

UDK: 343.541-053.2 : 004.738.5 (4-67 EU)
Preliminary communication

Dóra Rengel, PhD student
Faculty of Law, University of Pécs, Hungary
E-mail: rengel.dora@ajk.pte.hu
ORCID-ID: 0009-0001-9477-9726

THE EU REGULATORY FRAMEWORK ON DEEPFAKE CHILD SEXUAL ABUSE MATERIAL: CURRENT SOLUTIONS AND FUTURE DIRECTIONS

ABSTRACT

This study examines the European Union's regulatory framework governing synthetic content depicting the sexual abuse of children created through deepfake technology (AI-generated CSAM). Advances in artificial intelligence now enable the production of highly realistic imagery that may not be linked to an identifiable victim, yet still constitutes a serious infringement of children's sexual integrity. The analysis demonstrates that although the Digital Services Act and the AI Act introduce important platform-governance and transparency obligations, neither instrument provides a comprehensive response to the challenges posed by AI-generated CSAM. The current conceptual framework of Directive 2011/93/EU likewise struggles to address fully synthetic material. The Recast Directive represents a significant step forward by explicitly extending the definition of CSAM to include deepfake recordings and realistic digital representations. In parallel, the proposed CSAR would impose mandatory risk-assessment and detection obligations on service providers; however, this raises substantial EU fundamental-rights concerns, particularly regarding data protection and the right to privacy. The study concludes that an effective response to deepfake child sexual abuse material requires coordinated criminal-law, platform-regulation and AI-governance mechanisms. Such a framework can only be realised through sustained cooperation between legislators, technology developers, service providers and civil-society actors.

Keywords: *deepfake, AI-generated child sexual abuse material, AI Act, DSA, future EU regulatory framework*

1. INTRODUCTION

The development of artificial intelligence-based image-generation and image-manipulation technologies has created new challenges in the field of cybercrime. Deepfake technology enables the production of visual and audiovisual content that creates the appearance of reality while depicting individuals or events that do not in fact exist. One of the most severe manifestations of this phenomenon is the

artificial creation of sexualised depictions of children (hereinafter: AI-generated CSAM). These technologies are evolving more rapidly than the law can follow, creating an urgent need for legislative frameworks that provide modern, deepfake-specific solutions.¹

The European Union (hereinafter: EU) has recently introduced comprehensive reforms to regulate the digital environment, most notably through the adoption of Regulation (EU) 2022/2065 of the European Parliament and of the Council on digital services and amending Directive 2000/31/EC (hereinafter: Digital Services Act, DSA), and Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence and amending certain Union legislative acts (hereinafter: AI Act). The core criminal-law framework related to child sexual abuse material remains defined by Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA (hereinafter: Directive 2011/93/EU). However, deepfake child pornography challenges both the effectiveness and internal coherence of these norms.

A central question is how AI-generated content—whether fully synthetic or created using the facial features or body parts of real children—fits within the EU’s conceptual framework on child pornography. At the same time, it must be examined whether the regulatory model grounds protection exclusively in the concrete child victim, or whether it also recognises an abstract legal interest in safeguarding children’s sexual integrity more broadly. From a practical perspective, further questions arise as to whether the new rules applicable to online platforms and to artificial intelligence systems are capable of ensuring the effective prevention and removal of such content.

The proposed recast of Directive 2011/93/EU (hereinafter: Recast Directive) and the draft EU Regulation laying down rules to prevent and combat child sexual abuse—known as the Child Sexual Abuse Regulation or “Chat Control” (hereinafter: CSAR)—are still pending at Union level. The CSAR proposal, however, raises significant fundamental rights concerns, particularly regarding the rights to respect for private and family life and to the protection of personal data,

¹ Zverev, V., Bushkov, V., Khrushkov, B., Sarychev, V., Ostaltsev, O., & Prokopovych-Tkachenko, Y., *Artificial intelligence and cybercrime: New challenges and prospects for legal regulation*, Contemporary Issues in Artificial Intelligence, 1/2025, p. 2.

as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.²

The key issue, therefore, is whether the EU regulatory framework can effectively counter deepfake child pornography without infringing fundamental rights—most notably the principles of necessity and proportionality. The aim of this study is to provide a systematic analysis of the EU legal framework governing deepfake child sexual abuse material, to identify conceptual and structural uncertainties, and, where appropriate, to formulate *de lege ferenda* recommendations. The analysis proceeds from the assumption that while the current normative toolbox is, in principle, capable of addressing the phenomenon, clarification of conceptual boundaries is essential to ensure legal certainty.

The research primarily employs a doctrinal legal methodology, focusing on the definitions of deepfake technology and child pornography in EU law and on the interpretation of the normative content of relevant legal sources. The study also takes account of the current state of ongoing legislative processes. The first part introduces the EU definitions of deepfake technology and child pornography and explains the social relevance and prevalence of the phenomenon, supported by statistical data. This is followed by an analysis of the relevant EU regulatory frameworks—particularly the DSA, the AI Act, Directive 2011/93/EU, the Recast Directive and the CSAR. The concluding part emphasises that combating deepfake child sexual abuse material requires a complex, multi-level approach in which legislation, law enforcement, and technological solutions play equally essential and mutually reinforcing roles.

