SUPPORTING VICTIMS OF AI-GENERATED SEXUALLY EXPLICIT AND INTIMATE IMAGERY

How can the European Union translate the legal recognition of AI-generated sexually explicit and intimate imagery into an effective, coherent and victim-centred system of protection?

Melina Lepida

Contents

Executive Summary 2

Introduction – The emergence of AI-generated sexually explicit and intimate imagey 3

Context – How has the EU responded? 4

Research question 4

Methodology 5

Limitations of the Paper 5

Theoretical framework 5

Image-Based Sexual Abuse (IBSA): from ''revenge porn'' to a continuum of abuse. 5

Sexual privacy and autonomy 6

Victim harms 6

Victim-centred justice 7

Analysis - Assessing the EU framework for victim protection 7

The Directive on Combating Violence Against Women & DomesticViolence 7

The Digital Services Act 8

The Artificial Intelligence Act 9

Overall assessment: towards a coherent victim-protection framework 10

Recommendations 10

Establish a coordinated, single entry point pathway for victim protection 11

Decouple rapid content removal from criminal prosecution 11

Move from transparency towards prevention and safety-by-design. 12

Conclusion 13

Annexes 14

Glossary 14

References 15

Supporting victims of AI - generated sexually explicit and intimate imagery

How can the European Union translate the legal recognition of AI-generated sexually explicit and intimate imagery into an effective, coherent and victim-centred system of protection?

Executive Summary

AI-generated sexually explicit and intimate imagery, commonly known as "sexual deepfakes", is an emerging form of image-based sexual abuse and technology-facilitated gender-based violence. Due to the non-consensual creation, manipulation and dissemination of such imagery, the abuse not only violates the depicted person's sexual privacy, autonomy and dignity, but can also cause serious and multifaceted harms to victims, including at psychological, social, professional and existential levels. The phenomenon disproportionately affects women and girls, rendering it a widespread, deeply gendered issue.

Amid the growing challenges accompanying this form of abuse, the EU has taken significant steps to address AI-generated sexually explicit and intimate imagery in order to protect those who fall victim to it. This position paper examines whether the European Union's existing legal framework provides effective, coherent and victim-centred protection against this form of abuse, focusing principally on the Directive on combating violence against women and domestic violence, the Digital Services Act and the Artificial Intelligence Act.

The analysis argues that, despite substantial progress in the right direction, the EU framework remains promising but partial: the three legal instruments address different stages and actors of the abuse, but rather than working jointly, they largely operate in a fragmented and siloed way, thereby failing to provide victims with a coherent system of protection.

The paper therefore calls for a more coordinated and proactive EU response that puts victims' needs at its core, including by establishing a coordinated, one-stop pathway for reporting, removal, referral and support; ensuring rapid content-removal mechanisms that operate independently of criminal prosecution or conviction; and imposing stronger preventive and safety-by-design obligations on AI providers and online platforms.

Introduction

The emergence of AI-generated sexually explicit and intimate imagery

"Even if it's not real, it's incredibly difficult to explain to the whole world, because not everyone will believe you. I constantly worried about being recognised, followed, or ridiculed, and I just wanted to hide at home every day." (Association Concerning Sexual Violence Against Women [ACSVAW], 2025, para. 2). This is how Janice, a victim of AI-generated sexually explicit imagery described living with fake sexual images of herself published and circulated online – a reality shared by thousands of women and girls across the world.

A "deepfake" is defined as "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful" (Regulation (EU) 2024/1689, 2024, Art. 3(60)). When AI technologies are used to create sexually explicit or intimate representations of identifiable individuals without their consent, they become **the latest technological manifestation of image-based sexual abuse (IBSA)**. This phenomenon is referred to in a variety of ways across the literature, including as "non-consensual sexual deepfakes", "AI-generated image-based sexual abuse", "deepfake pornography" and "sexual digital forgeries". This paper uses the term "AI-generated sexually explicit and intimate imagery" to foreground the harm to victims and situate the abuse within the broader continuum of image-based sexual abuse

The technology is not entirely new. The first deepfakes were created in 2017 and were based on superimposing celebrity faces onto pornographic recordings (Pawelec & Łabuz, 2025). With the tools to create them becoming widely available, often being free of charge, and requiring little or no technical expertise to use (Security Hero, 2023), deepfakes are growing at a breakneck speed: **the number of deepfake videos online was estimated to have increased by 550% between 2019 and 2023** (Security Hero, 2023).The accessibility of the technology is striking: a 60-second sexually explicit deepfake can be created in less than 25 minutes using just one clear facial image, and it has zero financial costs (Security Hero, 2023).

