

Regulating the Unregulatable: The Crisis of Image and Voice Protection in the Age of AI

by Rafał Wozba

A Comparative Analysis of Japanese Legislative Initiatives and the EU Legal Framework

ABSTRACT:

The rapid adoption of Artificial Intelligence has outpaced global legislative frameworks, creating a significant gap in the protection of individual rights. This paper examines the recent April 2026 advisory panel by the Japanese Ministry of Justice regarding civil liability for deep-fakes and compares it with the European Union's Digital Services Act (DSA). It is going to be argued that current "notice and takedown" mechanism introduced in DSA is insufficient for non-public figures and that a shift toward strict platform liability, ensuring genuine legal security in the digital age, should be the envisaged solution.

KEYWORDS: AI Regulation, Deep-fakes, Japan-EU Legal Relations, Digital Services Act, Personal Image Rights, Platform Liability.

The Legislative Crisis: Global Law in the Age of Artificial Intelligence

The development of artificial intelligence (AI) tools is triggering a profound regulatory crisis for global legislation. Legal frameworks, intended to respond to changes in the world around us, are unable to keep up with the rapid adoption of AI solutions.

A clear example of the above is the growing volume of fake and manipulated content in recent years, which aims to gain an advantage at the expense of others, stir up public anxiety and trigger tensions. This primarily refers to materials published on social media that have become a part of everyday life. This problem especially concerns content widely known as "deepfakes".

On April 24, 2026, the first panel on civil liability for the unauthorized use of an individual's image and voice was held at the Ministry of Justice of Japan. The main focus of the discussion was whether current regulations are sufficient to protect people from deepfakes and synthetic voice generation. This article presents a summary of the initial findings from the Japanese panel and examines current solutions in the European Union, as well as how existing laws can be adapted to this evolving reality.

Evolving Legal Frameworks and the Protection of Personal Rights

The ministerial panel emphasized the feasibility of utilizing existing legal frameworks rather than creating a new regulation dedicated to protection against AI-generated content that violates the rights of third parties. The initial findings concluded that the protection of individual rights should be based on the construct of personal and image rights. The panel intends to develop guidelines to facilitate the interpretation of provisions in cases concerning violations committed via AI, which is expected to streamline the redress process for the injured parties. Furthermore, the possibility of assigning the rights to seek damages to talent agencies was discussed, which could assist artists and performers in the practical enforcement of their rights.

While the proposals aimed at streamlining judicial proceedings should be considered appropriate, the legislative deliberations should also focus on the root of the problem, namely the passivity of AI tool providers and social media platform owners. It is these entities that enable users to generate content that violates the rights of third parties.

In essence, the direct perpetrator of the violation, the entity publishing generated content without the consent of the authorized party, is able to create such material only by virtue of the tools provided to them. It is no coincidence that the issues surrounding the rapid proliferation of infringing content in the digital environment intensified once free or subscription-based generative tools were made available to the general public. Today, creating manipulated audiovisual material requires nothing more than a smartphone with internet access, a concept that remained purely theoretical just five years ago.

The negligible cost of producing deepfake content for the unauthorized exploitation of third-party rights (such as voice or image) creates an extremely favorable risk-reward ratio. Identifying the individuals behind social media profiles that share illegal content is significantly hindered, which in turn complicates filing a lawsuit and conducting legal proceedings. Consequently, the infringer, who may also derive financial gain from such content, sees no reason to cease their activities, operating with a sense of impunity fueled by systemic inefficiencies.

European Union's "Notice and Takedown" Mechanism

The issue is not an isolated phenomenon in Japan - it is a subject of global debate, particularly within the European Union. With the introduction of the Digital Services Act (DSA), the EU formalized the "notice and takedown" mechanism. This allows any user to report illegal content through a user-friendly interface that every online platform is obligated to provide.

However, this system is inherently subjective, as individual users apply different criteria for what they consider illegal. This is where the obligations of platform owners become crucial, as they are required to analyze every report and promptly decide on the matter of the violation. This arises from the way platform liability is structured—namely, through a "negative" liability model. This means that the service provider is not liable for illegal content unless they have actual knowledge of it and fail to take immediate action to remove or disable access to it.

User reports therefore serve as the trigger upon which the subsequent liability of online platforms may depend. Unfortunately, the current "notice and takedown" system fails to effectively protect an individual's image and voice. This is due to the fact that a platform's obligation to react ends where a report requires an in-depth legal analysis. In other words, an online platform is obligated to take immediate action only in cases of manifest violations that do not require detailed and multifaceted investigation.

Ineffectiveness of The Current Legal Solutions

The issues mentioned above pose a significant hurdle for the average user, who bears the burden of proof in demonstrating that their image or voice was unlawfully used in AI-generated content. If the injured party is not a public figure (e.g., an actor or singer), the platform lacks the means to effectively verify the report. In such instances, the violation is not considered manifest and requires in-depth analysis, which effectively excludes the platform's liability regime. Consequently, the service provider has neither a legal nor an economic incentive to provide meaningful assistance to the complainant.

One potential solution would be the introduction of enhanced verification standards, such as biometric authentication, to facilitate the confirmation of the complainant's identity. However, this approach is costly and raises significant concerns regarding privacy rights and data protection. While the EU's out-of-court dispute settlement mechanism theoretically enables the most crucial outcome for the injured party—the swift removal of content—it suffers from fundamental flaws that, in practice, hinder the effective protection of an individual's image and voice.

In the author's view, the possibility of directing claims for image or voice infringement directly against AI system providers and online platforms should be considered. Given the dynamics of AI adoption, it is the owners of these tools who exercise a decisive influence over the nature of the output generated in response to user prompts. Since safeguards already exist to block responses that violate certain areas of law, the question remains: why do providers not implement mechanisms that significantly limit the creation of deepfakes and the generation of synthetic voices strikingly similar to those of real individuals?

Even assuming that this proposal is highly idealistic, it is justified to consider the introduction of a strict liability framework (liability based on risk). In such a model, an online platform could be held liable for content generated and published using the tools it provides. Consequently, the injured party would face no difficulty in identifying the defendant's identity, which would significantly facilitate legal proceedings and enhance legal certainty. Such liability on the part of platforms would not preclude their right of recourse against the user directly responsible for the infringement. However, the risk of the infringer's anonymity and the primary burden of identification would be shifted from the injured party to the online platform.

Conclusion

Regardless of the current legal solutions in Japan or the European Union, the mere fact that this issue is being explicitly addressed marks a significant milestone. It paves the way for the future development of robust systems designed to safeguard individual rights against the challenges posed by the rapid evolution of artificial intelligence. When we think about today's market, it is easy to see that companies - especially those operating at scale - are no longer confined to a single country or organizational model. Intercultural collaboration has become a reality. A particularly relevant example is the economic relationship between Poland and Japan, which has become an increasingly important component of broader bilateral relations, combining advanced technology with distinct approaches to communication and work organization. As this cooperation continues to develop, the ability to build relationships based on mutual understanding becomes ever more important.

About the author:

Rafał Wozba is a final-year law student at the University of Warsaw. His professional practice is centered on the TMT sector, with a particular focus on copyright, advertising, and media law. His academic interests revolve around the legal implications of the evolution of generative artificial intelligence and its impact on the protection of individual rights.