2. CONCEPTUAL FOUNDATIONS

2.1. Deepfake

2.1.1. The concept and origin of deepfakes

The complexity of the subject matter requires a clear clarification of the conceptual foundations. This chapter therefore begins with the definition of “deepfake.” In EU law, the term receives an explicit normative definition in the text of the AI Act. Pursuant to Article 3(60) of the Regulation, a deepfake is any AI-generated or

² Charter of Fundamental Rights of the European Union, Articles 7 and 8, ^[1]Official Journal of the European Union, C 326, 26.10.2012, pp. 391–407 (hereinafter: EU Charter)

AI-manipulated image, audio or video content that resembles existing persons, objects, places, entities or events, and that may appear authentic or real to a natural person in a misleading manner.³

Nevertheless, the term "deepfake" stems from the combination of "deep learning" and "fake."⁴ The phenomenon emerged in 2017 and represents a new form of artificially produced synthetic media.⁵ For a broader conceptualisation, a more comprehensive, synthesised definition is appropriate—one that draws on multiple definitional approaches. Deepfakes constitute digital media manipulation,⁶ a dangerous form of visual disinformation,⁷ generated using artificial intelligence and deep learning techniques.⁸ As a result, they produce falsified content⁹ that convincingly creates the impression that both the content and its depicted subjects are real and authentic, while they are in fact fully manipulated.¹⁰

In the context of the present study, deepfake technology appears in two principal forms.¹¹ First, existing visual material may be manipulated. In such cases, the facial features or body parts of a real child may be inserted into other—potentially sexually explicit—recordings, or the context of originally non-sexual material may be altered. Thus, offenders may employ artificial intelligence to modify an image of a child to make it appear as if the child were unclothed or depicted in illegal content, or to rework, extend, or reframe previously unlawful recordings, thereby

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Article 3(60), Official Journal of the European Union, L 2024/1689, 12.7.2024 (hereinafter: AI Act)

⁴ Kietzmann, J.; Lee, L. W.; McCarthy, I. P.; Kietzmann, T. C., *Deepfakes: Trick or Treat*, Business Horizons, year 63, 2/2019, pp. 135–146.

⁵ Sandoval, M.-P.; de Almeida Vau, M.; Solaas, J.; Rodrigues, L., *Threat of deepfakes to the criminal justice system: a systematic review*, Crime Science, year 13, 1/2024, p. 1.

⁶ Veszelszki, Á., *Deepfake: kételkedés a kételyben*, In: Aczél, P.; Veszelszki, Á. (eds.), *Deepfake: a valótlan valóság*, Gondolat Kiadó, Budapest, 2023, p. 15.

⁷ Weikmann, T.; Greber, H.; Nikolaou, A.; *After Deception: How Falling for a Deepfake Affects the Way We See, Hear, and Experience Media*, The International Journal of Press/Politics, 1/2025, p. 104.

⁸ Whittaker, L.; Mulcahy, R.; Letheren, K.; Kietzmann, J.; Russell, R.; Bennett, B.; *Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda*, Technovation, 1/2023, p. 23.

⁹ Temir, E.; *Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism*, Selçuk İletişim Dergisi, 2/2020, p. 1012.

¹⁰ Lendvai, G. F.; *Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából*, Gondolat Kiadó, Budapest, 2023, p. 122.

¹¹ Ganesh, H. K.; *Protecting Children Through Deepfake Child Pornography: A Moral, Legal, and Philosophical Discussion on the Intersection of the Evolution in Law and Technology*, American Criminal Law Review, 60/2022, p. 7.

creating additional victimisation for individuals already depicted.¹² Second, fully synthetic content may be produced, whereby AI systems generate realistic but non-existent individuals and scenes based on textual instructions (prompts).¹³ Despite their synthetic nature, such visual material can equally reinforce patterns that normalise abusive behaviour and may contribute to encouraging offences against real victims.¹⁴

2.1.2. Technological characteristics of deepfakes

2.1.2.1. Generative Adversarial Networks (GANs)

Understanding how manipulated content is constructed is essential; therefore, the underlying technological approaches—typically three major categories—require explanation. GANs constitute one of the most commonly used foundations of deepfake technology. They consist of two competing neural networks: the generator, which produces new, falsified images or videos, and the discriminator, which aims to distinguish the generator's output from real material. Through this "competition," both networks undergo continuous optimisation,¹⁵ contributing to increasingly convincing results.¹⁶

2.1.2.2. Autoencoders and Variational Autoencoders (VAEs)

An autoencoder consists of three components: an encoder that extracts key features from images—such as skin tone, facial expression or eye position—and compresses them; a latent space in which these features are stored; and a decoder that reconstructs the image from the latent representation. In deepfake

¹² U.S. Department of Homeland Security – Homeland Security Investigations, *Artificial Intelligence and Combating Online Child Sexual Exploitation and Abuse*, Know2Protect campaign, online infographic, https://www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_genai-bulletin.pdf, 3 January, 2026.

¹³ Internet Watch Foundation (IWF), *How AI is being abused to create child sexual abuse imagery, institutional report*, October 2023, p. 6, https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf, 18 January, 2026.

¹⁴ Dushi, D.; Berdufi, N.; Karagianni, A., *The legal framework and legal gaps for AI-generated child sexual abuse material*, Computer Law & Security Review, 59/2025, p. 1.

¹⁵ Luan, T., *A Survey on Deepfake Detection Technologies*, International Journal of Emerging Technologies and Advanced Applications, 2/2025, p. 2.