The phenomenon is also deeply gendered. In 2023, deepfake pornography made up 98% of all deepfake videos online, while 99% of individuals targeted in deepfake pornography were women (Security Hero, 2023). AI-generated sexually explicit and intimate imagery can therefore be situated both within image-based sexual abuse and the broader phenomenon of technology-facilitated gender-based violence (TFGBV). Women and girls across generations, professions and geographies are increasingly targeted, resulting in severe, multifaceted and long-lasting harms (UN Women, 2026). The scale and severity of the phenomenon have led UN Women (2026) to describe it as a "global crisis" (para. 10).

Context

How has the EU responded?

Faced with these emerging challenges, lawmakers across Europe and beyond have increasingly taken steps to strengthen legal responses addressing IBSA (Panorama Global, 2023, p. 8). In the EU, three instruments are particularly relevant to addressing the issue.

The Directive on combating violence against women and domestic violence (VAW Directive) is the most important EU initiative in the fight against technology-facilitated gender-based violence. Proposed in 2022 and adopted in 2024, it is the first EU-wide binding legislation addressing multiple forms of sexualised and gendered harm, including the non-consensual sharing of sexual and intimate material, and setting minimum rules for criminal offences, victim protection, support services, prevention, and coordination across Member States (Directive (EU) 2024/1385, 2024). EU Member States must transpose the Directive into national law by 14 June 2027 (Directive (EU) 2024/1385, 2024, Art. 49).

Alongside it, **the Digital Services Act (DSA)** regulates online intermediary services, namely the online platforms where abusive content is shared, and provides mechanisms through which victims may seek action against illegal content (Regulation (EU) 2022/2065, 2022), while **the Artificial Intelligence (AI Act)** regulates the development and use of AI systems, including those used to create or manipulate deepfake images, audio or video (Regulation (EU) 2024/1689, 2024).

Two additional EU legal frameworks are also relevant: **the Victims' Rights Directive (VRD)**, which establishes minimum standards on the rights, support and protection of victims of crime and was recently revised in 2026 (Directive 2012/29/EU, 2012; Directive (EU) 2026/1472, 2026), and the **General Data Protection Regulation (GDPR)**, which may provide remedies where the abuse involves the unlawful processing of personal data (Regulation (EU) 2016/679, 2016). However, their role in addressing AI-generated sexually explicit and intimate imagery is less direct than that of the VAW Directive, DSA and AI Act.

Research question

Despite legal recognition, research demonstrates that victims of IBSA continue to face barriers to the rapid removal of content, effective redress, access to justice and appropriate support (Rackley et al., 2021, pp. 315–319; Panorama Global, 2023, pp. 9–10, pp. 33). The challenge is therefore whether this emerging EU framework can deliver the protection, redress and support victims need in practice. This position paper therefore asks:

How can the European Union translate the legal recognition of AI-generated sexually explicit and intimate imagery into an effective, coherent and victim-centred system of protection?

Methodology

This position paper draws on a qualitative review of academic literature, particularly feminist legal literature, EU legislation and policy documents, complemented by publications from NGOs and other civil society stakeholders, and selected victim-informed and media sources. Together, these provide a conceptual and victim-centred framework for assessing not only what the EU framework provides on paper, but how far it responds to victims' needs in practice.

Limitations of the paper

This position paper has several limitations. It is based on desk research rather than primary empirical research, and the evidence on victims' experiences draws largely on broader image-based sexual abuse (IBSA) literature, as research specifically addressing AI-generated sexually explicit imagery remains limited. The legal analysis focuses primarily on three EU instruments, while comparative examples from other jurisdictions are illustrative rather than systematic. Moreover, the EU legal framework is still evolving, particularly ahead of the June 2027 deadline for transposing the VAW Directive. Finally, the recommendations offer policy directions rather than detailed institutional or technical solutions, particularly regarding safety-by-design measures. Further research and consultation with victims, frontline professionals, regulators and technology providers would be valuable in assessing their practical implementation.

