

DEEPFAKE, PORTRAIT RIGHTS AND IDENTITY PROTECTION: A COMPARATIVE ANALYSIS OF CHINESE AND BRAZILIAN LAW

*Jose Humberto Deveza Assola **

Abstract: The rapid development of generative artificial intelligence has transformed the ways in which human identity can be represented, reproduced, and manipulated. Deepfakes, in particular, enable the creation of highly realistic synthetic representations of individuals' faces, voices, and gestures, often without their knowledge or consent. This technology challenges traditional concepts of personality rights and raises complex questions concerning image, voice, privacy, dignity, reputation, and the allocation of liability among individuals, platforms, and technology providers. Against this background, this article examines the legal protection of identity against deepfakes through a comparative analysis of Chinese and Brazilian law. It first examines the Chinese framework, focusing on the 2021 Civil Code and its express protection against technologically generated forgery, as well as administrative regulations governing deep synthesis and generative artificial intelligence. It then analyzes the Brazilian framework, based on constitutional guarantees, personality rights under the Civil Code, the General Data Protection Law, the Marco Civil da Internet, and emerging judicial responses to synthetic content. The comparative analysis identifies two distinct regulatory approaches: a more preventive and technologically specific framework in China and a more reactive and jurisprudential model in Brazil. The article argues that, despite their different institutional structures, both systems face unresolved challenges concerning consent, platform responsibility, rapid content removal, freedom of expression, and the protection of identity in artistic, commercial, political, and personal contexts. It concludes by examining the extent to which existing personality rights can accommodate synthetic identity and whether additional legal and institutional mechanisms are necessary to provide effective protection in an increasingly synthetic information environment.

Keywords: deepfakes; personality rights; synthetic identity; comparative law; China and Brazil.

INTRODUCTION

In the last two decades, technological development has advanced at a pace that few observers could have anticipated. This acceleration has reshaped not only the functioning of contemporary societies but also the very foundations of human communication and interaction. Among the most disruptive innovations to emerge from this period is artificial intelligence. What began

* Brazilian intellectual property attorney; LL.M. candidate in Intellectual Property and Innovation Policy, Tsinghua University. Email: humbertodeveza@gmail.com / ORCID iD: <https://orcid.org/0009-0006-1271-5304>.

as relatively simple systems capable of performing limited text-based tasks has evolved into complex architectures capable of generating synthetic images, voices, and entire audiovisual narratives. This evolution has culminated in the phenomenon now widely known as deepfakes, a technology that dissolves the once clear boundary between reality and fabrication and forces legal systems around the world to confront challenges that were unimaginable only a generation ago.

Deepfakes are far more than technical curiosities or digital novelties. They represent a profound transformation in ways that identity can be manipulated, reproduced, and falsified. By enabling the creation of hyper-realistic portrayals of individuals without their consent, these tools destabilize long-standing principles of personality rights. The right to one's image, voice, and identity, once considered secure within traditional legal frameworks, is now exposed to unprecedented forms of exploitation. The distinction between authentic representation and fraudulent imitation, which for centuries served as a foundation for legal protection, has become increasingly difficult to maintain. The consequences of this shift extend well beyond personal privacy. They affect honor, reputation, emotional well-being, and even the credibility of democratic institutions that depend on the integrity of public communication.

This tension between technological innovation and the protection of fundamental rights is particularly visible in China and Brazil, two jurisdictions that have adopted distinct yet complementary approaches to the regulation of personality rights in the age of synthetic media. China's 2021 Civil Code marked a significant milestone by explicitly codifying protections for image and voice and by addressing forgery through technological means. These provisions, combined with an extensive administrative framework for regulating generative artificial intelligence, create a structured environment in which the risks associated with deepfakes can be identified, monitored, and mitigated. The Chinese model is characterized by a preventive logic, in which the state plays a central role in supervising technological development and ensuring that digital tools do not undermine social stability or individual rights.

Brazil, by contrast, relies on a constitutional and statutory foundation that is less explicit but nonetheless robust. The Federal Constitution, the Civil Code, and the General Data Protection Law (LGPD) form the core of the Brazilian system for safeguarding personality rights. In the absence of specific legislation addressing synthetic identity, Brazilian courts have assumed a central role in shaping legal responses to deepfake-related harms. Judicial decisions have been particularly important in cases involving non-consensual sexual content, fraudulent voice replication, and the dissemination of manipulated political material. The Brazilian model is

therefore more reactive and jurisprudential, relying on the adaptation of traditional legal categories to new technological realities.

Despite these efforts, neither country has yet developed a fully coherent theoretical model capable of addressing the wide spectrum of deepfake applications. The legal responses remain fragmented, reactive, and often dependent on judicial interpretation rather than comprehensive statutory design. This article therefore seeks to explore the comparative strengths and weaknesses of the Chinese and Brazilian systems. It asks whether existing personality rights are sufficient to confront the risks posed by synthetic identity and identifies the structural gaps that must be filled to ensure meaningful protection in the digital era. By examining these two jurisdictions side by side, the study aims to contribute to a broader understanding of how legal systems can adapt to the challenges posed by artificial intelligence and how the protection of identity can be preserved in an increasingly synthetic world.

I. DEEPFAKE AS A LEGAL CONCEPT: SYNTHETIC IDENTITY AND LEGAL RISKS

When discussing deepfakes in a legal context, it is essential to move beyond a purely technical description and consider the broader implications of what this technology represents. At its core, a deepfake is the construction of a synthetic identity, a digitally fabricated presence that convincingly imitates the appearance, voice, or gestures of a real individual without that person's participation or consent. This synthetic identity is not a simple reproduction of existing material. It is the result of a generative process that creates new content which appears authentic, even though it has no basis in the lived experience of the person being portrayed.

Unlike traditional forms of representation, which depend on voluntary expression and on the physical presence of the individual, synthetic identity emerges from algorithmic processes triggered by human commands. These algorithms are trained on extensive datasets that capture subtle details of human expression. As a result, they are capable of reproducing facial movements, vocal tones, and bodily gestures with remarkable precision. The output is an illusion of authenticity that can be extremely difficult to distinguish from reality, even for trained observers.

This capacity to fabricate identity raises profound legal and philosophical questions. Deepfakes challenge long-standing assumptions about what it means for an image or a voice to belong to someone. They disrupt the traditional link between identity and embodiment, replacing it with a model in which identity can be simulated, transferred, or manipulated by third parties. The legal system, which has historically relied on the stability of this link, must now confront situations in which the representation of a person is

no longer tied to their physical presence or their consent.

The implications extend far beyond personal privacy. Synthetic identity can be used to damage reputation, distort public debate, manipulate evidence, or create false narratives that influence social and political processes. For this reason, understanding deepfakes requires not only technical literacy but also a recognition of the broader social, ethical, and legal transformations that this technology introduces.

This phenomenon raises profound legal questions because it destabilizes the boundaries of identity and consent. If a person's likeness can be replicated without their involvement, the very notion of control over one's image and voice becomes precarious. Personality rights, traditionally designed to safeguard dignity and autonomy, are challenged by a technology that can fabricate presence at will. Scholars such as Dominika Kuźnicka-Błaszowska and Nadiya Kostyuk define deepfakes as "synthetic media created through AI algorithms to seamlessly superimpose one person's likeness onto another"¹. Their observation underscores not only the technical sophistication of the process but also its potential to be weaponized. As they note, deepfakes can serve as powerful instruments in information campaigns, enabling actors to manipulate narratives, distort facts, and influence public opinion on a massive scale.