¹⁶ Zhang, T., *Deepfake generation and detection, a survey*, Multimedia Tools and Applications, 81/2022, p. 6261.

face-swapping, two separate decoders are trained for two different faces, while a single shared encoder processes both. Thus, the face of Person A can be replaced with that of Person B by encoding A's image and decoding it with B's decoder. The resulting image shows Person B's face on Person A's body.¹⁷ Variational autoencoders differ somewhat, as they model the latent space statistically. While traditional autoencoders compress and reconstruct images in a fixed manner, VAEs encode inputs as probability distributions (mean and variance) within the latent space. The decoder then reconstructs images through sampling from these distributions, making it possible to generate multiple variations from a single input.¹⁸

2.1.2.3. Diffusion Models

In machine learning, diffusion models generate new data—such as images—by progressively adding noise to the training data and then learning to reconstruct the original data by reversing the noise-adding process.¹⁹ First, a neural network is trained to corrupt images with noise, as if making them increasingly blurred. The system then learns how to remove the noise, producing clean, high-fidelity images that resemble the originals. Technologies such as DALL·E 2, Midjourney and Stable Diffusion rely on this approach and can generate highly realistic images based solely on textual prompts.²⁰

2.2. Child Sexual Abuse Material

For assessing AI-generated child sexual abuse material within the EU legal framework, the point of departure is the definition in Article 2(c) of Directive 2011/93/EU. Before defining the term, the Directive clarifies that a “child” means

¹⁷ Patel, Y.; Tanwar, S.; Gupta, R.; Bhattacharya, P.; Davidson, I. E.; Nyameko, R.; Aluvala, S.; Vimal, V., *Deepfake Generation and Detection: Case Study and Challenges*, IEEE Access, 11/2023, p.143301.

¹⁸ Choudhary, A. S., *What is Variational Autoencoders?* Data Science Blogathon 2025, <https://www.analyticsvidhya.com/blog/2023/07/an-overview-of-variational-autoencoders/>, 22 April, 2025.

¹⁹ O'Connor, R., *Introduction to Diffusion Models for Machine Learning*, Assemblyai 2022, <https://www.assemblyai.com/blog/diffusion-models-for-machine-learning-introduction#:~:text=Let's%20dive%20in!,Diffusion%20Models%20%2D%20Introduction,through%20the%20learned%20denoising%20process>, 30 June, 2025.

²⁰ *Introduction to diffusion models for machine learning*. Superannotate 2025, <https://www.superannotate.com/blog/diffusion-models#:~:text=Diffusion%20models%20are%20prominent%20in,distribution%20from%20the%20noisy%20data>, 25 June, 2025.

any person below the age of 18 (Article 2(a)).²¹ Additionally, Article 2(b) introduces the concept of the "age of consent," referring to the age below which any sexual activity with a child is prohibited under national law.²²

The Directive's preamble emphasises the need for clarity regarding what constitutes child pornography under EU law.²³ This is crucial because such material can take numerous forms (real, simulated, realistic, depictions of persons appearing as children, etc.), and effective law enforcement requires a precise definition that covers all relevant conduct. The Directive therefore adopts a broad definition encompassing several partially distinct, partially overlapping categories.

Under point (i), child pornography includes any material that visually depicts a child engaged in real or simulated explicit sexual conduct. This category traditionally concerns recordings involving actual, identifiable children.

Point (ii) widens the scope further by independently criminalising depictions of the sexualised display of a child's sexual organs, irrespective of whether explicit conduct occurs.

Point (iii) directly addresses challenges arising from technological developments by covering material depicting a person appearing to be a child engaged in explicit sexual conduct, or the sexualised display of such a person's sexual organs.

Point (iv) adds further nuance by expressly including "realistic images" of children engaged in explicit sexual conduct or realistic images of a child's sexual organs when produced primarily for sexual purposes.²⁴

Thus, EU law adopts a broad protective approach that criminalises not only depictions involving real children, but also virtual child pornography (digitally generated content that creates sexualised depictions of child-like figures without involving real children)²⁵ and pseudo-child pornography (digitally altered content using body parts or facial features of real individuals to create material that appears

²¹ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011 (hereinafter: Directive 2011/93/EU), Article 2(a).

²² Directive 2011/93/EU, Article 2(b).

²³ Directive 2011/93/EU, Preamble (12).

²⁴ Directive 2011/93/EU, Article 2(c).

²⁵ Burke, D. D.; Doval, C. N., *Redefining child pornography in an age of technological advancement: The concept of avoidable harm*, Washington Journal of Law, Technology & Arts, year 20, 3/2025, p. 49.

to depict a child, without involving an actual minor).²⁶ This approach allows deepfake-generated content to fall within the definition of child pornography where it meets the criteria of "a person appearing to be a child" or "realistic images." Nonetheless, conceptual uncertainties arise—particularly concerning the category of "realistic images."²⁷ The proposed Recast Directive may introduce relevant modifications to these definitions, should the draft be adopted. These potential changes will be discussed later in this study.