Theoretical framework

Image-Based Sexual Abuse (IBSA): from ''revenge porn'' to a continuum of abuse.

To assess the EU's legislative response, AI-generated sexually explicit and intimate deepfakes must first be understood within the broader phenomenon of image-based sexual abuse (IBSA).

McGlynn et al. (2017, pp. 27–31) developed the concept of IBSA partly because "revenge porn" is both narrow and misleading: "revenge" assumes a particular perpetrator motivation, while "porn" risks trivialising the conduct and obscuring its non-consensual nature. **The central issue is whether sexual or intimate imagery was created, altered, disclosed or threatened without consent,** violating the victim's dignity and sexual autonomy.

IBSA encompasses practices including the non-consensual creation or distribution of sexual or intimate images, sexualised photoshopping and voyeuristic image capture, understood as a "continuum" because of common features including sexualisation, coercion, harassment and violations of sexual autonomy (McGlynn et al., 2017, pp. 28–29).

Whichever means are used to fabricate an image or video, the victim's identity, likeness and sexual self are appropriated without consent. **AI changes the means of perpetration, but not necessarily the underlying nature of the abuse.** AI-generated sexually explicit and

intimate imagery can therefore be understood as a technologically facilitated manifestation of the broader continuum of IBSA.

Sexual privacy and autonomy

If the sexually explicit image is fabricated, however, an important question arises: what, precisely, has been violated?

Danielle Keats Citron's (2019) concept of sexual privacy provides a basis for answering this question. Sexual privacy concerns an individual's ability to control access to, and information about, their body, sexuality and intimate life, and is closely connected to autonomy, dignity and equality (p. 1874).

From this perspective, the harm caused by sexually explicit and intimate deepfakes does not depend on the disclosure of an authentic intimate image. By appropriating a person's likeness and constructing a sexual or intimate representation of them without consent**, deepfakes violate a person's ability to determine how their sexual identity is represented and perceived by others.** The violation lies in the absence of consent.

Victim harms

With the IBSA framework explaining the nature of the abuse and sexual privacy identifying what is violated, the next question concerns the effects of that violation on victims.

"Devastating, like it broke me" (McGlynn et al., 2021, p. 550), "It is so harmful and isolating" (p. 554) and "There's such a level of permanence which affects everything" (p. 552) are among the words used by victim-survivors in a cross-national study of the impacts of IBSA by McGlynn et al. (2021), in which 89% of the 75 participants were women (p. 547). Their accounts demonstrate that **the harms extend beyond psychological distress, affecting how individuals understand themselves, experience relationships and navigate everyday life.**

One particularly relevant dimension identified by McGlynn et al. (2021) is **constancy**: images may remain online and be redistributed long after their initial dissemination. Victims cannot know who has viewed an image, where it may appear next or whether further exposure will occur. As one victim explained, "you have the image in your head, and it revisits and it revisits and revisits. ... It haunts you" (p. 552).

This continuing threat can constrain victims' liberty, causing them to **limit their online presence, withdraw from social or professional activities and organise everyday life around avoiding further exposure.** Some described how the abuse had "narrowed down [their] world", making it "small and claustrophobic" (p. 556). Drawing on Stark, the authors highlight that **understanding harm requires looking not only at what is done to victims, but also at what the abuse stops them from doing** (p. 556). The harm therefore lies not only in psychological effects, but in restricting a person's ability to participate freely in everyday life.

Victim-centred justice

What does meaningful justice and redress look like from the victim's perspective?

Rackley et al. (2021, p. 315) demonstrate that justice cannot be reduced to criminal prosecution and punishment. For many victims, **the priority is to "reclaim control" over their images, bodies and lives**, requiring a multi-stranded response extending beyond the criminal justice system.

Panorama Global's (2023) victim-informed research similarly calls for an integrated response combining effective laws with accessible legal assistance, victim support and mechanisms to report, remove and monitor abusive images (pp. 34–35). A victim-centred response must therefore consider not only whether abuse is criminalised, but whether the system as a whole can prevent abuse, stop ongoing harm, hold relevant actors accountable, provide meaningful redress and enable victims to regain control over their lives.

Analysis

Assessing the EU framework for victim protection

As explained in Chapter 2.1, EU protection against AI-generated sexually explicit and intimate deepfakes derives from complementary legal frameworks addressing different dimensions of the abuse. The following sections assess the contributions and limitations of the VAW Directive, DSA and AI Act, as the instruments most directly relevant to criminalisation, platform governance and AI regulation.

