

**What European legislation  
regarding cyber violence  
against women and girls?**

**our recommendations  
for further action**



# **NON-CONSENSUAL SHARING OF INTIMATE IMAGES (NCII) IN EUROPE:**

## **PREVALENCE, HARMS AND THE CASE FOR HARMONISED LEGAL RESPONSES**

# CONTEXT

The non-consensual sharing of intimate images (NCII) has emerged as one of the **most pervasive and harmful forms of cyber violence against women and girls in Europe**. This form of abuse, often referred to as “image-based sexual abuse” involves the distribution or threat of **distribution of intimate material without the consent of the person depicted**. It represents a serious violation of privacy, dignity and sexual autonomy, and its impacts extend far beyond the digital sphere.

Recent evidence underscores the scale of the problem. In Italy, a national study among young adults identified **NCII victimisation as a growing phenomenon**, strongly associated with intimate partner violence (Morelli et al., 2023, Computers in Human Behavior Reports).

The psychological and social consequences are severe. **Survivors frequently experience humiliation, anxiety, depression and post-traumatic stress**, particularly when intimate material remains accessible online (Henry et al., 2023, Frontiers in Psychology, PMC 10239214).

Many also face **secondary victimisation when seeking justice** or attempting to have the content removed.

Legal responses to NCII remain **fragmented** across the European Union. While some Member States have introduced specific offences (such as France, Germany or Spain), others continue to rely on general privacy or defamation laws, leaving **gaps in protection and inconsistent access to justice**.

**Directive 2024/1385 on combating violence against women and domestic violence represents a major step forward** by explicitly criminalising “non-consensual sharing of intimate or manipulated material”, however, further harmonisation and coordinated implementation remain necessary to ensure equal protection for victims throughout the Union.

**As NCII continues to expand across platforms and borders, the European Union faces a critical moment to establish a coherent legal and policy framework. This note explores the prevalence, harms and policy gaps surrounding NCII, and outlines recommendations for a harmonised European response grounded in human rights and feminist principles.**

# Non-consensual sharing of intimate material

A European framework still incomplete

**The Digital Services Act (DSA) contains ambiguous wording and uneven regulation:**

**The removal of Article 24b, which provided for strict moderation rules—training of specialized moderators and rapid removal of violent or illegal content—represents a clear step backward.** From now on, these enhanced obligations only apply to Very Large Online Platforms (VLOPs), i.e., those with more than 45 million users, a figure that the platforms declare themselves.

**This approach poses several problems:**

- It allows certain platforms to deliberately underestimate their audience in order to avoid increased scrutiny;
- It ignores medium-sized and emerging platforms, even though many forms of cyber violence are also developing there.
- There is no proactive obligation for online platforms to detect illegal content. The result is a two-speed regulatory system that leaves a large proportion of users less protected against violent or illegal content.

**The Directive 2024/1385 also offers limited protection:**

**The Directive only penalizes the sharing of intimate images when they are made “public,” excluding so-called private online spaces.** Its recital 25 limits its scope to content that is automatically accessible, without human control, which excludes closed groups, forums, or accounts requiring a subscription. In practice, images circulating in WhatsApp chats, private forums, or protected accounts are therefore not covered by the text, even though these are spaces where such content is particularly shared. **On the internet, so-called “private” content can quickly become uncontrollable.** The artificial distinction made by the Directive ignores the reality of the digital world and weakens the protection of the right to privacy and dignity.

**The GDPR theoretically guarantees a “right to be forgotten,” but its enforcement remains ineffective:**

**The unauthorized dissemination of intimate content is not systematically perceived as manifestly unlawful, which slows down rapid responses from authorities or platforms.** The latter often apply the GDPR very restrictively: they sometimes refuse to remove content if the victim's name does not appear, or request a court order before taking action. This situation leaves an operational vacuum, where the protection of victims depends essentially on the goodwill of hosting providers. **In practice, the removal of intimate content shared without consent is slow, uneven, and often arbitrary.** Victims then suffer serious consequences: prolonged exposure of their privacy, ongoing harassment, blackmail, and extortion, as well as a veritable “social death” marked by isolation, job loss, or lasting damage to their reputation and psychological health.

## Regulation against online terrorism



The European Regulation on addressing the dissemination of terrorist content online (2021/784) requires the removal of reported content within one hour, provides for penalties for non-compliance, and obliges exposed platforms to put preventive measures in place.

This framework could serve as a model for combating the non-consensual sharing of intimate content by imposing **short deadlines, clear obligations, and appropriate tools on platforms.**

## our recommendations

- **Establish a binding injunction procedure** requiring hosting service providers to remove or block access to non-consensual intimate content within a maximum of 24 to 48 hours after notification by the competent authority.
- **Require platforms to provide immediate justification in the event of technical or operational impossibility** to comply with the injunction, in order to avoid unjustified inaction.
- **Designate platforms as “systemic risk” within the meaning of the Digital Services Act** if they host content such as pornographic websites and social networks frequently used for the dissemination of non-consensual intimate content. Impose specific preventive measures on these platforms, based on objective criteria such as receiving several removal orders over a defined period.
- **Require platforms to submit regular reports on the actions taken**, subject to review by a competent authority, which could impose additional measures in the event of failure to comply.
- **Include all platforms that allow the dissemination of sexual content among Very Large Online Platforms (VLOPs)** in order to impose increased obligations on them in terms of content control and systemic risk management.
- **Establish effective and proportionate sanctions not only against uncooperative digital platforms**, but also internet service providers (ISPs) that facilitate the dissemination of such content by neglecting their removal and prevention obligations.
- **Impose clear obligations on platforms to detect and remove implicit hateful content**, including through contextual and human moderation systems.

# our recommendations

- **Systematically train magistrates and law enforcement officers** on digital violence and gendered interpretations of online harassment.
- **Facilitate cross-border cooperation between judicial authorities and regulators** to ensure uniform enforcement across the EU.
- **Establish an independent monitoring mechanism** to verify the implementation of these obligations and sanction non-compliance.
- **Define common criteria for assessing “serious harm”** (e.g., duration, frequency, documented psychological impact) to avoid differing interpretations among Member States.
- **Ensure victims have access to rapid protection measures** (restraining orders, content removal) without requiring complex proof of the severity of the harm.
- **Broaden the definition of misogynistic hate speech** to include implicit, coded, or contextual remarks (such as memes).

## contacts

**Céline Piques**, spokesperson for Osez le Féminisme (OLF) : [piques.celine@gmail.com](mailto:piques.celine@gmail.com)

**Alyssa Ahrabare**, President of the French Coordination for the European Women's Lobby (CLEF):  
[alyssa.ahrabare.afev@gmail.com](mailto:alyssa.ahrabare.afev@gmail.com)



**OSEZ  
LE FÉMINISME** 



La Coordination Française  
pour le Lobby Européen des Femmes



EUROPEAN WOMEN'S  
**LOBBY**  
EUROPEEN DES FEMMES