The current framework leaves certain discretion to Member States. They may, for example, decide whether to criminalise material falling under point (iii) where the individuals depicted are adults who are made to appear younger.²⁸ Member States may also choose whether to prohibit the creation or possession of "realistic" images under point (iv) when such content is created and held exclusively for private use, is purely fictional, does not involve real children, and presents no risk of dissemination.²⁹

Article 8(3) further expands this discretion by allowing Member States to decide whether criminal sanctions apply in cases where:

- the persons depicted are minors who have reached the age of consent,
- the material was produced and is possessed with their mutual consent,
- and no coercion, abuse or exploitation occurred.³⁰

3. STATISTICAL DIMENSIONS OF THE DEEPFAKE PHENOMENON

The social harmfulness of the deepfake phenomenon is unequivocally supported by empirical data. The spread of the technology has been extraordinarily rapid: while an estimated 500,000 deepfake items were accessible online in 2023, projections indicated that by 2025 this number would exceed 8 million. This represents an increase of more than 1,500% within two years,³¹ with the volume

²⁶ Negredo, L.; Herrero, Ó., *Child pornography on the Internet*, Papeles del Psicólogo / Psychologist Papers, year 37, 3/2016, p. 218.

²⁷ Rigotti, C.; Gkioka, C. P.; Do Rosario Da Graça, S.; Lannier, S., *Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors*, New Journal of European Criminal Law, 2025, p. 17.

²⁸ Directive 2011/93/EU, Article 5(7).

²⁹ Directive 2011/93/EU, Article 5(8).

³⁰ Directive 2011/93/EU, Article 8(3).

³¹ European Parliament, *Children and deepfakes*, Briefing, European Parliamentary Research Service (EPRS), 2025, 2025, p. 2,

of such content doubling approximately every six months. The phenomenon is therefore not merely expanding, but doing so at an exponential pace.³²

However, the problem is not solely quantitative. According to estimates by the European Commission, approximately 98% of deepfake content is pornographic in nature,³³ indicating that current patterns of technological use are predominantly shifting toward sexual exploitation. Europol's forecasts reinforce the seriousness of these trends: by 2026, up to 90% of online content may be synthetically generated, fundamentally challenging the credibility of digital material and the ability to distinguish between reality and manipulation. Within the category of sexual deepfakes, the proportion involving minors is particularly alarming. Studies indicate that one in seven internet users has encountered a sexual deepfake, while approximately 17% of artificially generated sexualised content involves minors.³⁴ The large-scale emergence of AI-generated child sexual abuse material (AI-CSAM) has become one of the most severe online safety trends within the European Union.³⁵ International data from 2024 show that 90% of such material reaches a level of realism that may render it equivalent, from a legal-assessment perspective, to recordings involving real children. Reports related to AI-CSAM increased from 4,700 in 2023 to 67,000 in 2024—a 1,325% rise—most of which exhibited a clear European nexus.³⁶

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.

³² Sensity, *How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos*, 2021, <https://sensity.ai/blog/how-to-detect-a-deepfake/>, 24 June, 2025.

³³ Furizal; Ma'arif, A.; Maghfiroh, H.; Suwarno, I.; Prayogi, D.; Kariyamin; Lonang, S.; Sharkawy, A.-N., *Social, legal, and ethical implications of AI-generated deepfake pornography on digital platforms: A systematic literature review*, Social Sciences & Humanities Open, Year 12, 2025, p. 13.

³⁴ European Parliament, *Children and deepfakes*, mBriefing, European Parliamentary Research Service (EPRS), 2025, p. 2-3, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.

³⁵ Internet Watch Foundation (IWF), *What has changed in the AI CSAM landscape?*, AI CSAM Report Update, Version 1.1, July 2024, p. 25, https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf, 5 January, 2026.

³⁶ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025, p. 1, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

4. EU THE EU'S EXISTING NORMATIVE FRAMEWORK

4.1. DSA

4.1.1. Illegal Content from the Perspective of the DSA

Following the risk assessment of deepfakes, this section examines how the European Union's current regulatory framework—most notably the DSA, which partly replaces the previously inconsistent and divergent self-regulatory practices of digital platforms—responds to this phenomenon.³⁷ The DSA seeks to more effectively tackle illegal content disseminated via online intermediary services and to provide stronger user protection, while balancing the fundamental rights of both service providers and users.³⁸

Although the DSA does not contain explicit provisions concerning deepfake child sexual abuse material, child sexual abuse material (CSAM) unequivocally falls within the Regulation's category of "illegal content."³⁹ Under the DSA, illegal content is defined broadly as any information that is unlawful under EU or national law.⁴⁰ Even though the domestic law of certain Member States does not yet expressly criminalise AI-generated CSAM, such material remains illegal under EU law based on the definitional framework of Directive 2011/93/EU. Accordingly, the DSA applies fully to AI-generated and manipulated CSAM. Article 7 of the DSA allows providers to voluntarily undertake investigations and implement measures aimed at the detection, identification and removal of illegal content.⁴¹ Under Article 16, hosting service providers must operate efficient notice-and-action mechanisms, enabling users to report illegal content in a straightforward and transparent manner.⁴² To support this, Article 12 requires providers to designate a single point of contact that ensures swift and direct

³⁷ Sorbán, K., *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, Belügyi Szemle, 10/2020, p. 81.

³⁸ Wilman, Folkert, *The Digital Services Act (DSA) – An Overview, working paper*, European Commission, 2022, p. 1.

³⁹ Buri, I.; van Hoboken, J., *The Digital Services Act (DSA) proposal: a critical overview, Discussion paper, Digital Services Act (DSA) Observatory*, Institute for Information Law (IViR), University of Amsterdam, 2021, p. 8.