The risks associated with deepfakes extend far beyond individual harm. Although the violation of personal rights is often the most visible consequence, the potential for broader societal damage is equally significant. Deepfakes can be deployed as instruments of political disinformation, corporate sabotage, or even international propaganda. In each of these contexts, synthetic identity becomes a tool for manipulating public perception, eroding trust in audiovisual evidence, and destabilizing the credibility of institutions that depend on reliable communication. When the authenticity of images and voices can no longer be taken for granted, the foundations of public discourse are weakened, and the ability of societies to engage in informed decision-making is compromised.

For this reason, the legal concept of synthetic identity must address not only the protection of personal rights but also the safeguarding of collective interests. These include the preservation of democratic debate, the integrity of electoral processes, and the stability of public communication channels. The challenge for contemporary legal systems lies in designing frameworks capable of recognizing the unique nature of synthetic identity, classifying its risks, and establishing mechanisms of accountability for its misuse. Traditional categories of liability, which were developed in an era of analog

¹ Dominika Kuźnicka-Błaszowska & Nadiya Kostyuk, *Emerging Need to Regulate Deepfakes in International Law: The Russo-Ukrainian War as an Example*, 11 J. Cybersecurity, art. tyaf008 (2025), <https://doi.org/10.1093/cybsec/tyaf008>.

representation, are often insufficient to capture the complexity of harm generated by artificial intelligence.

Recognizing the existence of a synthetic identity is only the first step in addressing the legal challenges posed by deepfakes. The more pressing question is whether such an identity should be treated as a bearer of rights and obligations, or whether it remains a mere imitation of reality, devoid of any legal standing. This distinction is crucial because it determines whether synthetic identities are capable of being integrated into the legal order or whether they should be dismissed as artifacts without normative significance. Lawrence Solum insightfully notes that “the question whether an entity should be considered a legal person is reducible to other questions about whether or not the entity can and should be made the subject of a set of legal rights and duties”². His observation highlights the need for a principled framework that can guide courts and legislators in deciding how to classify synthetic identities.

Deepfakes complicate this debate because they do not simply replicate isolated features of a person but instead reconstruct the entire constellation of traits that make up an individual’s identity. Image, voice, facial expressions, gestures, and even subtle mannerisms are reproduced with such precision that the resulting figure can convincingly deceive audiences, including experts familiar with digital manipulation. This capacity to mimic authenticity undermines the traditional safeguards of personality rights, which were designed to protect individuals from unauthorized use of their likeness. The difficulty of distinguishing between genuine and fabricated representations raises profound risks: reputational harm, erosion of trust in audiovisual evidence, and the possibility of attributing actions or statements to individuals who never performed them.

From a legal perspective, the challenge lies in determining whether these synthetic identities should be treated as independent entities or as unlawful distortions of existing people. If considered subjects of rights, they would require a framework of regulation and accountability. If treated as mere simulacra, the focus would shift to protecting the real individuals whose identities are appropriated. Either way, the complexity of deepfakes forces legal systems to confront the boundaries of personhood and the adequacy of existing doctrines in safeguarding both individual dignity and collective trust in information.

The ability of deepfake technology to replicate human identity in its entirety introduces risks that were previously unimaginable within the legal sphere. By generating synthetic versions of a person’s image, voice, and gestures, this technology undermines the individual’s control over their own

² Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L. Rev. 1231, 1239 (1992).

representation and challenges the adequacy of existing legal protections. The unauthorized appropriation of identity elements - whether visual or auditory - constitutes, in principle, a violation of personality rights, a conclusion that both Brazilian and Chinese jurisprudence would recognize. This reality compels a thorough and integrated analysis of current legal frameworks to determine whether they are sufficient to address the complexities of synthetic identity or whether new regulatory structures must be developed.

Margaret Jane Radin's reflections provide a valuable lens for this debate. She emphasizes that certain attributes of the human person cannot be commodified, as they are inherently inalienable. Voice and image, for example, are not mere economic goods but essential components of human dignity. As Radin explains, "something that is market-inalienable is not to be sold, which in our economic system means it is not to be traded in the market"³. This principle resonates strongly in the context of deepfakes, where the transformation of identity into a manipulable digital product collides with the notion that personality rights are beyond the reach of market transactions.

Both Brazil and China enshrine this inalienability within their legal systems, albeit through different mechanisms. Brazil relies on constitutional guarantees, civil law provisions, and data protection statutes, while China incorporates explicit protections into its Civil Code and supplements them with administrative regulations on artificial intelligence. Despite these differences, the principle underlies the fact that identity cannot be treated as a commodity available for appropriation. The emergence of deepfake, however, directly challenges this principle by creating simulacra of real individuals without consent, thereby forcing legal systems to confront the tension between technological innovation and the inviolability of human dignity.

As will be explored in detail in the following chapters, both Brazilian law and the Chinese legal system enshrine the inalienability of personality rights, affirming that attributes such as image and voice cannot be commodified or transferred. The emergence of deepfakes, however, directly challenges this principle by producing simulacra of real individuals without consent, thereby colliding with the legal provisions of both countries. Identity, in theory, is not a commodity available for appropriation, yet synthetic technologies attempt to transform it into precisely that.

The risks stemming from this scenario are immediate and multifaceted. One of the most evident dangers is defamation. Deepfakes can place fabricated versions of real people in compromising or immoral situations, destroying reputations that may have taken decades to build. The viral nature of online content exacerbates this harm, allowing false portrayals to spread

³ Margaret Jane Radin, *Market-Inalienability*, 100 Harv. L. Rev. 1849, 1852 (1987).

globally within minutes. Even more severe is the use of deepfakes in involuntary pornography, where faces and bodies are inserted into sexual content without authorization. Victims are subjected to humiliation, symbolic violence, and lasting psychological trauma, with some cases linked to revenge porn⁴ and targeted harassment.

The political sphere presents another alarming dimension in the discussion of deepfakes. Synthetic identity technologies can be weaponized to fabricate speeches, interviews, or actions attributed to candidates or public officials, creating entirely false narratives that appear authentic to the average viewer. These manipulations distort democratic debate by introducing fabricated information into the public sphere, often at moments of heightened political tension. Once such content circulates widely, the damage is difficult to reverse. Even when the fabrication is later exposed, the initial impact on public perception may persist, eroding trust in institutions and weakening the credibility of legitimate political communication.

In the commercial environment, synthetic identity introduces a different but equally serious set of risks. Deepfakes can be used to falsely associate individuals with products, services, or commercial endorsements they never approved. This practice misleads consumers, manipulates market behavior, and undermines the integrity of commercial transactions. In more severe cases, the consequences may extend to public health and safety. If a deepfake is used to promote a harmful or unregulated product, consumers may rely on the fabricated endorsement and expose themselves to significant risks. The reputational harm to the individual whose identity was misused is compounded by the broader harm inflicted on the public.

These examples illustrate that the legal challenges posed by synthetic identity cannot be confined to the realm of personal rights. They implicate collective interests, including the preservation of democratic discourse, the reliability of commercial communication, and the stability of public trust. The central challenge for legal systems is to design frameworks capable of recognizing the unique nature of synthetic identity, classifying its risks, and establishing mechanisms of accountability for its misuse. This requires a combination of doctrinal clarity, technological understanding, and institutional readiness, so that the law can respond effectively to the rapidly evolving landscape of artificial identity manipulation.

In confronting these risks, legal systems must engage in the delicate task of balancing principles. Joseph Raz reminds us that “legal principles have certain relative ‘weights.’ Some have greater weight than others. This dimension of weight determines what ought to be done in cases to which

⁴ Revenge porn refers to the distribution of intimate images or videos without the victim’s consent, usually by former partners, with the intent to cause embarrassment or retaliation.

conflicting principles apply”⁵. Applied to deepfakes, this means weighing freedom of expression against the protection of honor and dignity. It also requires considering contractual and liability regimes that can address abusive uses, ensuring rapid removal of harmful content before damage becomes irreversible, particularly in sensitive contexts such as electoral campaigns.