The Directive on Combating Violence Against Women and Domestic Violence (VAW)

While it does not specifically address IBSA as a distinct category of gender-based violence, **the VAW Directive provides the most direct EU legal recognition of the harm** by requiring Member States to criminalise the intentional production, manipulation or alteration and subsequent public dissemination through ICT of material making it appear that a person is engaged in sexually explicit activities, without their consent and where the conduct is likely to cause serious harm (Directive (EU) 2024/1385, 2024, Art. 5(1)(b)).

Despite this recognition, Article 5 contains significant limitations. First, its scope for manipulated material is narrow. Article 5(1)(a) protects "intimate parts" when dealing with authentic imagery, but the Directive does not use the same formulation for manipulated imagery. Instead, Article 5(1)(b) requires manipulated material to make a person appear to be "engaged in sexually explicit activities", potentially excluding AI-generated intimate nudity produced through nudification applications. Second, while Article 5(1)(b) covers the production or manipulation of sexually explicit material, it does so only where the material is subsequently made accessible to the public, rather than recognising its non-consensual creation as a standalone violation of sexual autonomy. Third, by requiring the conduct to be "likely to cause serious harm", it introduces an additional threshold, rather than recognising non-consensual interference with sexual autonomy as sufficient in itself.

The Directive nevertheless contains important victim-centred provisions. Article 25(1)(d) requires specialist support for victims of IBSA, including information on documenting the harm, available judicial remedies and ways of removing online content. Article 34(8) provides for digital literacy measures enabling users to identify and address cyber violence, seek support and prevent its perpetration. As Rigotti et al. (2024, p. 1487) argue, however, digital literacy should be accompanied by wider initiatives to increase public awareness and promote sexual consent in cyberspace.

The Directive also establishes a connection with online platform regulation. Under Article 23, Member States must provide measures for the prompt removal or restriction of access to online material, enabling competent authorities to issue binding orders to hosting service providers. **Yet victims' access to removal appears closely connected to criminal proceedings and ultimately conviction: Article 23(3) provides that removal orders are discharged where criminal proceedings do not result in a conviction.** As Rigotti et al. (2024, p. 1488) argue, it remains unclear whether such orders can be issued where there is no criminal report or prosecution, potentially leaving victims without effective removal and falling behind jurisdictions where civil or regulatory mechanisms enable removal independently of successful criminal prosecution.

The Digital Services Act

The Digital Services Act (DSA) **regulates the online environment through which harmful content is disseminated, amplified and potentially removed**, establishing mechanisms for reporting illegal content and obligations relating to platform accountability and systemic risks (Regulation (EU) 2022/2065, 2022). While the DSA does not explicitly use the term "deepfake", Article 35(1)(k) addresses "generated or manipulated" images, audio or video by identifying measures to make such content distinguishable.

More specifically, Articles 34 and 35 introduce an anticipatory approach requiring VLOPs and VLOSEs to assess and mitigate systemic risks arising from their services, including the dissemination of illegal content, impacts on fundamental rights and gender-based violence (Regulation (EU) 2022/2065, 2022, Arts. 34–35). As Jóźwiak and Ohnesorge (2026) argue, **the DSA thereby treats technology-facilitated gender-based violence as a question of platform governance:** the object of regulation is not simply harmful content but the platform systems and design choices that enable such harms to spread at scale.

Alongside its systemic-risk framework, the DSA provides several mechanisms through which victims may seek removal and redress:

- **Notice and action – Article 16:** requires hosting services to provide accessible mechanisms through which victims or other users can report illegal content, and to process notices in a timely, diligent, non-arbitrary and objective manner.
- **Internal complaints – Article 20**: enables victims whose notices do not result in action to challenge online platforms' decisions through an internal complaint- handling mechanism.

- **Out-of-court dispute settlement – Article 21:** enables victims to challenge content moderation decisions through certified out-of-court dispute settlement bodies, providing an escalation route where initial removal efforts are unsuccessful.
- **Trusted flaggers – Article 22:** requires online platforms to give priority to notices submitted by recognised trusted flaggers within their area of expertise and process them without undue delay.