⁴⁰ 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 (hereinafter: DSA), Article 3(h)

⁴¹ European Data Protection Board (EDPB), *Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR*, 2025, p. 9-10, https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf, 10 December, 2025.

⁴² DSA, Art. 16(1)–(2)

electronic communication with users and competent authorities.⁴³ Platforms must act without undue delay, inform the notifier of the decision taken, and provide access to redress mechanisms.⁴⁴

The DSA establishes differentiated obligations based on the size and societal impact of platforms. Digital service providers fall into four categories: intermediary services, hosting services, online platforms and very large online platforms and search engines (VLOPs and VLOSEs).⁴⁵ Very large platforms and search engines with more than 45 million EU users⁴⁶ (such as AliExpress International (Netherlands) B.V., Amazon EU S.à.r.l., Google Ireland Ltd.)⁴⁷ are subject to extensive risk-management obligations. The Commission has designated 17 platforms as VLOPs and 2 services as VLOSEs.⁴⁸ Under Article 35, these providers must identify and assess systemic risks—including the dissemination of illegal content such as CSAM and AI-generated CSAM⁴⁹—and develop reasonable and effective mitigation measures.⁵⁰

Such measures may include modifications to user interfaces, revisions of terms of service, improvements in notice-and-action processes, adjustments to algorithmic systems, enhanced visibility of reliable information, labelling of suspicious content, and the adoption of codes of conduct.⁵¹

Action against illegal content is ensured through cooperation with national authorities; accordingly, Articles 9 and 10 of the DSA allow for specific removal or data-disclosure orders, while continuing to prohibit any general monitoring obligation.⁵² The DSA further dedicates a separate chapter to the online protection

⁴³ Gsell, Florence; *The Digital Services Act (DSA): A General Assessment*, In: von Ungern-Sternberg, Antje (ed.), *Content Regulation in the European Union – The Digital Services Act*, TRIER Studies on Digital Law, year 1, Verein für Recht und Digitalisierung e.V., Institute for Digital Law (IRDT), Trier, 2023, p. 9.

⁴⁴ DSA, Art. 16 (5)

⁴⁵ Genç-Geleç, B., *Regulating digital platforms: Will the DSA correct its predecessor's deficiencies?*, Croatian Yearbook of European Law and Policy, year 18, 2022, p. 59.

⁴⁶ DSA, Art. 33(1)

⁴⁷ European Commission, *Supervision of the designated very large online platforms and search engines under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>, 10 February, 2026.

⁴⁸ European Commission, *The enforcement framework under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.

⁴⁹ Parti, K.; Szabó, J.; *The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe*, Laws, year 13, 6/2024, p. 3,

⁵⁰ DSA, Art. 33-35.

⁵¹ Gsell, *op. cit.*, note 43, p. 16.

⁵² Gsell, *op. cit.*, note 43, p. 10.

of minors. Article 28 mandates service providers accessible to minors to adopt measures ensuring a high level of privacy, safety and protection.⁵³ Additionally, targeted advertisements based on profiling using minors' personal data—within the meaning of the GDPR—are strictly prohibited where the provider can reasonably determine that the user is a minor.⁵⁴

The DSA's enforcement architecture operates through a dual structure: national Digital Services Coordinators supervise compliance at Member State level, whereas the European Commission exercises exclusive oversight over very large platforms.⁵⁵ The Commission may launch investigations, request information and conduct on-site inspections.⁵⁶ Non-compliant very large platforms may face fines of up to 6% of their global annual turnover. Since the Regulation's entry into force, several high-profile investigations have been initiated, including against TikTok for a potentially addictive reward system, and against AliExpress for the dissemination of illegal products.⁵⁷ Major platforms—such as TikTok and Facebook—have introduced specialised training for content moderators to improve their ability to identify and address illegal material, including CSAM.⁵⁸

4.1.2. Practical Enforcement of the DSA and the Lessons of the Grok Scandal

The January 2026 Grok scandal highlighted the risks involved. The Grok chatbot developed by xAI was capable of generating sexually explicit synthetic images of minors through the digital removal of clothing, producing approximately 6,700 such images within two days. Although xAI quickly introduced restrictions, the EU launched an investigation to determine whether the platform had violated the DSA provisions on combating illegal content.

The Commission had already imposed a €120 million fine on X for earlier transparency infringements and ordered the preservation of all data related to

⁵³ Wilman, Folkert, *The Digital Services Act (DSA) – An Overview, working paper*, European Commission, 2022, p. 11.

⁵⁴ DSA, Art. 28(2)

⁵⁵ European Commission, *The Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 8 October, 2025.

⁵⁶ European Commission, *The enforcement framework under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.

⁵⁷ European Commission, *Digital Services Act: keeping us safe online*, 2025, https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en, 19 December, 2025.

