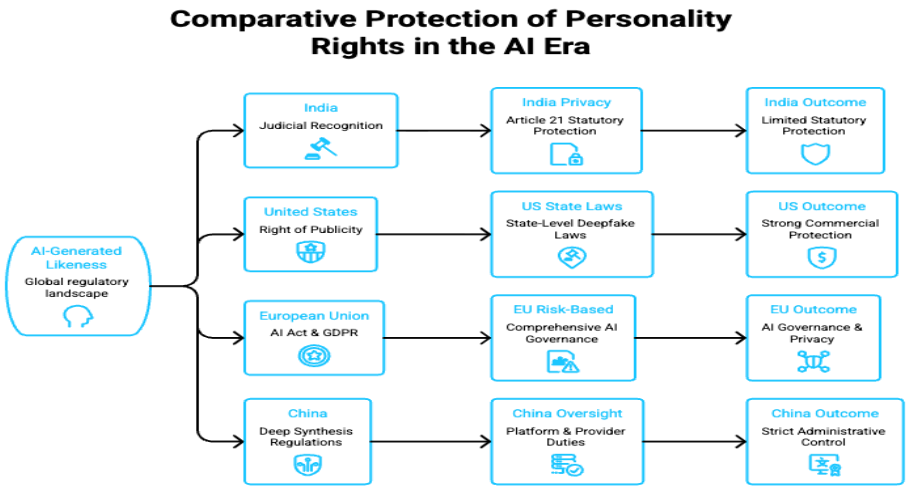

Fig1 : Comparative Regulatory Approaches to AI-Generated Likeness in India, the United States, the European Union, and China

FUTURE PATHWAYS: LAW, ETHICS, AND TECHNOLOGY

As AI-generated content becomes increasingly sophisticated and accessible, the intersection of law, ethics, and technology presents critical opportunities—and challenges—for protecting individual rights in the digital age. The proliferation of deepfakes and synthetic media has revealed significant gaps in legal frameworks, ethical standards, and technological safeguards. Moving forward, addressing these gaps will require a multi-dimensional approach involving proactive legislation, ethical design principles, and responsible innovation.

Legal Innovations and International Harmonization

Future legal pathways must focus on establishing comprehensive and cohesive standards for protecting personality rights in both national and international contexts. While current legal protections are often fragmented—varying from jurisdiction to jurisdiction—a harmonized approach could provide individuals with more consistent recourse against misuse of their likenesses, regardless of geographical boundaries. This could involve the development of international treaties or model laws, similar to the **Berne Convention** for copyright, but aimed at digital identity and personality rights.

Additionally, new legislation should move beyond reactive enforcement and adopt proactive requirements. This includes mandating informed consent for the use of personal likenesses in AI-generated media, requiring labeling or watermarking of synthetic content, and imposing accountability on developers and platforms who distribute such tools or content. Moreover, laws must address platform liability, striking a balance between free expression and the protection of individuals from digital harm.

Ethical Design and Responsible AI Development

The ethical dimension of AI-generated likeness must be integrated into the design and deployment of new technologies. AI developers and companies should adopt principles of "ethics-by-design", where privacy, consent, transparency, and fairness are embedded into systems from the outset. For example, facial recognition or generative media tools should include built-in limitations to prevent unauthorized use, such as requiring verified identity or consent before content is generated or shared. Ethical AI development also requires a strong emphasis on inclusivity and accountability. Developers must be aware of the cultural, racial, and gendered biases that can be exacerbated by synthetic

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

media, especially when deepfakes are used to target vulnerable or marginalized groups. Institutional review boards or AI ethics committees, modelled after those in biomedical research, could offer guidance and oversight for high-impact AI applications.

Technological Safeguards and User Empowerment

Technology itself can be a powerful tool in combating misuse. Future pathways include the development of robust deepfake detection tools powered by machine learning that can identify synthetic media with high accuracy. Collaborations between tech companies, academic institutions, and governments can enhance these detection capabilities and make them widely accessible to journalists, courts, and the general public.

User empowerment is also key. Platforms must equip users with tools to report, flag, and challenge unauthorized use of their likenesses. Digital literacy campaigns can educate the public on identifying and responding to manipulated content, fostering a more informed and resilient digital society.

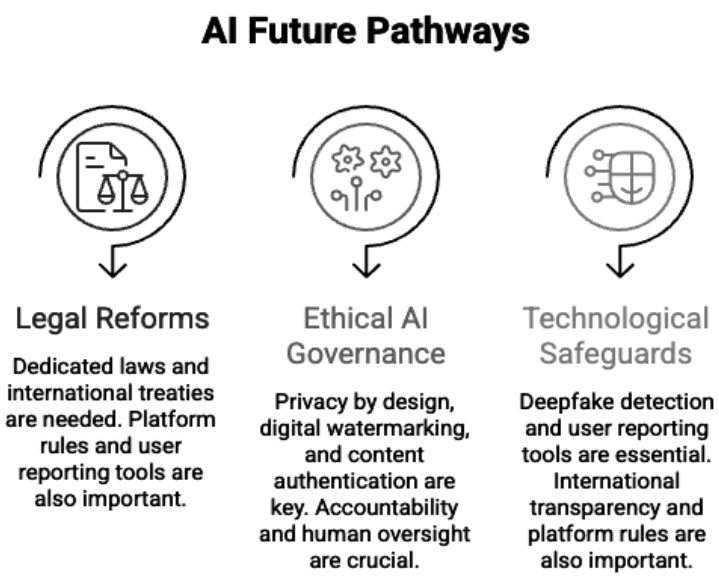

Fig 2 :Future Pathways for Protecting Personality Rights in the AI Ecosystem

CONCLUSION

The emergence of AI-generated likeness and deepfake technology marks a defining moment in the evolving relationship between technology, identity, and law. While these tools offer impressive capabilities for creativity, entertainment, and innovation, they also present profound ethical and legal challenges, especially concerning the unauthorized use of personal identity in the digital realm. As this technology becomes increasingly democratized and accessible, the risks of exploitation—particularly on social media platforms—have grown at an alarming rate.