Ultimately, deepfakes cannot be regarded as neutral technological innovations. They represent a dangerous frontier of legal and social vulnerability, where the line between legitimate representation and manipulative distortion becomes perilously thin. This is precisely where the comparative study of Brazilian and Chinese law gains relevance. Brazil emphasizes constitutional guarantees of personality and honor, while China has introduced specific legal provisions targeting the digital synthesis of images and voices. Each system, with its own instruments and emphases, seeks to confront the challenge of framing synthetic identity within its normative order, offering valuable insights into how law can adapt to protect human dignity in the digital age.

II. CHINESE LAW

A. PERSONALITY RIGHTS IN THE 2021 CIVIL CODE

The confrontation of risks brought by deepfakes within the Chinese legal system reveals a normative strategy that combines general civil norms with recent administrative regulations, reflecting the State’s concern with aligning the protection of personality rights to the preservation of social stability. The underlying logic is clear: while there is recognition of the need to protect individual dignity against digital manipulations, there is also a parallel effort to prevent the proliferation of synthetic identities from undermining public trust and social order.

The promulgation of the 2021 Civil Code was a decisive milestone in this process. For the first time, China structured a robust chapter dedicated to personality rights, incorporating provisions that directly engage with the challenges posed by artificial intelligence and digital manipulation. Article 1018 inaugurates this protection by enshrining the right of likeness, defining it as “an external image reflected on a certain carrier by means of video, sculpture, or painting”⁶. This definition, seemingly traditional, acquires unprecedented relevance in the context of deepfakes, as it establishes a normative parameter for cases in which faces are inserted into false

⁵ Joseph Raz, *Legal Principles and the Limits of Law*, 81 *Yale L.J.* 823, 830 (1972).

⁶ Civil Code of the People’s Republic of China art. 1018 (promulgated May 28, 2020, effective Jan. 1, 2021) (P.R.C.).

audiovisual materials without authorization.

Article 1019 deepens this protection by expressly prohibiting violations of the right of likeness through “defamation, defacement, or forgery by information technology”⁷. The inclusion of this last expression demonstrates the legislator’s sensitivity to new forms of violation, recognizing that technological manipulation is not merely an extension of traditional fraud but an autonomous phenomenon requiring specific legal treatment. This provision grants the Chinese system a comparative advantage, offering courts a clear normative basis to classify deepfakes as civil wrongs without resorting to strained analogies.

Article 1020, in turn, introduces exceptions to the requirement of consent, permitting the use of image or voice in situations of public interest or informational necessity. However, Chinese jurisprudence has interpreted these exceptions restrictively, ensuring they do not become an open door for abuse. This judicial posture reveals a concern with preserving the essence of personality rights, reinforcing that individual identity cannot be trivialized in the name of vague collective interests.

The protection of voice provided in Article 1023⁸ is equally significant. By determining that voice protection shall follow, *mutatis mutandis*, the rules applicable to likeness, the legislator acknowledges that auditory identity is as vulnerable as visual identity. In an era of voice-cloning technologies capable of reproducing timbre and intonation with alarming precision, this normative equivalence proves indispensable for preventing financial fraud, political manipulation, and other forms of abuse.

Finally, Article 1032 enshrines the general right to privacy, functioning as an open clause to address unpredictable risks. This provision grants flexibility to the system, allowing courts to recognize violations of dignity and personal freedom even in situations not explicitly foreseen in earlier articles. Recent studies, such as *The Infringement of Deepfake Technology on Personal Privacy and Legal Protection*⁹, emphasize that this normative openness is essential given the speed at which deepfakes evolve, generating new forms of privacy violations, disruption of personal tranquility, and reputational harm.

Beyond the Civil Code, it is important to note that China complements this protection with administrative regulations specifically targeting

⁷ Civil Code of the People’s Republic of China art. 1019 (promulgated May 28, 2020, effective Jan. 1, 2021) (P.R.C.).

⁸ Civil Code of the People’s Republic of China art. 1023 (promulgated May 28, 2020, effective Jan. 1, 2021) (P.R.C.).

⁹ Mengqi Han, *The Infringement of Deepfake Technology on Personal Privacy and Legal Protection: A Discussion Based on Article 1032 of the Civil Code*, 41 J. Educ., Human. & Soc. Sci. (2024) (abstract), <https://pdfs.semanticscholar.org/1786/77ea3bbf08ceef700d35a5aa02822f7c35e2.pdf>.

generative artificial intelligence. Rules issued by the Cyberspace Administration of China (CAC) establish requirements of transparency, labeling, and accountability for platforms that produce or disseminate synthetic content. This combination of civil and administrative norms reveals an integrated approach: while the Civil Code protects individual rights, administrative regulations aim to control the technological ecosystem, imposing obligations on companies and preventing the mass dissemination of manipulated content.

In summary, the Chinese legal system constructs a normative framework that combines specificity with openness. On one hand, there are clear provisions that classify digital manipulation as a violation of personality rights; on the other, there are general clauses that allow the law to keep pace with technological evolution. This structure reflects an attempt to balance innovation and protection, individual dignity and social stability, offering a model that, although still under development, already appears more systematic than many Western legal systems.

B. ADMINISTRATIVE REGULATIONS

In addition to the provisions introduced in the 2021 Civil Code, China has moved swiftly to adopt administrative regulations specifically designed to address the risks posed by synthetic identity and deepfake technologies. These regulations complement civil law by imposing obligations on service providers and platforms, thereby creating a preventive framework that seeks to control the technological ecosystem itself.

The *Provisions on Deep Synthesis Internet Information Services*¹⁰, enacted in 2022, represent the first comprehensive attempt to regulate deep synthesis technologies at the administrative level. They require that all content generated through deep synthesis be accompanied by a visible label, ensuring that users can distinguish between authentic and synthetic material. This labeling requirement is crucial in combating misinformation and protecting individuals from unauthorized identity appropriation. The regulation also mandates that the consent of the person whose likeness or voice is reproduced must be obtained, reinforcing the principle of autonomy

¹⁰ Provisions on the Administration of Deep Synthesis Internet Information Services (2022) (P.R.C.). The Provisions are administrative regulations issued jointly by the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security. They constitute China's first comprehensive framework specifically targeting risks arising from AI-generated content, including deepfakes. The Provisions require service providers to implement labeling obligations for synthetic content, conduct security assessments, prevent the misuse of deep synthesis technologies, and ensure that individuals' likeness, voice, and personal data are not altered or generated without their consent.

enshrined in the Civil Code. Furthermore, it places responsibility on content distribution platforms, holding them accountable if they allow the circulation of inappropriate or harmful synthetic material. This provision reflects China's broader regulatory philosophy: platforms are not neutral intermediaries but active participants in maintaining social order.

Building on this foundation, the government introduced the *Interim Measures for the Administration of Generative Artificial Intelligence Services*¹¹ in 2023. These measures extend regulation to the broader field of generative AI, addressing not only deepfakes but also other synthetic outputs such as text, images, and audio. Providers offering generative AI services are required to adopt robust security safeguards, implement labeling mechanisms for AI-generated content, and actively prevent the production of false or harmful information. Importantly, the regulation also requires providers to obtain consent for the use of personal data in training AI models, thereby linking the regulation of generative AI to broader principles of data protection and privacy.

