

Policy Brief

Targeted and Ignored

Sexualised Deepfakes of Women MEPs and the Failure of Platform Responses

Benjamin Shultz, Stefan Heumann, Torben Klaus & Vivien Benert

Executive Summary

AI-generated non-consensual intimate imagery (AIG-NCII), colloquially known as deepfake pornography, is a systemic threat to women in European politics. The results of our new external audit measuring the exposure of members of the European Parliament (MEPs) in AIG-NCII are clear: the EU's current rules governing this harm are not stopping it. Examining hundreds of websites known to host or produce AIG-NCII, we find that one in six women MEPs are depicted in or associated with deepfake pornography. Like in our recent audit of the exposure members of the EU's national parliament face, we find that exposure to this harm falls overwhelmingly on women, is amplified by institutional visibility and affects all major groups across the political spectrum.

The current EU framework fails these women for three reasons. It acts only after the harm is done; it depends on victims finding AIG-NCII and filing reports themselves; and its strongest duties apply only to the largest platforms, while most of the harm sits on small, often offshore sites. Neither the Digital Services Act (DSA), the General Data Protection Regulation (GDPR) nor the impending Digital Omnibus on AI set a fixed deadline for platforms to remove violative content, whereas the newly enacted rules in United States (US) and the United Kingdom (UK) now require removal of AIG-NCII within 48 hours.

We recommend the EU move regulation upstream:

- **Enforce the “nudifier” app ban fully.** The upcoming Omnibus regulations should also cover gateway sites and the misuse of open-weight models.
 - **Require automatic de-indexing.** Search engines should remove all results for a domain once authorities have seized it.
 - **Hold the supply chain accountable.** App stores, payment providers, hosts and domain registrars should have due-diligence duties, using the Digital Fairness Act and a “failure to prevent” liability on the British model.
 - **Take the burden off victims.** Regulators should act on their own initiative, collective redress should be strengthened, and success should be measured by prevention, not takedowns.
-

50 MEPs affected by deepfake pornography

Our new analysis shows 50 MEPs—46 women and four men—to be depicted in or associated with deepfake pornography. This translates to roughly one in six women MEPs. This analysis examined an expanded sample of domains known to host deepfake pornography, “celebrity leaks,” and inappropriate candid images of women in public life. We searched the names of all 720 MEPs against 200 of these websites using a Google Custom Search engine. An analysis of the types of exposure MEPs faced from this search can be seen in the table below.

Code	State	Interpretation	MEP Count
C	Manipulated imagery actively hosted	Depiction exists and is live	8
G	Gateway website	AI-generation tools linked on a page named for an individual directly, with their bio and/or portrait	22
S	Name-specific result, indexed and findable	Expressed demand, currently served with an active named page, raw material, or a request in a forum	11
S-	Name-specific result, indexed, <i>not</i> findable	Records persist, remaining indexed, while content may have been removed, deleted, or never existed (e.g., misuse of an elected official’s name for search optimization purposes)	37
R	Domain removed	Still-indexed records of known origin; e.g. domain seizure	26

Eight MEPs, all women, were found to be depicted outright with manipulated, sexualized imagery using their likeness. We identified the likeness of 22 MEPs on so-called “gateway” sites (see Figure 1 below), directly linking a nudifier app next to their biography, social media accounts and/or official portraits. As well, we identified 46 MEPs impacted by search index persistence: 37 MEPs for whom results remain indexed despite linking to content that is no longer findable online, and 26 MEPs for whom search results persist even after confirmed domain seizure. (The distinction we draw between results coded S- and R is pinpointing with confidence what content used to exist, as well as the exact source of its confirmed removal.) To that end, search results for 10 MEPs yielded positive hits for CFAKE, a domain that was [seized nearly four months ago](#), in June 2026. Results from domains [seized recently by New York State prosecutors](#) also appeared in search results returned by Google for the names of 10 MEPs.