These mechanisms provide victims with routes to seek platform action once AI-generated sexually explicit and intimate deepfakes have been disseminated online. Nevertheless, important limitations remain. First, the DSA does not itself determine whether a sexually explicit deepfake is illegal, but relies on substantive EU or national law (Regulation (EU) 2022/2065, 2022, Art. 3(h)). Second, its systemic-risk obligations apply only to VLOPs and VLOSEs. Third, **its individual reporting and redress mechanisms remain inherently remedial**, operating only after harmful content has already been disseminated.

The Artificial Intelligence Act (AI Act)

The AI Act establishes a unified legal framework for the development and use of AI systems through which deepfakes can be generated, thereby addressing a different stage of the abuse lifecycle (Regulation (EU) 2024/1689, 2024).

The Act defines a "deep fake" in Article 3(60**). Deepfakes are addressed primarily through the transparency obligations of Article 50**, rather than the high-risk regime.

In particular, Article 50(2) requires providers of AI systems generating or manipulating synthetic audio, image, video or text content to ensure that outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Under Article 50(4), deployers of AI systems generating or manipulating deepfakes must disclose that the content has been artificially generated or manipulated. Where deepfakes form part of an "evidently artistic, creative, satirical, fictional or analogous work or programme", the disclosure obligation is adapted so as not to hamper the display or enjoyment of the work. This reflects an attempt to balance transparency with fundamental rights, including freedom of expression, but arguably creates a potential legal grey area that malicious actors could exploit.

Despite representing a significant step towards digital accountability, Article 50 falls short in protecting victims of AI-generated sexually explicit and intimate deepfakes. **Transparency is not the same as protection.** Even where a sexually explicit deepfake is marked and disclosed as artificial, the victim's likeness has still been sexualised without consent and the violation of sexual autonomy has already occurred. Knowing that an image is AI-generated does not stop its creation or circulation, prevent the psychological, social and relational harms caused to victims, or provide them with a remedy. Labelling therefore risks reflecting what Habgood-Coote (2023, p. 14) describes as "technochauvinism": an approach that reframes social problems as technological ones and privileges technological solutions over their wider social dimensions. As Łabuz (2023, p. 278) argues, "transparency obligations are not a universal solution".

Lastly, despite growing awareness of AI's capacity to facilitate gender-based violence, the Act does not explicitly address the issue. Instead, Recital 136 frames risks associated with artificially generated or manipulated content primarily in terms of deception, manipulation, fraud, democratic processes and civic discourse (Regulation (EU) 2024/1689, 2024, Recital 136), leaving the specifically gendered and individualised harms of IBSA largely outside its focus.

Overall assessment: towards a coherent victim-protection framework

The EU has taken important steps towards addressing IBSA including AI-generated sexually explicit and intimate imagery, but it still falls short of providing an effective, coherent and victim-centred system of protection. This is because the three legal instruments discussed, which address different purposes and actors, each have their own limitations and do not function in an integrated way.

The VAW Directive, which criminalises the conduct of individual abusers and introduces measures to support victims of gender-based violence, is narrow in scope and its removal mechanisms are closely tied to criminal proceedings and conviction.

The DSA, which addresses the platforms where abusive content is shared, provides notice-and-action mechanisms, but these operate only after deepfake imagery has been uploaded.

The AI Act provides a transparency and detection layer, but focuses primarily on disclosure rather than prohibition and does not provide victims with mechanisms for removal, redress or support nor a robust safeguard against deepfakes. Its contribution to victim protection therefore depends on its interaction with the VAW Directive, the DSA and the wider EU framework. It relies heavily on technical fixes and does not go as far as introducing safety-by-design or prohibition measures to prevent the abuse.

Despite their collective potential, **none of these instruments alone provides a comprehensive protection pathway for victims.** As Rigotti et al. (2024, pp. 1472–1473) argue, the EU framework represents a "promising but partial approach" rather than a comprehensive solution.

For a victim-centred system of protection, the central challenge is to provide a coherent system.

Recommendations

To move beyond the current siloed approach and provide effective protection for victims of AI-generated sexually explicit and intimate imagery, **the EU should put victims' needs and journey at the heart of its response**.