Together, these administrative measures illustrate China's preventive and systemic approach to synthetic identity. While civil law provides remedies for individuals whose rights have been violated, administrative law seeks to minimize the occurrence of violations by imposing obligations on the entities that develop and disseminate synthetic content. This dual structure - civil protection combined with administrative oversight - creates a more comprehensive framework than that found in many jurisdictions, where regulation often lags behind technological innovation.

In addition to the Civil Code provisions and the specific regulations on deep synthesis and generative artificial intelligence, China has also enacted a broader set of laws addressing network security and personal information protection. Among the most significant are the *Personal Information Protection Law (PIPL)*, the *Cybersecurity Law*, and the *Regulation on the Administration of Online Audiovisual Information Services*¹². Together, these instruments form a comprehensive regulatory ecosystem that situates the governance of synthetic identity within the wider framework of digital rights,

¹¹ Interim Measures for the Administration of Generative Artificial Intelligence Services (2023) (P.R.C.). The Measures are also regulations issued by the Cyberspace Administration of China to govern the provision of generative AI systems to the public. The Measures require providers to ensure the legality, accuracy, and safety of generated content; prevent the production or dissemination of false, harmful, or misleading information; implement data-protection safeguards; obtain consent before using personal data to train models; and establish mechanisms for content labeling, user complaint handling, and algorithmic transparency. The Measures complement the Provisions on Deep Synthesis Internet Information Services by extending regulatory oversight to AI systems capable of generating text, images, audio, and video autonomously.

¹² Han, *supra* note 9 (abstract).

data security, and online content management.

The *Personal Information Protection Law*, adopted in 2021, establishes detailed rules for the collection, storage, and use of personal data. Its relevance to deepfakes lies in the requirement that consent be obtained before personal information - including biometric data such as facial features or voice recordings - can be processed. This law therefore reinforces the principle that identity attributes are not freely available for technological exploitation but must be treated as protected personal assets.

The *Cybersecurity Law*, enacted in 2017, complements this by imposing obligations on network operators to safeguard data and prevent misuse. In the context of deepfakes, it provides a legal foundation for holding platforms accountable when synthetic content threatens national security, public order, or individual rights. Similarly, the *Regulation on the Administration of Online Audiovisual Information Services* requires platforms distributing audiovisual content to monitor and control the dissemination of harmful or illegal material, a mandate that directly applies to deepfake videos.

Taken together, these administrative regulations are not merely ancillary to civil law - they are central instruments in China's regulatory strategy. They embody a preventive philosophy: rather than relying solely on individuals to pursue remedies after harm has occurred, the State imposes proactive duties on platforms and AI providers. By requiring visible labeling of synthetic content, explicit consent for identity reproduction, and direct responsibility for distribution, China ensures that those who control digital ecosystems play an active role in mitigating risks.

This approach reflects a broader objective that goes beyond the protection of privacy, image, and voice. The ultimate aim is to safeguard social stability and reinforce public trust in digital communication. In the Chinese model, technological innovation is welcomed, but only under conditions that prevent its misuse from destabilizing society. The emphasis on preventive control - through labeling, consent, and accountability - illustrates the priority given to collective order and confidence in information systems, positioning China's regulatory framework as one of the most comprehensive responses to the challenges of synthetic identity worldwide.

C. JURISPRUDENTIAL TRENDS

In alignment with the provisions of the Chinese Civil Code and the administrative regulations discussed above, Chinese jurisprudence has begun to consolidate around several identifiable trends that reflect both the doctrinal foundations of personality rights and the broader policy objectives of the State. Three main tendencies can be observed. First, courts have consistently emphasized the protection of identity integrity, treating image and voice as

core attributes of personality¹³ that cannot be appropriated without consent. This approach underscores the recognition that identity is not merely a private interest but a fundamental component of human dignity. Second, exceptions to consent requirements have been interpreted narrowly, with judges limiting non-consensual use of likeness or voice strictly to cases of genuine public interest¹⁴, thereby preventing the dilution of personality rights. Third, jurisprudence has highlighted the importance of social stability and risk prevention, framing the regulation of deepfakes not only as a matter of individual protection but also as a collective security¹⁵ measure aimed at preserving trust in digital communication and safeguarding public order.

Concrete cases illustrate how these principles are applied in practice. In April 2023, the influencer CaroLailai discovered that her face had been inserted into a pornographic video through deepfake technology. The case triggered a police investigation into an illegal digital manipulation network and drew widespread attention to the dangers of identity abuse, particularly in the context of non-consensual sexual content. The incident underscored the vulnerability of public figures and the urgent need for legal mechanisms capable of responding to reputational harm and symbolic violence.

Shortly thereafter, in May 2023, businessman Guo, the legal representative of a technology company in Fuzhou, became the victim of a sophisticated fraud scheme. During a video call, his interlocutor used deepfake technology to impersonate a close friend, successfully convincing him to transfer 4.3 million yuan. This case highlighted the financial risks associated with synthetic identity, demonstrating how deepfakes can be weaponized to exploit trust in professional and personal relationships. It also revealed the difficulty of distinguishing authentic communication from manipulated content, even for experienced business professionals.

Together, these cases illustrate the dual dimension of Chinese jurisprudence on deepfakes, considering the protection of individual rights and the safeguarding of collective stability. Courts have shown a willingness to apply the Civil Code provisions on likeness, voice, and privacy in innovative ways, while also reinforcing the preventive objectives of administrative regulations. The emerging jurisprudence thus reflects a hybrid model, reactive in its remedies for victims, but preventive in its emphasis on deterrence and social order.

¹³ Supreme People's Court of China, Typical Civil Cases on Personality Rights Protection (Apr. 11, 2022), https://english.court.gov.cn/2022-04/12/c_768408.htm.

¹⁴ Andrea Liang, Navigating Public Personality Rights in China (Dec. 2, 2025), <https://cnipcase.com/navigating-celebrity-portrait-rights-in-china/>.

¹⁵ Emmie Hine & Luciano Floridi, New Deepfake Regulations in China Are a Tool for Social Stability, but at What Cost?, *Nat. Mach. Intel.* (2022), <https://www.nature.com/articles/s42256-022-00513-4.pdf>.

These episodes, along with others in recent years, have contributed to the consolidation of Chinese jurisprudence around the principle that the use of artificial intelligence to imitate, clone, or manipulate the image and voice of individuals constitutes a violation of personality rights, regardless of whether immediate economic loss can be demonstrated. This doctrinal stance reflects a broader understanding that identity attributes - such as facial likeness and vocal signature - are integral to human dignity and autonomy and therefore deserve protection even in the absence of quantifiable financial harm.

A landmark decision in 2024 by the Beijing Internet Court reinforced this position by ruling that the unauthorized imitation of voice through AI infringes upon personality rights linked to vocal identification¹⁶. The court explicitly grounded its reasoning in the Civil Code's provisions on image and voice, thereby extending traditional protections into the domain of synthetic identity. This case illustrates how Chinese courts are willing to adapt established legal principles to novel technological contexts, ensuring that the law remains responsive to emerging risks.

On another front, the Supreme People's Court included in its collection of typical cases matters involving voice cloning and face swapping, particularly in the context of cyberbullying and digital violence. By elevating these cases to the status of "typical," the Court signaled its intention to guide lower courts in applying personality rights to new forms of AI misuse¹⁷. This move demonstrates the judiciary's proactive role in shaping legal doctrine, ensuring consistency across jurisdictions, and emphasizing the seriousness of synthetic identity violations.