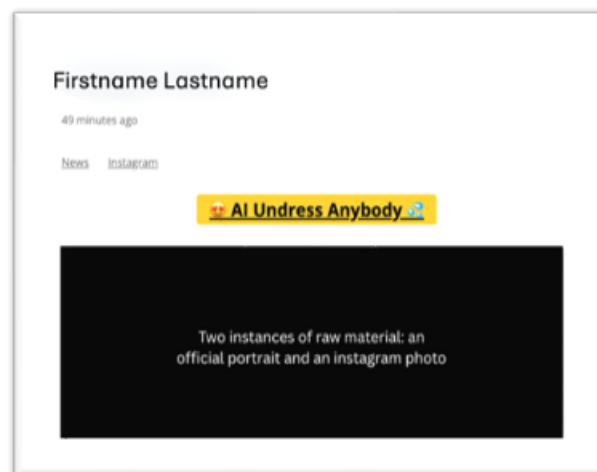


Figure 1: An example of a “gateway” site, showcasing an elected official’s portrait next to a link to an AI nudifier app.



Also noteworthy is the continued cross-partisan impact of exposure that MEPs faced. Like our first study examining members of the EU's national parliaments, all major party groups from across the political spectrum in the European Parliament have been impacted. This includes: Greens/EFA, EPP, The Left, Renew, S&D, ESN and Patriots.

Methods

Between 26-30 September we queried the names of 720 sitting members of the European Parliament against 200 domains known to host deepfake pornography, "celebrity leaks," and inappropriate candid images of women in public life (e.g., upskirting). We constructed 10 Google Custom Search engines, assigning 20 domains to each, and leveraged Google's application programming interface (API) to pull down results. Our methodology was designed to be non-intrusive: we neither interacted with any producers or distributors of depictive content, nor downloaded or stored depictive content at any stage. Each valid 'hit' from the API was coded into one of five categories capturing: 1) whether AIG-NCII was actively hosted; 2) whether a generation tool was linked next to a named individual's biographical information, social media accounts and/or official portrait 4) whether an indexed search record persisted, with or 5) without a named webpage or a production request specific to a parliamentarian; or 6) whether a domain had been formally removed by authorities.

Policy Analysis: Addressing Symptoms, Lacking Enforcement

Background: misogyny in society

Sexualized deepfakes are not a new technological phenomenon, so much as a new tool for an old problem: violence against women. The pattern our analysis documents has the same misogynous roots as harassment, stalking and intimidation offline. Women in public life are targeted far more often than men. Their risk of exposure grows with their visibility and power. The aim is to humiliate, silence and push them out of public roles. [Hate Aid's research](#) shows that 22% of the women in politics affected by digital violence considered a complete withdrawal from political work. Generative AI hasn't created this hostility, but it has made it cheaper, faster and harder to trace. Regulating the technology alone will therefore fall short unless it is part of a wider strategy against gender-based violence, both online and offline.

Legal bans on deepfakes are important but ineffective

Several countries have already adopted AIG-NCII-specific legislation, including [Australia](#), [France](#), [Italy](#) and the [United States](#). This sends an important message that the generation of deepfake pornography without consent is considered a serious crime. But where such laws are already in place, there are still challenges in properly deterring this crime. Perpetrators are often difficult to identify, reporting processes put a high burden on victims, while the technical infrastructure to produce and distribute illegally generated deepfake content remains in place or—as [early evidence](#) may suggest—goes underground. All the while, nudifier apps [continue to make millions](#) of Euros every year, taking advantage of the boundaryless nature of the internet.



Another example of failed GDPR enforcement

In the EU, the GDPR is very clear. A sexualised deepfake of an identifiable MP or MEP involves the processing of personal data with no lawful basis. Art. 9 (special-category data) explicitly prohibits such data processing. Gateway sites that combine biographies, photos and social media account links are unlawful processing too. Here, the problem is not the GDPR itself but its proper enforcement.

- **Complaints:** it largely depends on the victim noticing and complaining, but the brief shows the harm is often unseen until it has spread.
- **Who is liable:** operators are anonymous or offshore, and the obligation for non-EU operators to appoint an EU representative in Art. 27 is rarely enforceable.
- **De-indexing:** if at all, the right to erasure works one URL and one person at a time. Our finding of delayed de-indexing finding shows records outlive takedowns.