Underpinning this response should be **the principle of assumption of victimhood**, whereby professionals take victims' reports seriously and operate on the assumption that victimisation has occurred, while allowing the facts to be properly investigated (Blondé et al., 2023, p. 12). This principle is paramount to a humane and fair path to a solution, and it should inform the

design and implementation of EU and national policies, ensuring that victims are treated with dignity, empathy and respect throughout their journey. It should also translate into appropriate victim-centred training for all professionals involved, including law enforcement, criminal justice and victim support professionals, to minimise secondary victimisation and ensure that victims can access protection, support and redress without experiencing further harm.

Guided by this overarching principle, three priority actions are recommended:

👉 Establish a coordinated, single entry point pathway for victim protection

Having to navigate separate AI, platform, criminal-law and support systems can be exhausting and disheartening for victims and risks causing further harm and secondary victimisation. Given the serious harms caused by AI-generated sexually explicit and intimate deepfakes, **the "do no harm" principle and minimisation of further harm should guide the EU's response** (Blondé et al., 2023, pp. 2, 13, 18).

The EU should therefore establish **a coordinated pathway, providing victims with a single entry point for reporting, takedown, referral and support**. Rather than necessarily creating a new EU authority, this could build on existing structures, such as the network of Digital Services Coordinators (European Commission, 2026), drawing inspiration from Australia's eSafety Commissioner and its Image-Based Abuse Scheme (eSafety Commissioner, n.d.). The designated mechanism should have trusted-flagger status under the DSA, enabling notices submitted on behalf of victims to receive priority treatment and be processed without undue delay (Regulation (EU) 2022/2065, 2022, Art. 22), while connecting victims with specialised support services.

👉 Decouple rapid content removal from criminal prosecution

While Article 23 of the VAW Directive requires Member States to ensure that certain illegal online content is promptly removed or access to it disabled, Article 23(3) provides that removal orders are discharged where criminal proceedings are terminated without a finding that an offence has been committed (Directive (EU) 2024/1385, 2024, Art. 23). This is an important limitation that may significantly restrict victims' access to redress (Rigotti et al., 2024, p. 1488), and Member States should address it when transposing the Directive into national law, particularly because the harm continues while images remain available and circulate.

Criminal prosecution and conviction should not be a prerequisite for content removal. **If justice means helping victims to "reclaim control," removal cannot wait for criminal justice to run its course** (Rackley et al., 2021, p. 315). Making removal dependent on criminal proceedings also risks exposing victims to further harm and secondary victimisation: 44% of victims interviewed by FRA reported that their experience of investigations and court proceedings added to the harm caused by the offender (FRA, 2019, p. 90).

Therefore, when transposing the Directive, Member States should offer victims genuinely fast-track civil or administrative routes to removal, rather than making practical relief dependent on the outcome of criminal proceedings. Approaches in other jurisdictions may provide useful models: Australia's eSafety Commissioner provides an independent regulatory route to removal, while the US TAKE IT DOWN Act (Federal Trade Commission [FTC], 2026) and recent UK legislation (Crime and Policing Act 2026, Explanatory Notes, § 100) require platforms to remove reported non-consensual intimate imagery within 48 hours of the removal request.

👉 Move from transparency towards prevention and safety-by-design.

Knowing that an image or video is AI-generated or manipulated does not undo or reduce the profound violation of sexual autonomy and privacy. The AI Act's labelling requirements are largely reactive rather than proactive: they may help identify deepfake content, but they do not prevent the initial creation of abusive imagery or the harm it causes (Regulation (EU) 2024/1689, 2024, Art. 50; Łabuz, 2023, p. 278). Moreover, while the Act places transparency obligations on AI providers, it does not go far enough in requiring them to prevent the foreseeable misuse of their systems for the creation of non-consensual sexual or intimate imagery.

The EU should complement transparency requirements with stronger preventive obligations on providers of AI systems. In practice, this means requiring providers, the architects of AI systems, to address potential misuse from the outset by assessing foreseeable misuse and implementing safety-by-design safeguards, including risk assessment, testing, detection and mitigation measures.

The aim should not be simply to make abusive AI-generated content identifiable after it has been created, but to make its creation more difficult in the first place. This preventive approach should be complemented at platform level by stronger measures under the DSA to limit the dissemination, amplification and recirculation of abusive imagery once it enters the online environment (Regulation (EU) 2022/2065, 2022, Arts. 34–35).