Further jurisprudence from the Beijing Internet Court has extended protection to AI-generated virtual images, imposing civil liability on providers that disseminate such content without consent¹⁸. This expansion is significant because it recognizes that synthetic identities need not be tied to existing individuals to warrant protection; even virtual likenesses created by AI can fall within the scope of personality rights when they are linked to identifiable persons or when their misuse causes reputational harm.

Taken together, these decisions illustrate the evolution of Chinese jurisprudence toward a comprehensive framework that encompasses violations arising from deepfakes and synthetic content under the heading of personality rights. The courts have demonstrated a willingness to interpret the Civil Code dynamically, applying its provisions to contexts unforeseen at

¹⁶ AI-Generated Voice Mimicry Infringes on Rights, *China Daily* (Apr. 24, 2024) (reporting a Beijing Internet Court decision).

¹⁷ SPC Releases Typical Cases on AI Voice, Face-Swapping & Cyberbullying, *China Justice Observer* (Jan. 2, 2023).

¹⁸ Early Jurisprudence from Beijing on the Intersection of AI and Personality Rights, *China IP Law Update* (Sept. 13, 2025).

the time of drafting.

This combination of civil norms, administrative regulations, and judicial practice reveals a holistic approach to synthetic identity in China. Identity is treated as a sensitive legal asset whose manipulation requires express consent, and whose circulation must be strictly controlled by platforms. The emphasis on preventive regulation, coupled with judicial recognition of personality rights, reflects a model that prioritizes both individual dignity and collective stability.

In the next chapter, attention will turn to Brazil, where similar challenges are confronted through distinct legal and jurisprudential instruments.

III. BRAZILIAN LAW

A. CONSTITUTION AND CIVIL CODE

Brazilian law approaches the phenomenon of deepfakes through a structure that is less explicit and less technologically oriented than the Chinese regulatory model. Instead of relying on detailed statutory provisions that directly address synthetic identity, Brazil depends on a combination of constitutional guarantees, civil law principles, and judicial interpretation. This means that courts often play a decisive role in shaping the legal response to deepfake-related harms, filling the gaps left by legislation that was drafted before the emergence of artificial intelligence capable of manipulating image and voice. Even so, the Brazilian legal system contains several normative instruments that, when read together, provide a coherent basis for the protection of personality rights against digital manipulation.

The foundation of this protection lies in the Federal Constitution. Article 5, items V and X¹⁹, establishes the inviolability of intimacy, private life, honor, and image, and guarantees the right to compensation for material or moral damages resulting from their violation. These constitutional provisions form the core of Brazil's approach to deepfakes. They affirm that image and voice are essential expressions of human dignity and therefore cannot be appropriated or distorted without consent. This constitutional protection applies across a wide range of contexts, including non-consensual pornographic deepfakes, political manipulation through synthetic videos, and commercial exploitation of a person's likeness in advertising or promotional materials.

¹⁹ Constituição Federal [C.F.] art. 5, V, X (Braz. 1988), https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Article 5 provides: "V – the right to reply is ensured, proportional to the offense, as well as compensation for material, moral or image damages; X – the privacy, private life, honor and image of persons are inviolable, and the right to compensation for material or moral damages resulting from their violation is ensured."

Because the Constitution recognizes personality rights as fundamental rights, any interference with image or voice through artificial intelligence is presumed to be unlawful unless justified by a legitimate legal basis. This gives courts a strong platform from which to impose liability on those who create, disseminate, or benefit from deepfake content. It also allows judges to adapt constitutional principles to new technological realities, ensuring that the protection of dignity remains effective even as digital tools evolve. In this way, the Constitution functions as both a shield for individuals and a guide for judiciary as it confronts the challenges posed by synthetic identity.

From another perspective, the Brazilian Civil Code provides an important normative foundation for addressing deepfakes, even though it does not expressly mention synthetic identity or artificial intelligence. Articles 11 to 21 regulate personality rights and affirm their inalienable and non-waivable character. These provisions establish that attributes such as name, image, and voice cannot be transferred, renounced, or commercially exploited without the express consent of the individual. This structure resembles, in certain respects, the protections codified in the Chinese Civil Code, although the Brazilian approach relies more heavily on general clauses and judicial interpretation. Within this framework, the digital manipulation of image, voice, or name without authorization constitutes a direct violation of personality rights. Courts may therefore grant both compensatory damages and injunctive relief, including orders for the immediate removal of the manipulated content and the cessation of its circulation.

Brazilian scholars have increasingly recognized that deepfakes represent a new and complex form of injury to identity. Because the Civil Code was drafted long before the emergence of artificial intelligence capable of generating synthetic images and voices, the task of adapting traditional legal categories to contemporary risks has fallen largely to legal doctrine and jurisprudence. Scholars argue that the principles governing personality rights already contain the conceptual tools necessary to confront deepfake-related harms, provided that they are interpreted in a technologically informed manner.

Among these scholars, Anderson Schreiber has been particularly influential. He argues that civil liability for damages arising from deepfake should be understood as a natural extension of the principles that already govern the protection of identity. According to his view, the interpreter must apply the Civil Code in a flexible and evolutionary way, recognizing that artificial intelligence introduces new modalities of harm that threaten the integrity of personal identity²⁰. This requires courts to adapt established doctrines, such as the right to image and the right to name, so that they remain

²⁰ Anderson Schreiber, Felipe Ribas & Rafael Mansur, *Deepfakes: regulação e responsabilidade civil*, 27 *Revista Brasileira de Direito Civil* 251, 270 (2021).

effective in the face of digital manipulation.

In this sense, the Civil Code functions as a living instrument. Although it does not explicitly regulate synthetic identity, its general principles allow the judiciary to respond to the challenges posed by deepfakes and to protect individuals against unauthorized digital reproduction of their identity.

B. SPECIFIC LAWS USED AS GROUNDS FOR JUDGING DEEPPAKES

The constitutional and civil foundations that structure the protection of personality rights in Brazil are reinforced by additional legislation that plays a central role in judicial decisions involving deepfakes. Among these laws, two stand out for their relevance and practical impact. The first is the General Data Protection Law, known as the LGPD, which was strongly influenced by the European General Data Protection Regulation and shares its objective of safeguarding personal data in all phases of processing. The LGPD introduces a specific and robust layer of protection by classifying biometric data as sensitive information. This category includes facial features, voice patterns, and other elements that artificial intelligence systems commonly used to generate synthetic identities. Because sensitive data can only be processed under strict legal conditions, any deepfake created without the explicit consent of the person whose identity is reproduced constitutes a violation of data protection rules.

This means that deepfake production and dissemination can simultaneously infringe personality rights under the Constitution and the Civil Code and also amount to unlawful processing of personal data under the LGPD. Those responsible for creating or circulating synthetic content may therefore face administrative penalties, civil liability, and in some cases, obligations to adopt corrective measures. The LGPD also imposes duties on data processing agents, including the need to implement security measures, maintain transparency regarding data use, and adopt governance practices that reduce the risk of misuse. These obligations extend to companies that develop artificial intelligence models, platforms that host or distribute content, and any entity that handles biometric data.

In this sense, the LGPD operates not only as an individual protection mechanism but also as a collective safeguard. By imposing preventive obligations on data controllers and processors, the law seeks to reduce the systemic risks associated with synthetic identity technologies. It encourages responsible innovation by requiring that artificial intelligence systems be designed and operated in a manner that respects privacy, autonomy, and informational self-determination. As a result, the LGPD has become one of the most important legal tools for addressing deepfake-related harms in Brazil, complementing constitutional and civil protections and providing courts with a clear normative basis for sanctioning unauthorized digital

manipulation of identity.