The DSA fails women targeted by deepfake pornography

The DSA's strongest tool doesn't reach where the harm is. The risk assessment duty described in Art. 34 explicitly covers gender-based violence and effects on civic discourse. As demonstrated in our audit of the EU's national parliaments, a 33x gender gap that grows with political seniority fits both. But that duty only applies to very large platforms and search engines. The 200 domains, including gateway sites and nudifier apps, we have examined are small, often registered or hosted outside the EU, and covered only by the reactive notice-and-action procedure (Art. 16). Moreover, in cases where nudifier apps are advertised or made available for download, only very large online platforms must declare which entities maintain these apps (Art. 26). This said, where the DSA does apply, it does not provide relief. Take, for example:

- **Google:** Google Search is a designated very large online search engine. Our initial analysis found 47 records still indexed more than a month [after the domain CFAKE was seized](#). We replicated this finding upon audit of MEPs' exposure, nearly four months after the seizure. That's the kind of risk the mitigation duty Art. 35 is meant to cover. Where hosting and indexing run on separate clocks, an undefined removal window means the slowest system sets the pace.
- **X:** Art. 34 requires a risk assessment before high-impact features launch. Yet the Commission only opened proceedings against X on 26 January 2026, after Grok had generated an [estimated three million sexualised images](#). That's enforcement after the harm has occurred, not preventive risk assessment.
- **Meta:** Art. 26 requires very large online platforms to provide the "the natural or legal person on whose behalf the advertisement is presented." Research shows, however, that even in cases where such disclosures are provided, e.g., in cases of nudifier apps, [they are often falsified](#) with limited or no oversight from Meta, while both Meta and said nudifier apps continue to make millions of Euros per year.

No immediate deadline anywhere in EU law

Neither the DSA nor the GDPR sets a time limit for removal. Art. 16 of the DSA requires platforms to act "in a timely manner." Turning to the GDPR, erasure requests under Art. 12 can run up to one month, but are extendable to three, while Art. 17 separately requires erasure "without undue



delay.” In practice the content stays up while the clock is undefined. Other jurisdictions have moved farther than European law in this regard. The [US TAKE IT DOWN Act](#) requires covered platforms to remove non-consensual intimate imagery, including synthetic imagery, within 48 hours of a valid request, with a notice-and-removal process mandated from May 2026 and FTC enforcement behind it. An [amendment](#) to the UK Online Safety Act Crime and Policing Bill outlines a similar 48-hour window for removal upon receipt of a valid takedown request. A fixed deadline matters here more than in most content cases.

Our analysis documents harm that comes from production

In every single case of AIG-NCII we examined involving a national MP or an MEP, the victim posted nothing, the raw material was an official portrait or a public social media photo, and the tools used to create the content sat upstream of any platform. In this setting, the shortcomings of existing frameworks are threefold. Firstly, they are reactive: they act after a depiction exists. Secondly, they are individualised: they depend on the victim complaining. Thirdly, they are limited by platform size: the systemic duties only bind the largest players.

Policy Recommendation: Moving Upstream

Ban on nudifier apps: first step in the right direction – but far from enough

The [Digital Omnibus on AI ban on nudifier apps](#) applies in cases of:

“placing AI systems on the EU market with the purpose of creating such content [...‘depicting the intimate parts of an identifiable person, or them engaged in sexually explicit activities, without that person’s consent’]; placing them on the EU market without reasonable safety measures to prevent such creation; and deployers using these systems for the purpose of creating such content.” ([EU Parliament](#)).

Within the context of the language that will come into effect on 2 December, we recommend the following steps:

Accountability at the product level, whatever the provider’s size. Open questions include enforcement capacity for dealing with small or open-source platforms, grappling with providers and users of such platforms residing outside the EU and open-weight models being misused on machine learning exchanges, like [HuggingFace](#) and [CivitAI](#), to facilitate local, offline deepfake AIG-NCII production. Individuals’ likenesses [have been exploited](#) using open-weight models on such platforms. We argue this misuse provides evidence for assessing existing safety measures as unreasonable and insufficient.