This article has explored the multifaceted implications of AI-generated likenesses through the lens of personality rights, legal liability, social media exploitation, and comparative jurisdictional responses. What becomes evident is the pressing need for a more robust legal infrastructure that can adapt to the speed and complexity of technological advancement. Many jurisdictions are still in the early stages of formulating responses, with most legislation reactive rather than proactive. The lack of cohesive international frameworks creates loopholes that can be easily exploited, especially in cross-border digital environments.

Economic Sciences
https://economic-sciences.com
ES(2026) 22, 2 (2) , 61-73 | ISSN:1505-4683

At the heart of the debate lies the protection of individual autonomy and dignity. Personality rights—encompassing one's name, likeness, and voice—must be recognized as essential components of digital identity and safeguarded accordingly. The challenge lies in striking a balance between freedom of expression, artistic creativity, and the individual's right to privacy and consent.

Social media platforms must also shoulder greater responsibility. Their algorithms and recommendation systems play a pivotal role in the viral spread of synthetic media. While some have adopted content moderation and labeling practices, the enforcement remains inconsistent. A coordinated effort involving governments, platforms, developers, and users is essential for curbing misuse while promoting digital literacy and accountability.

Looking forward, a multidisciplinary approach that combines legal reform, ethical AI design, and advanced detection technologies will be crucial. Developers should integrate consent-based mechanisms into generative tools, platforms must enhance moderation transparency, and legislators need to close gaps in personality rights laws. Most importantly, the conversation about digital identity and AI ethics must continue to evolve in tandem with technology itself.

If the digital world is to be one where trust, authenticity, and dignity prevail, then society must rise to the challenge of governing emerging technologies not only with innovation, but with foresight, justice, and humanity.

REFERENCES

1. AI Now Institute. (2021). **Algorithmic Accountability Policy Toolkit**.
2. AlgorithmWatch. (2022). **Deepfakes and Synthetic Media Policy Tracker**.
3. Brookings Institution. (2020). **Confronting Deepfakes: Policy, Law, and Tech**.
4. California Legislative Information. (2019). **AB-602 Deceptive Use of Digital Media**.
5. California Legislative Information. (2019). **AB-730 Elections: Deceptive Audio or Visual Media**.
6. Chesney, R., & Citron, D. (2019). **Deepfakes and the New Disinformation War**, *Foreign Affairs*.
7. Citron, D. K. (2014). **Hate Crimes in Cyberspace**, Harvard University Press.
8. Columbia Journal of Law & the Arts. (2021). **Protecting Identity in the Age of Deepfakes**.
9. Communications Decency Act, 47 U.S.C. § 230.
10. Cyberspace Administration of China (CAC). (2022). **Regulations on Deep Synthesis Internet Information Services**.
11. Deeptrace Lab. (2019). **The State of Deepfakes: Landscape, Threats, and Impact**.
12. Ethics & Information Technology Journal. (2022). **The Morality of Synthetic Media**. 13. European Commission. (2021). **Proposal for a Regulation on Artificial Intelligence (AI Act)**.
14. European Commission. (2022). **Digital Services Act (DSA)**.
15. European Parliament. (2016). **General Data Protection Regulation (GDPR)**.
16. Floridi, L., & Cowls, J. (2019). **A Unified Framework of Five Principles for AI in Society**, *Harvard Data Science Review*.
17. Future of Privacy Forum. (2023). **Deepfakes, Biometrics, and Privacy**.
18. Harvard Law Review. (2020). **Regulating Deepfakes under Existing Law**.
19. House of Lords (UK). (2021). **Deepfakes and the Law**, Select Committee Report.
20. Klonick, K. (2017). **The New Governors: The People, Rules, and Processes Governing Online Speech**, *Harvard Law Review*.
21. Legal Information Institute, Cornell Law School. (2023). **Right of Publicity**.
22. McStay, A. (2021). **Emotional AI: The Rise of Empathic Media**, *SAGE Publishing*.
23. MIT Media Lab. (2021). **Detecting Deepfakes with Neural Networks**.
24. National Institute of Standards and Technology (NIST). (2022). **AI Risk Management Framework**.
25. Office of Science and Technology Policy (OSTP). (2022). **Blueprint for an AI Bill of Rights**.
26. Rini, R. (2020). **Deepfakes and the Epistemic Backstop**, *Philosophy & Technology*.
27. Stanford Internet Observatory. (2023). **The Landscape of AI-Generated Media**.
28. Tiku, N. (2023). **How AI Deepfakes Threaten Democracy**, *Washington Post*.
29. U.S. Congress. (2019). **DEEPFAKES Accountability Act**.
30. UK Information Commissioner's Office (ICO). (2022). **Guidance on Biometric Data and AI**.
31. United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). **Recommendation on the Ethics of Artificial Intelligence**.

32. West, S. M., Whittaker, M., & Crawford, K. (2019). **Discriminating Systems: Gender, Race, and Power in AI**, AI Now Institute.
33. WIPO. (2023). **AI and Intellectual Property Policy**.
34. Woodrow Hartzog. (2018). **Privacy's Blueprint: The Battle to Control the Design of New Technologies**, Harvard University Press.
35. World Economic Forum. (2020). **Global Technology Governance Report**.