The Marco Civil da Internet, enacted through Law No. 12,965 of 2014, occupies a central position in the Brazilian regulatory landscape concerning digital rights. Although it was drafted before the emergence of deepfake technologies, it established principles that remain highly relevant for addressing the challenges posed by synthetic identity. The statute affirms the protection of privacy and the inviolability of intimacy in digital communications, and it also sets out rules for the liability of internet service providers. These provisions create a general framework that can be applied to deepfake cases, particularly when manipulated content is used to spread false information, influence public opinion, or interfere with electoral processes. In such contexts, deepfakes may be classified as forms of disinformation or as abuse of digital tools, which strengthens the argument for platform responsibility.

The Marco Civil establishes that platforms must respect fundamental rights and act with diligence when notified of illicit content. This includes the obligation to remove material that violates personality rights or that contributes to the spread of harmful misinformation. Courts have relied on these principles to require the removal of deepfake videos and to impose liability on intermediaries that fail to act promptly. The statute therefore provides an important legal basis for demanding accountability from platforms that host or disseminate synthetic content without adequate safeguards.

However, scholars have pointed out that the Marco Civil was not designed with artificial intelligence in mind. Emanuely Ignez Alves Silva and Filipe Eduardo Macedo Menezes argue that the statute lacks specific mechanisms capable of addressing the complexity of violations generated by deepfake technologies²¹. According to their analysis, the law does not offer detailed criteria for identifying manipulated content, nor does it impose technical obligations on platforms to detect or prevent the circulation of synthetic media. As a result, the legal system remains vulnerable to the increasing sophistication of artificial intelligence tools that can create highly realistic and difficult to detect fabrications.

This gap highlights the need for interpretative evolution and possibly legislative reform. While the Marco Civil provides a valuable foundation for protecting fundamental rights online, it does not fully anticipate the challenges posed by synthetic identity. Courts and policymakers must therefore adapt its principles to contemporary technological realities, ensuring that the protection of privacy, dignity, and democratic integrity

²¹ Emanuely Ignez Alves Silva & Filipe Eduardo Macedo Menezes, *Regulamentação dos deepfakes no Brasil: desafios jurídicos e soluções tecnológicas*, 1(1) *Revista Mundo em Movimento* 75 (2024).

remains effective in the face of rapidly advancing digital manipulation techniques.

C. JURISPRUDENTIAL TRENDS

Although Brazil does not yet have a large body of case law comparable to the extensive jurisprudence developed in China, its courts have begun to articulate more consistent and predictable understandings regarding deepfakes and the legal foundations applicable to them. The absence of explicit statutory provisions on synthetic identity has required judges to rely on constitutional principles, civil law doctrines, and analogies with existing categories of digital harm. As a result, Brazilian jurisprudence is gradually forming a coherent framework that treats deepfake-related violations as extensions of already recognized injuries to personality rights.

One of the clearest areas in which this trend appears is the treatment of pornographic deepfakes. Within the Brazilian legal system, the creation or dissemination of manipulated intimate videos or images is understood as a direct affront to personality rights, particularly the rights to image, intimacy, and human dignity. These rights are protected by Article 5, item X, of the Federal Constitution and by Articles 11 and 20 of the Civil Code. Courts have consistently held that the unauthorized exposure of a person's intimate representation, even when digitally fabricated, produces moral harm and violates the core of personal autonomy.

Although there are still few decisions that explicitly mention deepfakes, Brazilian courts have relied on established jurisprudence concerning revenge pornography and the non-consensual disclosure of intimate images. These precedents provide a strong analogy, since both involve the unauthorized circulation of content that affects the victim's dignity and social reputation. Higher courts have recognized moral damages in such cases and have imposed civil liability on individuals who create or share the content, as well as on platforms that fail to remove it after notification.

This approach reflects a broader judicial understanding that deepfakes, even when technologically sophisticated, do not fall outside the scope of existing legal protections. Instead, they represent a new modality of an already familiar category of harm. Judges have therefore applied traditional principles in a technologically informed manner, emphasizing that the digital nature of manipulation does not diminish its capacity to cause psychological, social, and reputational damage.

As jurisprudence continues to evolve, Brazilian courts are likely to refine these analogies and develop more explicit criteria for evaluating deepfake-related claims. For now, the emerging trend demonstrates a commitment to protecting personality rights in the digital environment and to ensuring that artificial intelligence does not become a tool for violating dignity or intimacy.

The Superior Court of Justice of Brazil has already articulated an important doctrinal foundation for addressing deepfakes by analogy with cases involving the unauthorized dissemination of intimate images. In a leading decision, the court held that personality rights are violated even when the victim's face is not visible in the material. The court emphasized that the absence of facial identification does not diminish the gravity of the violation, since the core harm lies in the unlawful exposure of intimacy and the resulting affront to dignity²². According to the court, a woman who becomes a victim of revenge pornography experiences a clear and undeniable breach of her personality rights, regardless of whether her face can be recognized. This reasoning is directly applicable to pornographic deepfakes, which reproduce the same type of injury by fabricating intimate content that falsely associates the victim with sexual acts. Technology does not reduce the harm but rather intensifies it by creating realistic fabrications that can spread rapidly and remain online indefinitely.

In the political sphere, Brazilian jurisprudence has developed more quickly due to the existence of specific regulations governing the use of artificial intelligence in electoral contexts. The Superior Electoral Court issued Resolution No. 23.732 of 2024, which establishes detailed rules for the use of AI in electoral propaganda. The resolution expressly prohibits the creation or dissemination of deepfakes involving candidates, political parties, or public authorities. It also requires that any content produced or altered by artificial intelligence be clearly labeled so that voters can identify its synthetic nature. Failure to comply with these requirements may result in civil and electoral liability, including fines, removal of content, and even the annulment of candidacies in cases of serious misuse.

These rules have enabled courts to decide cases involving political deepfakes with greater uniformity. Judges can rely on the explicit prohibition contained in the resolution, which functions as a clear legal basis for sanctioning those who produce or disseminate manipulated political content. The regulatory approach resembles, in certain respects, the administrative measures adopted in China, where platforms and content creators are required to label synthetic material and are held responsible for its misuse. In Brazil, the TSE resolution plays a similar preventive role by imposing obligations on political actors and digital platforms to ensure transparency and to prevent the manipulation of public opinion through artificial intelligence.

Together, these developments show that Brazilian jurisprudence is gradually constructing a coherent framework for addressing deepfakes. Courts have adapted existing principles to new technological realities and have relied on electoral regulations to address political manipulation.

²² Superior Tribunal de Justiça [STJ], REsp No. 1.660.168/RJ, Rel. Min. Nancy Andrighi (Oct. 17, 2017) (Braz.).

Although the system is still evolving, it demonstrates a growing capacity to protect personality rights and democratic integrity in the face of synthetic identity technologies.

Brazilian electoral courts have increasingly confronted situations in which deepfakes were used to distort public debate, defame candidates, or manipulate voter perception. In these cases, the judiciary has consistently recognized that the use of synthetic audiovisual content violates electoral law and undermines the principles that guide the democratic process. Among these principles, probity and equality of conditions among competitors occupy a central place. Deepfakes are understood as tools capable of artificially altering the informational environment, creating false impressions about candidates, and compromising the fairness of electoral competition.

Based on these principles, a Regional Electoral Court in northeastern Brazil judged a case involving a deepfake with superimposed manipulated audio in the voice of a candidate, holding that “*the artificial superimposition of audio onto the video, attributing false and defamatory statements to the pre-candidate, together with the caption ‘Rios Family NEVER AGAIN’, constitutes an offense to honor and an attempt to negatively influence voters. (...) The use of a manipulation technique capable of altering the audiovisual content amounts to unlawful early negative electoral propaganda*”²³. As it can be seen from the decision, judges emphasized that the use of a technique capable of altering audiovisual content amounted to unlawful early negative propaganda, since it introduced fabricated information into the electoral arena before the official campaign period. This decision illustrates how Brazilian electoral courts are adapting traditional principles to the new challenges posed by artificial intelligence.