Treat gateways as “deployers.” We argue that gateways listing the personal information and non-nude portraits of elected officials, linking directly next to them to a banned nudifier app serve no legitimate purpose other than promoting the creation of AIG-NCII, and should be therefore actioned as deployers in accordance with the Omnibus.

Treat timely de-indexing as a “reasonable safety measure.” Automatic and collective de-indexing after an AIG-NCII domain seizure can be, for example, supported by the GDPR’s right to be

forgotten (Art.17) or the DSA's risk-identification (Art. 34) and risk-mitigation duties (Art. 35), instead of individual erasure requests. The delay between content or domain deletion and de-indexing is [well-researched](#) outside of our audits of national MPs' and MEPs' exposure and, in the case of AIG-NCII, simply should not entail a many-months-long process. Search providers must also ensure that reuploads of non-consensual material are automatically removed.

Examine the production chain's "reasonable safety measures." Payment processors, app stores, content delivery networks, web hosts, domain registrars and web privacy services should face due-diligence duties towards nudifier apps, gateway websites and the like. These services [profit](#) off the creation of AIG-NCII yet face no responsibility for their role in supporting the creation and distribution of such content.

Shift the burden away from victims. That means regulators acting on their own initiative, collective redress (GDPR Art. 80, DSA Art. 86) and measuring pre-emptive enforcement actions rather than counting post-hoc takedowns.

Enhance enforcement capabilities. To ensure effective oversight, Member States must significantly increase the resources allocated to regulators to meet their obligations under Art. 50 DSA and Art. 70 AI Act. At EU level, an [independent enforcement agency](#) should be established to pool resources and prevent political interference.

Increase deterrence through personal liability. Nudifier apps are part of a lucrative ecosystem, in which regulatory penalties are often merely a calculated business expense. We argue that senior decision makers should be held [personally liable](#) for the systemic harm caused by their AI models, particularly if gross negligence or intentional noncompliance can be proven.

Criminalise non-consensual deepfake creation. Current criminal laws target the distribution of deepfakes, not their creation. Closing this gap through a harmonised legal framework across all Member States would enable law enforcement to intervene earlier, provide clear legal grounds for seizing offending software, and eliminate the loophole by which perpetrators claim that they never published the material.

The Digital Fairness Act: fixing the gaps within current regulatory frameworks

The European Commission's forthcoming Digital Fairness Act, expected by the end of 2026, offers a rare chance to close several gaps in the AIG-NCII production chain that our findings expose. Because the Digital Fairness Act targets unfair commercial practices and harmful design in digital markets, it is the natural place to address much of the enabling infrastructure of AIG-NCII. It could prohibit the marketing and sale of tools built to create AIG-NCII, place clear duties of care on the intermediaries that profit from them and give consumer protection authorities enforcement powers that do not depend on victims coming forward one case at a time. Unless the Digital Fairness Act fills these gaps, the burden of responding will keep falling on those who are targeted, not on the companies whose services make the abuse possible.

Learn from Britain: adopt the concept of "failure to prevent"

It is not simply the app developer or website owner, wherever they are in the world, that should be held accountable. We must not forget the platforms upon which AIG-NCII is hosted, the app



stores that make it available at the click of a button, the search engines that return links to it, and the payment processors that facilitate its profitability. If they fail to act in preventing this harm, they need to be held liable.

There are several examples of how Britain has put the “failure to prevent” approach into law: the Bribery Act 2010 (s.7), the Criminal Finances Act 2017 (s.45–46, failure to prevent the facilitation of tax evasion), and the Economic Crime and Corporate Transparency Act 2023 (ECCTA), whose failure-to-prevent-fraud offence (s.199) has been in force since 1 September 2025. ECCTA also reformed the identification doctrine (s.196), making a company liable for economic crimes committed by its senior managers acting within the scope of their authority. The Crime and Policing Act 2026 has since extended this rule to all criminal offences.

Contact Person at Agora Digitale Transformation



Benjamin Shultz

Data Fellow

Fellow.Shultz@agoradigital.de