Conclusion

Over the past years, the EU has taken substantial steps towards legally recognising and addressing AI-generated sexually explicit and intimate deepfake imagery. What is missing from the EU's "promising but partial" framework (Rigotti et al., 2024, pp. 1472–1473) is not another major piece of legislation, but **greater operationalisation of the three relevant legal instruments**, with clear responsibilities among the actors involved, clear pathways for victims to seek support and redress, and clear timelines for content removal.

A victim-centred approach should be proactive rather than reactive, move away from the compartmentalisation of the legal building blocks and instead place victims' needs at its core. Such an approach should be grounded in the assumption of victimhood and the principle of minimising further harm, ensuring that victims are taken seriously, treated with dignity and supported throughout their journey, from initial reporting to accessing justice and redress. For victims, what matters is whether the system can put an end to the harm, not whether it is an AI regulation, platform governance or criminal law issue. Is the system for reporting abusive content and having it removed easy to navigate? Are the people involved appropriately trained to refer victims to the single point of entry? **Can victims access support and redress without experiencing further harm or trauma, and ultimately reclaim control over their lives?** These are the questions that EU Member States should keep in mind as they transpose the VAW Directive, and as the EU further advances the implementation of the AI Act and the DSA.

In the case of AI-generated sexually explicit and intimate imagery, effective victim protection is not merely about removing an image or punishing perpetrators. Considering the constancy and depth of the harm, it is also about **restoring victims' autonomy and their freedom to live their lives** without the continuing constraints imposed by the abuse.

Given that the phenomenon predominantly targets women, often causing them to withdraw from social, professional or digital spaces and thereby restricting their liberty and equal participation in society, the issue extends beyond individual victim protection. **Effective protection against AI-facilitated gender-based violence is therefore also a question of gender equality and, ultimately, democratic participation**. The challenge for the EU is therefore to translate its growing legal recognition of this abuse into an effective, coherent and victim-centred system of protection that enables victims to regain control and participate freely in society.

Annexes

Glossary

‘’Deep fake’’ (AI Act – Article 3 (60)) means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful;

Deployers of AI systems: Natural or legal persons, public authorities or other bodies using an AI system under their authority, except for personal non-professional use (Regulation (EU) 2024/1689, Art. 3(4)).

Digital Services Coordinators (DSCs): National authorities designated by each Member State to oversee the application and enforcement of the DSA and coordinate with other DSCs and the European Commission (European Commission, 2026).

Intermediary services: Information society services comprising “mere conduit”, “caching” and “hosting” services (Regulation (EU) 2022/2065, Art. 3(g)).

Hosting services: Intermediary services consisting of the storage of information provided by, and at the request of, a recipient of the service (Regulation (EU) 2022/2065, Art. 3(g)(iii)).

Online platforms: Hosting services that, at a user’s request, store and disseminate information to the public, subject to limited exceptions (Regulation (EU) 2022/2065, Art. 3(i)).

Providers of AI systems: Natural or legal persons, public authorities or other bodies that develop, or have developed, an AI system and place it on the market or put it into service under their own name or trademark (Regulation (EU) 2024/1689, Art. 3(3)).

Trusted flaggers: An independent entity recognised under Article 22 DSA by a Digital Services Coordinator as having particular expertise and competence to detect, identify and notify illegal content diligently, accurately and objectively. (DSA – Article 22 (2) – page 56)

VLOPs Very large online platforms (VLOPs) are online platforms with an average of at least 45 million monthly active recipients of the service in the EU and designated as such by the European Commission under the DSA **(**Regulation (EU) 2022/2065, Article 33(1) and (4)).

VLOSEs Very large online search engines (VLOSEs) are online search engines meeting the same threshold of at least 45 million average monthly active recipients of the service in the EU and designated as such by the European Commission (Regulation (EU) 2022/2065, Article 33(1) and (4)).

The Commission explains that this threshold corresponds to platforms/search engines reaching more than 10% of the EU population and that designation triggers the DSA's additional obligations addressing the particular systemic risks posed by services of this scale.