The judiciary has also begun to address the growing practice of voice cloning. Courts have frequently granted urgent injunctions to halt the misuse of voice, grounding their decisions in personality rights and in the rules of the LGPD, which classifies biometric data as sensitive information that requires special protection. These injunctions reflect the understanding that vocal identity is an essential component of personal autonomy and that its unauthorized reproduction can cause immediate and irreparable harm.

Although case law is still developing, Brazilian courts already recognize that the unauthorized use of an individual’s voice through artificial intelligence constitutes a violation of the rights to image and voice. This recognition has led to the imposition of civil liability and to the adoption of urgent measures aimed at preventing the continuation of the violation. In cases involving the use of voice databases to generate synthetic speech, courts have stressed that companies employing such technologies must act with

²³ Tribunal Regional Eleitoral do Maranhão [TRE-MA], Recurso Eleitoral No. 0600260-92.2022.6.10.0000 (2022) (Braz.).

diligence. In cases of unauthorized use of artificially generated voice by third parties through voice databases, jurisprudence emphasizes the obligation of reparation and diligence by those who employ the technology, stressing that *“the company that used the technology to generate a voice similar to that of the plaintiff cannot exempt itself from liability. The lack of diligence in the use of AI that infringes personality rights, especially vocal identification, may result in legal consequences, including the obligation to compensate for damages”*²⁴.

Taken together, these developments show that the Brazilian legal system, although still adapting to the rapid evolution of artificial intelligence, already possesses a set of robust instruments capable of addressing the challenges posed by deepfakes. Through constitutional guarantees, civil law protections, data protection rules, and electoral regulations, Brazil articulates both individual protection and the defense of democratic order.

Having outlined the legal frameworks of both countries, the next chapter will present a comparative analysis of different issues involving deepfakes and how the legal bases of Brazil and China apply to each of these points.

IV. COMPARATIVE ANALYSIS

A comparative analysis of the legal systems of China and Brazil reveals two markedly different approaches to the regulation of deepfakes and the protection of synthetic identity. These differences are not limited to the presence or absence of specific legislation. They reflect broader structural characteristics of each legal order, including the degree of legislative centralization, the role of administrative regulation, and the extent to which courts are expected to fill normative gaps. By examining these elements side by side, it becomes possible to identify the strengths and limitations of each model and to draw insights that may guide future regulatory developments.

In China, the legal response to deepfakes is anchored in a clear and direct normative foundation. The 2021 Civil Code expressly incorporates the concept of forgery by information technology in Article 1019, which provides an explicit legal basis for addressing digital manipulation of image and voice. This provision is complemented by a series of administrative regulations specifically designed to govern artificial intelligence and deep synthesis technologies. These regulations require labeling of synthetic content, mandate consent for the use of identity attributes, and impose duties on platforms to prevent the circulation of harmful or misleading material. As a result, Chinese courts operate within a structured and coherent framework that allows them to apply personality rights directly to cases involving

²⁴ Tribunal de Justiça de São Paulo [TJSP], Proc. No. 1002353-33.2023.8.26.0100 (2023) (Braz.).

synthetic identity. The jurisprudence that has emerged is therefore relatively uniform, with courts consistently recognizing deepfakes as violations of image, voice, and privacy rights.

Brazil, by contrast, relies on a more fragmented and less explicit set of legal norms. Protection against deepfakes must be constructed from the combined interpretation of constitutional guarantees, civil law provisions, and data protection rules. None of these instruments contains a specific reference to synthetic identity or digital manipulation, with the exception of the regulation issued by the Superior Electoral Court, which applies only to political propaganda. This means that Brazilian courts must engage in more extensive interpretative work, drawing analogies with existing categories such as revenge pornography, unauthorized use of image, or unlawful processing of biometric data. As a result, the jurisprudence is less uniform and varies depending on the context in which the deepfake is used. Pornographic deepfakes tend to be analyzed through precedents on non-consensual intimate exposure. Political deepfakes rely on the specific TSE resolution. Voice cloning cases often depend on the LGPD and its classification of biometric data as sensitive information.

This comparison shows that China benefits from a more centralized and technologically oriented regulatory structure, which provides clarity and predictability. Brazil, on the other hand, compensates for the absence of explicit legislation through judicial creativity and the flexible application of general principles. Each system offers valuable lessons. China demonstrates the advantages of explicit statutory guidance, while Brazil illustrates how broad constitutional and civil principles can be adapted to new technological realities.

Another important point of contrast between the two systems concerns the regulation of artificial intelligence itself. China adopts a preventive and comprehensive regulatory stance, marked by the use of administrative rules designed to anticipate risks before they materialize. The Chinese model seeks to ensure social stability and public order by imposing obligations on platforms, requiring labeling of synthetic content, and establishing mechanisms for rapid intervention when digital manipulation threatens individual rights or collective interests. This approach reflects a broader philosophy in which the state plays a central role in supervising technological development and in shaping the conditions under which artificial intelligence can be deployed.

Brazil, by contrast, presents a more fragmented and reactive regulatory landscape. The country does not yet have a unified legal framework specifically dedicated to artificial intelligence. Instead, the legal response to deepfakes and other forms of digital manipulation emerges primarily through judicial interpretation and through the application of the LGPD, which

governs the processing of personal data. This reactive posture means that courts often serve as the primary arena for resolving disputes involving synthetic identity. Judges must interpret general principles and adapt them to new technological contexts, which leads to a more contentious and case-driven model of enforcement. In this scenario, Bill No. 2,338 of 2023, currently under consideration in the Brazilian National Congress, represents an attempt to create a specific regulatory framework for artificial intelligence. The proposal is inspired by European models and seeks to introduce risk-based regulation, but its approval and implementation remain uncertain.

A further distinction arises from the political and social context in which deepfakes circulate. Brazil has experienced intense electoral clashes and heightened political polarization in recent years. Elections occur every two years, which creates a constant cycle of political communication and public debate. In this environment, deepfakes have become powerful instruments of disinformation, capable of influencing voter perception and damaging the integrity of the electoral process. The Brazilian Constitution assigns significant weight to freedom of expression, which complicates the task of balancing this right with the need to protect honor, image, and democratic order. Courts must navigate this tension carefully, ensuring that restrictions on synthetic content do not unduly limit legitimate political speech.

In China, the situation is different. Freedom of expression is subordinated to values of public order and social stability. This hierarchy allows the state to impose stricter restrictions on the use of digital manipulation technologies and to intervene more decisively when synthetic content threatens social harmony. As a result, the Chinese regulatory model faces fewer constitutional obstacles when limiting the circulation of deepfakes.

Finally, both China and Brazil lack a consolidated doctrinal test for artistic or satirical uses of deepfakes. This absence is significant because synthetic media is increasingly used in cultural, humorous, and creative contexts. Neither legal system has yet developed clear criteria for distinguishing legitimate artistic expression from harmful manipulation. The lack of guidance creates uncertainty for creators, platforms, and courts, and highlights the need for further theoretical and jurisprudential development. As artificial intelligence continues to evolve, both countries will need to refine their legal frameworks to address the complex and often ambiguous boundaries between creativity, parody, and identity violation.