⁵⁸ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 3, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

Grok's operation. In the wake of the scandal, several Members of the European Parliament called for a Union-wide ban on such systems, and an amendment to the AI Act was also discussed that would classify AI-generated sexual content involving children as an "unacceptable risk" practice.⁵⁹

4.2. AI Act

4.2.1. The Regulatory Architecture of the AI Act

The objective of the AI Act is to ensure that AI systems are developed and deployed in a manner that is safe and trustworthy for EU citizens, while supporting the emergence of a strong and competitive European AI ecosystem. The Regulation simultaneously protects individuals' safety and fundamental rights, enhances transparency and accountability, fosters innovation, and creates a stable and predictable market environment.⁶⁰

The Act is built upon a risk-based regulatory structure, classifying AI systems into four categories according to their potential risks: prohibited (unacceptable), high-risk, limited-risk and minimal-risk systems. Each category entails distinct compliance obligations and corresponding levels of oversight.⁶¹

The AI Act imposes a full ban from February 2025 on AI systems that pose unacceptable risks to individuals' safety or fundamental rights, including manipulative or exploitative practices, social scoring and certain intrusive biometric techniques.⁶² High-risk AI systems — such as those used in healthcare or the administration of justice — are subject to strict requirements, including risk management and human oversight. AI tools falling under transparency obligations, including those generating deepfake content, must ensure that such outputs are recognisable and appropriately labelled; these provisions will apply from August 2026.

⁵⁹ European Newsroom (ENR), *Nudification blocks: The EU's struggle for more safety online*, 2026, <https://europeannewsroom.com/nudification-blocks-the-eus-struggle-for-more-safety-online/>, 6 February, 2026.

⁶⁰ Kim, B.-J.; Jeong, S.; Cho, B.-K.; Chung, J.-B., *AI Governance in the Context of the EU AI Act*, IEEE Access, 2025, p. 144127.

⁶¹ Ducret, M.; Wahal, E.; Gruson, D.; Amrani, S.; Richert, R.; Mouncif MOUNGACHE, M.; Schwendicke, F., *Trustworthy Artificial Intelligence in Dentistry: Learnings from the EU AI Act*, Journal of Dental Research, year 103, 11/2024, p. 1052.

⁶² Boştân, I., *Consolidating the Role of AI in the Economy and Society: Combatting the Deepfake Phenomenon Through Strategic and Normative Approaches – The Case of Romania in the EU Context*, Economies, year 13, 5/2025, p. 12.

The regulation imposes no requirements on AI systems that present minimal or negligible risk, such as AI-enhanced video game features or spam filters.⁶³

Since the current risk categories are tied to the application domains of AI systems, there is a possibility that a system's actual risk level may be misjudged, potentially undermining the effective enforcement of the AI Act. This issue is particularly acute in the case of general-purpose AI (GPAI), which can be used in numerous, and often unpredictable, ways.⁶⁴

Moreover, the AI Act only partially addresses several risks associated with malicious AI use, which becomes especially evident in relation to severe abuses such as AI-generated child sexual abuse material. Although AI-generated CSAM does not appear as a separate category in Article 5, a potential link may arise under Article 5(1)(b).⁶⁵ This provision covers AI systems specifically designed or used to exploit the vulnerabilities of certain groups—such as children, who are inherently vulnerable due to their age. Nevertheless, the AI Act does not itself establish any dedicated prohibitions or obligations aimed at the prevention, detection or mitigation of AI-generated CSAM. The Act's transparency-based rules for identifying deepfake content can be easily circumvented and are insufficient for addressing the risks posed by AI-generated CSAM. Effective intervention therefore necessarily requires the combined application of multiple EU legal instruments specifically tailored to this domain.⁶⁶

In designing their risk-management systems, providers must pay particular attention to whether a high-risk AI system is accessible to children or likely to have an impact on them.⁶⁷ Due to children's heightened vulnerability and their distinct rights,⁶⁸ developers and operators of such systems must implement additional safeguards to ensure an appropriate level of protection.⁶⁹

⁶³ European Commission, *AI Act*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, 14 November, 2025.

⁶⁴ Novelli, C.; Casolari, F.; Rotolo, A.; Taddeo, M.; Floridi, L., *Taking AI risks seriously: a new assessment model for the AI Act*, AI & Society, year 39, 2024, p. 1.

⁶⁵ AI Act, Art. 5(1)(b)

⁶⁶ Elcano Royal Institute, *Risk without borders: the malicious use of AI and the EU AI Act's global reach*, Analysis, <https://www.realinstitutoelcano.org/en/analyses/risk-without-borders-the-malicious-use-of-ai-and-the-eu-ai-acts-global-reach/>, 10 February, 2026.

⁶⁷ Charisi, V.; Chaudron, S.; Di Gioia, R.; Vuorikari, R.; Escobar-Planas, M.; Sanchez, I.; Gomez, E., *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy*, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2022, p. 21.

⁶⁸ AI Act, Recital (9)

⁶⁹ Schuett, J., *Risk Management in the Artificial Intelligence Act*, European Journal of Risk Regulation, year 15, 2/2023, p. 16-17.

Article 50 sets out transparency obligations for the creation, use and labelling of deepfakes and other forms of synthetic media. Under paragraph (4), any person who creates AI-manipulated image or audio content that appears realistic must disclose its artificial origin, except in cases of lawful use in criminal proceedings; for artistic or satirical content, a lighter form of labelling is permitted. Paragraph (2) further requires providers to ensure that generated content is labelled in a machine-readable, reliable and interoperable manner.⁷⁰ At present, however, no existing technology fully satisfies these requirements.⁷¹

4.2.2. Practical Labelling and Detection of Deepfake Content

Although the Regulation requires deepfake content to be labelled, it does not specify the precise technical form such labelling should take. The most common method is the use of digital watermarking. Digital watermarking is a technology that enables information related to intellectual property rights—such as the author's name, a logo or a serial number—to be embedded into multimedia content.⁷² Its greatest disadvantage is that even minor alterations may easily remove the protection. Furthermore, if someone is aware that a document is protected in this manner, the watermark can be removed quickly and automatically.⁷³