References

Association Concerning Sexual Violence Against Women. (2025, July 17). *Deepfake image-based sexual violence inflicts profound, real harm and long-term trauma, says victim-survivor*. RainLily. https://rainlily.org.hk/eng/news/2025/7/17/deepfake

Blondé, A., Altan, L., Boychenko, O., & Van Den Heuvel, L. (2023). *Safe justice for victims of crime: Challenging how we perceive success in justice—Moving towards an integrated, victim-sensitive system*. Victim Support Europe. Safe Justice for Victims of Crime

Citron, D. K. (2019). Sexual privacy. *The Yale Law Journal, 128*(7), 1870–1960. https://www.yalelawjournal.org/article/sexual-privacy

Crime and Policing Act 2026, Explanatory Notes, § 100 (UK). legislation.gov.uk – Section 100 Explanatory Notes

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 **on combating violence against women and domestic violence**, 2024 O.J. (L 1385). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401385

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards **on the rights, support and protection of victims of crime**, and replacing Council Framework Decision 2001/220/JHA, 2012 O.J. (L 315) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0029

eSafety Commissioner. (n.d.). *Image-based abuse*. Australian Government. eSafety image-based abuse page

European Commission. (2026). *Digital Services Coordinators*. Shaping Europe's Digital Future. Digital Services Coordinators

Directive (EU) 2026/1472 of the European Parliament and of the Council of 17 June 2026 amending Directive 2012/29/EU establishing minimum standards **on the rights, support and protection of victims of crime**, and replacing Council Framework Decision 2001/220/JHA, 2026 O.J. (L 1472). 1 – 30.
https://eur-lex.europa.eu/search.html?scope=EURLEX&text=Directive+%28EU%29+2026%2F1472&lang=en&type=quick&qid=1795457176541

European Union Agency for Fundamental Rights. (2019). *Proceedings that do justice: Justice for victims of violent crime—Part II*. Publications Office of the European Union. FRA report

Federal Trade Commission. (2026, May). *Complying with the TAKE IT DOWN Act*. FTC guidance on the TAKE IT DOWN Act

Habgood-Coote, J. (2023). Deepfakes and the epistemic apocalypse. *Synthese, 201*, Article 103. https://doi.org/10.1007/s11229-023-04097-3

Jóźwiak, M., & Ohnesorge, J. (2026, July 13). *Platform governance and technology-facilitated gender-based violence: Positioning the DSA in the EU's legal framework*. DSA

Observatory. https://dsa-observatory.eu/2026/07/13/platform-governance-and-technology-facilitated-gender-based-violence-positioning-the-dsa-in-the-eus-legal-framework/

Łabuz, M. (2023). Regulating deep fakes in the Artificial Intelligence Act. *Applied Cybersecurity & Internet Governance*, *2*(1), 239–280. https://doi.org/10.60097/ACIG/162856

McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). 'It's torture for the soul': The harms of image-based sexual abuse. *Social & Legal Studies*, *30*(4), 541–562. https://doi.org/10.1177/0964663920947791

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, *25*, 25–46. https://doi.org/10.1007/s10691-017-9343-2

Panorama Global. (2023). *I didn't consent: A global landscape report on image-based sexual abuse*. https://panobucket.nyc3.digitaloceanspaces.com/panobucket/documents/IBSA_Landscape_Report_2023_by_Panorama_Global_v20230228.pdf

Pawelec, M., & Łabuz, M. (2025, May 23). What is Europe doing about deepfake porn? Not enough. *EUobserver*. https://euobserver.com/3672/what-is-europe-doing-about-deepfake-porn-not-enough/

Rackley, E., McGlynn, C., Johnson, K., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). Seeking justice and redress for victim-survivors of image-based sexual abuse. *Feminist Legal Studies*, *29*(3), 293–322. https://doi.org/10.1007/s10691-021-09460-8

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC **(General Data Protection Regulation),** 2016 O.J. (L 119), 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC **(Digital Services Act)**, 2022 O.J. (L 277), 1–102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence **(Artificial Intelligence Act),** 2024 O.J. (L 1689). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Rigotti, C., McGlynn, C., & Benning, F. (2024). Image-based sexual abuse and EU law: A critical analysis. *German Law Journal*, *25*(9), 1472–1493. https://doi.org/10.1017/glj.2024.49

Security Hero. (2023). *2023 state of deepfakes: Realities, threats, and impact*. https://www.securityhero.io/state-of-deepfakes/

UN Women. (2026, February 26). *When justice fails: Why women can't get protection from AI deepfake abuse*. https://www.unwomen.org/en/articles/explainer/when-justice-fails-why-women-cant-get-protection-from-ai-deepfake-abuse