CONCLUSION

The comparative analysis of the legal systems of China and Brazil regarding the treatment of deepfakes demonstrates that, although these countries emerge from profoundly different legal traditions, both recognize that synthetic identity technologies pose a concrete and growing threat to

personality rights. Image, voice, and privacy are particularly vulnerable in an environment where artificial intelligence can reproduce, distort, or fabricate identity attributes with increasing realism and speed. Despite their differences, both jurisdictions acknowledge that deepfakes challenge the very foundations of personal autonomy and informational self-determination.

China responds to this challenge through a structured and coordinated normative strategy. The inclusion of the expression forgery by information technology in the 2021 Civil Code, combined with a series of administrative regulations specifically aimed at artificial intelligence, creates a legal environment that is both preventive and comprehensive. Chinese regulations emphasize labeling, consent, and platform responsibility, and they impose duties on providers to monitor and control the circulation of synthetic content. This model allows for rapid and centralized responses to new risks, and it reflects a broader regulatory philosophy that prioritizes social stability and collective security.

Brazil, by contrast, relies on a more dispersed set of legal instruments. Protection against deepfakes is grounded in open constitutional clauses, in the general principles of the Civil Code, and in the rules of the LGPD. These instruments provide important safeguards, but they do not contain explicit provisions addressing digital manipulation technologies. As a result, Brazilian courts must adapt traditional legal categories to the new reality of synthetic identity. Jurisprudence plays a central role in shaping the legal response, whether by analogizing pornographic deepfakes to revenge pornography, applying electoral regulations to political deepfakes, or invoking data protection rules in cases of voice cloning. This reactive and case-driven model allows for flexibility, but it also produces fragmentation and legal uncertainty.

The differences between the two systems reveal both strengths and limitations. China operates with a preventive and vertically coordinated model that facilitates the containment of systemic risks. However, this approach may restrict creative, artistic, or experimental uses of digital manipulation, since the regulatory framework tends to prioritize control over expressive freedom. Brazil, on the other hand, adopts a reactive and contentious model that leaves more room for balancing freedom of expression with personality protection. Yet this flexibility comes at the cost of slower institutional responses and a lack of uniformity in case law, which can be problematic in a context where deepfakes spread rapidly and unpredictably.

Neither system, however, has yet developed a fully satisfactory theoretical and practical framework. Although the Chinese model appears more aligned with the demands imposed by synthetic identity technologies, especially due to its rapid administrative responses, both countries still face

unresolved challenges. These include the need for clearer criteria for artistic, satirical, and journalistic uses of deepfakes, the development of objective parameters for assessing damage, and the creation of liability models that integrate creators, platforms, and artificial intelligence providers. Effective solutions will require not only legal innovation but also technological safeguards, such as verification tools, labeling mechanisms, and authentication systems capable of distinguishing real content from synthetic fabrications.

Ultimately, the comparative analysis shows that the protection of identity in the age of artificial intelligence is not merely a legal issue. It is a broader societal and civilizational imperative. China and Brazil are moving toward this goal through different paths, but both recognize that safeguarding human dignity in the digital era requires a combination of legal, technological, and institutional strategies. The evolution of these frameworks will determine how effectively societies can confront the challenges posed by deepfakes and preserve the integrity of personal identity in an increasingly synthetic world.

REFERENCES

- Bryson, Joanna J., Mihailis E. Diamantis & Thomas D. Grant, Of, for, and by the People: The Legal Lacuna of Synthetic Persons, 25 *Artificial Intelligence & Law* 273 (2017).
- Civil Code of Brazil (Código Civil), Lei No. 10.406, de 10 de janeiro de 2002 (Braz.).
- Civil Code of the People's Republic of China (promulgated May 28, 2020, effective Jan. 1, 2021) (P.R.C.).
- Constituição Federal [C.F.] (Braz. 1988).
- Han, Mengqi, The Infringement of Deepfake Technology on Personal Privacy and Legal Protection: A Discussion Based on Article 1032 of the Civil Code, 41 *J. Educ., Human. & Soc. Sci.* (2024), <https://pdfs.semanticscholar.org/1786/77ea3bbf08ceef700d35a5aa02822f7c35e2.pdf>.
- Hine, Emmie & Luciano Floridi, New Deepfake Regulations in China Are a Tool for Social Stability, but at What Cost?, *Nat. Mach. Intel.* (2022), <https://www.nature.com/articles/s42256-022-00513-4.pdf>.
- Huang, Jiaying, The Protection of Personal Privacy in “Deepfake”: Risks and Countermeasures, *J. East China Univ. Sci. & Tech.*, no. 1, at 129–30 (2022).
- Kuźnicka-Błaszowska, Dominika & Nadiya Kostyuk, Emerging Need to Regulate Deepfakes in International Law: The Russo–Ukrainian War as an Example, 11 *J. Cybersecurity*, art. tyaf008 (2025), <https://doi.org/10.1093/cybsec/tyaf008>.
- Lei No. 13.709, de 14 de agosto de 2018 (Braz.) (Lei Geral de Proteção de

- Dados Pessoais).
- Liang, Andrea, Navigating Public Personality Rights in China (Dec. 2, 2025), <https://cnipcase.com/navigating-celebrity-portrait-rights-in-china/>.
- Radin, Margaret Jane, Market-Inalienability, 100 Harv. L. Rev. 1849 (1987).
- Raz, Joseph, Legal Principles and the Limits of Law, 81 Yale L.J. 823 (1972).
- Schreiber, Anderson, Felipe Ribas & Rafael Mansur, Deepfakes: regulação e responsabilidade civil, 27 Revista Brasileira de Direito Civil 251 (2021).
- Schwartz, Paul M., Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056 (2004).
- Shi, Dongxiu, On the Legal Regulation of Deepfake for Face Swap, 5 Shanghai Law Research Collection 77–78 (2021).
- Silva, Emanuely Ignez Alves & Filipe Eduardo Macedo Menezes, Regulamentação dos deepfakes no Brasil: desafios jurídicos e soluções tecnológicas, 1(1) Revista Mundo em Movimento 75 (2024).
- Solum, Lawrence B., Legal Personhood for Artificial Intelligences, 70 N.C. L. Rev. 1231 (1992).
- Stone, Christopher D., Should Trees Have Standing? Toward Legal Rights for Natural Objects, 45 S. Cal. L. Rev. 450 (1972).
- Superior Tribunal de Justiça [STJ], REsp No. 1.660.168/RJ, Rel. Min. Nancy Andrighi (Oct. 17, 2017) (Braz.).
- Supreme People's Court of China, Typical Civil Cases on Personality Rights Protection (Apr. 11, 2022), https://english.court.gov.cn/2022-04/12/c_768408.htm.
- Tribunal de Justiça de São Paulo [TJSP], Proc. No. 1002353-33.2023.8.26.0100 (2023) (Braz.).
- Tribunal Regional Eleitoral do Maranhão [TRE-MA], Recurso Eleitoral No. 0600260-92.2022.6.10.0000 (2022) (Braz.).
- Zhu, Minming, The Application Risks of “AI Face Swap” Technology and Its Regulatory Guidance, Hangzhou Internet Court (June 22, 2024) (WeChat post).

Jose Humberto Deveza Assola

Brazilian intellectual property attorney with eight years of experience handling complex IP disputes, currently pursuing an LL.M. in Intellectual Property and Innovation Policy at Tsinghua University. Professional practice and academic research focus on IP litigation and innovation, with particular emphasis on standard-essential patents (SEPs), fair, reasonable, and non-discriminatory (FRAND) licensing, trademarks, copyright, creative industries, and emerging technologies.

Email: humbertodeveza@gmail.com

ORCID iD: <https://orcid.org/0009-0006-1271-5304>