To support the practical implementation of the transparency obligations under Articles 4 and 50 of the AI Act, the AI Office has initiated the development of a new Code of Conduct. The purpose of the Code is to provide detailed guidance on the appropriate labelling of AI-generated audio, image, video and textual content, thereby reducing the risks of manipulation, misinformation and identity misuse. The drafting process involves generative AI providers, developers of technical

⁷⁰ AI Act, Art. (2)-(4)

⁷¹ Fauchoux, V., *Transparency of AI-Generated Content: In-depth legal analysis of the Draft Code of Practice implementing Article 50 of the EU AI Act*, 2026, <https://www.ddg.fr/actualite/transparency-of-ai-generated-content-in-depth-legal-analysis-of-the-draft-code-of-practice-implementing-article-50-of-the-eu-ai-act>, 15 February, 2026.

⁷² Makhrif, Z. F.; Karim, A. A., *Digital Watermark Technique: A Review*, *Journal of Physics: Conference Series*, year 1999, 2021, p. 1.

⁷³ Pataki, M., *Algoritmusok egynyelvű és különböző nyelvek közötti fordítások és plágiumok megtalálására*,

PhD dissertation, Pázmány Péter Katolikus Egyetem, Információs Technológiai Kar, Multidiszciplináris Műszaki Tudományok Doktori Iskola, 2012. p. 14.

labelling solutions, civil society organisations, researchers and experts, and the final text is expected in May–June 2026.⁷⁴

Beyond Codes of Conduct, practical detection tools must target the distinctive features of deepfakes. These comprise biometric anomalies (unnatural blinking, irregular movements, unrealistic rendering), model-based fingerprints unique to the generating system, and media-based characteristics, including spatiotemporal inconsistencies and distortion noise. Analyzing these technical categories is essential for differentiating synthetic from authentic recordings.⁷⁵ Human observation is often insufficient to identify such discrepancies, whereas detection technologies and forensic methods increase the likelihood of accurate identification. In recent years, several software tools and online platforms have emerged, such as DeepFake-o-meter or FakeBuster, which are capable of detecting audiovisual manipulation. These platforms, however, remain in an early stage of development and require further refinement to keep pace with continuously evolving deepfake techniques.⁷⁶

State-of-the-art deepfake detection methods rely on deep learning to extract unique features. The most well-known architectures include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and their advanced variants. Examples are Long Short-Term Memory networks (LSTMs), a specialised type of RNN, and Residual Networks (ResNets), a more advanced form of CNN.⁷⁷ Also significant are hybrid approaches, such as combinations of CNN and RNN architectures, which may enhance detection accuracy. In such a system, the CNN extracts visual features from video frames, while the RNN analyses temporal relationships between frames to identify inconsistencies. This construction can, for instance, detect the absence of blinking. Its limitation is that it is effective only with short video clips—typically those lasting no more than two seconds—and relies solely on blink absence as an indicator. As a result, it is incapable of detecting manipulated recordings in videos with frequent blinking.⁷⁸⁷⁹

⁷⁴ European Commission, *Code of Practice on marking and labelling of AI-generated content*, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>, 9 January, 2026.

⁷⁵ Zhang, T., *Deepfake generation and detection, a survey*, Multimedia Tools and Applications, 81/2022, p. 6264–6267.

⁷⁶ Masood, M.; Nawaz, M.; Malik, K. M.; Javed, A.; Irtaza, A.; Malik, H., *Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward*, *Applied Intelligence*, 1/2022, p. 25.

⁷⁷ Zhang, *op. cit.*, note 81, p. 6261–6264.

⁷⁸ Masood et al., *op. cit.*, note 82, p. 13.

⁷⁹ Zhang, *op. cit.*, note 81, p. 6261.

Despite many existing methods and combinations, each has limitations that affect its effectiveness depending on the content analysed.

5. FUTURE DIRECTIONS OF EU DIGITAL CHILD PROTECTION REGULATION

5. 1. Recast Directive

The European Union's child-protection framework is grounded in the Charter of Fundamental Rights, which in Article 24 enshrines the rights of the child to well-being and protection, as well as the principle that the child's best interests must be a primary consideration.⁸⁰ This legal foundation underpins Directive 2011/93/EU. The Directive sets out minimum EU rules concerning the definition of offences, sanctions, prevention and victim protection.⁸¹ Its recitals emphasise the severely rights-violating nature of child sexual abuse material,⁸² as well as the explosive growth of such material driven by the internet and emerging technologies, which justifies strengthened EU-level action.⁸³

Article 5 clearly defines the behaviours related to child sexual abuse material that Member States must criminalise, including acquisition or possession of CSAM, intentional access to such material, distribution, transmission or sharing, offering or making it available, and its production. These offences are punished at varying levels of severity, typically with imprisonment ranging from one to three years.⁸⁴

EU child-protection criminal law is now undergoing substantial reform, as the European Union seeks a regulatory framework better suited to addressing challenges of the digital age, particularly deepfakes and AI-generated content. The Recast Directive significantly revises and expands the conceptual and criminal-law framework applicable to child sexual abuse material—referred to in the updated terminology as "material depicting the sexual abuse of children." The Recast Directive introduces broader and clearer definitions, expressly encompassing content depicting persons appearing to be children; realistic digital images, including modified or entirely computer-generated material; reproductions and depictions of children such as avatars or other virtual characters;

⁸⁰ EU Charter Article 24

⁸¹ Klimek, L., *European responses criminalising online solicitation of children for sexual purposes*, Balkan Social Science Review, 6/2020, p. 13-14.

