Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Meloni case has shown how unprepared Europe is for the deepfake era

On 5 May, Italian Prime Minister Giorgia Meloni posted an AI-generated image of herself in underwear on X and Facebook profiles.

The picture was fake; it had circulated on Italian networks for days, and Meloni chose to share it herself with the comment: "In recent days, several fake images of me have been circulating, generated using artificial intelligence and passed off as real by some overzealous opponents. I must admit that whoever created them ... even improved my appearance quite a bit. But the fact remains that, in order to attack and spread falsehoods, people are now willing to use absolutely anything. Deepfakes are a dangerous tool, because they can deceive, manipulate and target anyone. I can defend myself. Many others cannot."

The incident itself is not surprising. In 2024, Meloni sued two men for €100,000 in compensation for deepfake pornographic videos using her image, which were posted on an American pornographic platform. The court proceedings are ongoing.

What is new this time is not the content itself, but the way it spread: no longer through the periphery of the Internet, but via major platforms, algorithmic recommendations, and users who share the content without any verification.

The difference between 2024 and 2026 is not only technological; it is also political and cultural. This kind of content is gradually ceasing to be a scandal and is becoming a standard method of political attack.

When a tool becomes a political weapon

Applications for generating fake images now work on mobile phones, are easy to use, cost only a few euros per month or are completely free, and the quality has reached a level where distinguishing an authentic photo from AI-generated content without specialised tools is no longer reliably possible.

The American organisation American Sunlight Project identified more than 35,000 examples of deepfake content depicting 26 members of the US Congress, 25 of whom are women.

> For victims, the consequences are almost always severe, regardless of their political power, financial resources, or level of protection

Research has shown the same pattern for years: women in public office are disproportionately more likely to be targets of non-consensual deepfake content than their male counterparts.

This is no longer a matter of isolated incidents, but a recognisable method of political pressure designed to make public engagement more costly, aggressive, and personally destructive.

The price for those who create such content is virtually non-existent. For victims, the consequences are almost always severe, regardless of their political power, financial resources, or level of protection.

Brussels is responding to a scandal, not a problem

A day after Prime Minister Meloni's announcement, on 6 May, the European Parliament and the Council of the EU reached an agreement to ban so-called ‘nudification’ apps as part of a review of the AI Act.

The ban applies to AI systems whose primary purpose is to generate non-consensual sexually explicit images or videos of identifiable persons, with a compliance deadline of 2 December 2026.

At the same time, the application of the rules for high-risk AI systems has been postponed again to December 2027 for stand-alone systems and to August 2028 for AI tools integrated into other products.

The AI Act was passed in 2024. The ban on one of its most dangerous practical applications comes two years later. That time gap reveals much about how European regulation works: it is mostly reactive, driven by public scandal, and far less anticipatory.

An important exception was added to the agreement under industry pressure. The ban will not apply to models with "effective security measures".

> The EU AI Office will have the right to access the internal practices of AI system providers

What exactly constitutes effective measures, and who will assess them, remains unclear. Responsibility has been transferred to national regulatory bodies and the new EU AI Office, which will not be operational until August 2026.

This is where the main problem with the European approach begins. As with the GDPR, the legislative framework exists, but enforcement has been postponed.

The EU AI Office will have the right to access the internal practices of AI system providers, and a spokesperson for the European Commission said the institution would "if necessary" provide access to the models.

That statement allows for broad interpretation and weak application. It is this gap between formal authorisation and political willingness to enforce it that often becomes the greatest weakness of European digital regulation.

Enforcement is split between European institutions and national regulators – the same model that has repeatedly caused slow implementation, differing interpretations, and significant gaps in oversight within the EU.

The first serious test will be the case of xAI's Grok, which generated explicit images of real people without meaningful restrictions and introduced protective measures only after a public scandal.

Elections precede regulation

Germany and Sweden will hold elections in 2026. The ban on 'nudification' apps will not be in force during these campaigns. Mandatory watermarking, labelling video as AI-generated, will also not yet apply. Tools originating outside the EU's jurisdiction will, in practice, remain beyond the reach of European regulation.

In the final stages of election campaigns, when propaganda efforts are at their peak and there is little time to verify content, this regulatory gap provides an opportunity for manipulation.

The same pattern has already been observed during election cycles in the US, UK, Pakistan and Bangladesh. There is no compelling reason for Europe to expect a different scenario.

The EU has banned only a narrow segment of the problem, delayed the implementation of key rules, and left enforcement to an institution that has not yet begun operating

This is why Meloni's court proceedings from 2024 could have a much greater practical impact than European regulation itself.

If the Italian court upholds the high compensation and clearly establishes criminal liability for non-consensual deepfake pornography, the case could set an important precedent for courts throughout Europe.

Platforms generally respond more quickly to financial risk than to regulatory principles. This has already been demonstrated by the first major fines under the GDPR and the initial significant sanctions under the DSA.

Only when digital manipulation becomes financially and legally costly do companies begin to change their behaviour.

Meloni's action succeeded in shifting the issue of deepfake content from a technological discussion to the political centre of the European debate.

However, this communication effect does not change the basic fact: the EU has banned only a narrow segment of the problem, delayed the implementation of key rules, and left enforcement to an institution that has not yet begun operating.

Meanwhile, the rules are still set by American tech companies and tools that largely remain outside European jurisdiction. Past experience shows that these companies almost never act preventively; they respond only when the political or financial cost becomes excessive.

Therefore, the question is no longer whether deepfakes will become a systematic political tool in upcoming election cycles, as this is already happening.

The real question is who will bear responsibility when the consequences become serious, and whether the regulatory system will once again lag behind a problem that has already escalated.