⁸² Directive 2011/93/EU, Preamble (1).

⁸³ Directive 2011/93/EU, Preamble (3).

⁸⁴ Directive 2011/93/EU, Article 5

and all non-visual formats providing guidance or instructions for the sexual abuse, exploitation or solicitation of children. The expanded definition aims to ensure that the legal framework covers deepfakes, AI-generated images and other technologically produced forms of abusive content. The Recast Directive clarifies that "realistic representation" includes any reproduction or digital rendering depicting children in a sexual context, and extends its scope to all material providing advice, guidance or instruction facilitating child sexual abuse, exploitation or solicitation. This would eliminate interpretative uncertainties present in the current Directive. Article 8(3) of the current Directive allows Member States to exempt certain content from criminal liability, provided it is created and possessed solely for private use, produced with mutual consent, and involves individuals above the national age of consent, without coercion or harassment. In practice, however, some Member States interpreted this exemption too broadly, applying it even in cases involving significant age or power imbalances while classifying such relationships as "peer situations." The Recast Directive therefore expands the scope of punishable conduct beyond the production and possession of material to include access, while also introducing stricter safeguards. The exemption is moved to Article 10 and applies only where the individuals concerned are above the age of consent and are genuine peers. The concept of a "genuine peer" is defined in Article 2 as persons "close in age and in psychological and physical maturity." Although the Recast Directive substantially broadens the concept of CSAM, debate continues over the extent to which purely virtual material—created without any real child—should be criminalised. The central issue concerns the legal basis for criminalisation and the potential harm caused by such content. Since these materials do not depict a real child, there appears to be no direct, identifiable victim at first glance.⁸⁵

However, this does not mean that such content is harmless. Research and regulatory developments clearly indicate that entirely virtual CSAM can normalise sexual abuse of children, encourage consumption of such material and contribute to its wider dissemination.⁸⁶ Deepfake-based material can negatively affect both depicted proxies and viewers, and therefore society as a whole.⁸⁷ Research indicates that AI-generated CSAM and similar phenomena can impose severe psychological burdens on affected individuals, increasing the risk of depression, anxiety, and even suicidal ideation. In addition, the consumption of virtual pornographic content can distort users' sexual attitudes and reinforce unrealistic

⁸⁵ Rigotti et al., *op. cit.*, note 27, p. 17-10.

⁸⁶ Dushi, *op. cit.*, note 14, p. 1.

⁸⁷ Karasavva, V.; Noorbhai, A., *The Real Threat of Deepfake Pornography: A Review of Canadian Policy*, Cyberpsychology, Behavior, and Social Networking, year 24, 3/2021, p. 207.

or harmful behavioural patterns, effects that deepfake technology further aggravates by enabling the creation of sexualised depictions of any person.⁸⁸

Virtual CSAM may also serve as a tool in the grooming process,⁸⁹ facilitating manipulation and trust-building while presenting lower detection risks compared with real CSAM. From a rational-choice perspective, offenders often turn to virtual CSAM because they perceive its benefits (sexual gratification, facilitation of contact, support for grooming) as outweighing the risks. Consumption of virtual material may therefore act as a gateway to offences against real children.⁹⁰

These concerns are reinforced by research showing that 52% of individuals who self-identify as offenders fear that their consumption of pornographic material could lead them to commit an actual offence. Thus, the absence of a real victim does not eliminate the societal risk; on the contrary, digital material may even constitute a first step towards real-world abuse.⁹¹

5.2. CSAR

In addition to the planned reforms of the criminal-law framework for child protection, the EU is also preparing a broader regulatory measure that would directly affect the operation of digital service providers. The proposed EU Regulation laying down rules to prevent and combat child sexual abuse (CSAR) represents a legislative effort to strengthen online child protection. The Commission presented the proposal on 11 May 2022, building on the 2020 EU Strategy, with the aim of establishing a harmonised response to the dissemination of child sexual abuse material and the online solicitation of children. The proposal seeks to impose mandatory risk-assessment, detection and reporting obligations on online service providers, including hosting services and end-to-end encrypted messaging applications such as WhatsApp and Signal.⁹²

⁸⁸ *Ibid.*, p. 204.

⁸⁹ Parti, *op. cit.*, note 49, p. 11-12.

⁹⁰ Christensen, L.; Moritz, D.; Pearson, A., *Psychological Perspectives of Virtual Child Sexual Abuse Material*, Sexuality & Culture, year 25, 4/2021, p. 1362.

⁹¹ Harkavy, R., EU moves to criminalise AI-generated CSAM, Global Legal Insights, 2025, <https://www.globallegalinsights.com/news/eu-moves-to-criminalise-ai-generated-csam/>, 12 February, 2026.

⁹² ASSEDEL (European Association for the Defense of Rights and Freedoms), *Regulation to Prevent and Combat Child Sexual Abuse (CSAR), policy analysis*, 2026, p. 1, https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February, 2026.

The emergence of EU-level rules aimed at combating online child sexual abuse developed in several stages. The first step was the adoption of the EU Interim Regulation 2021/1232, which temporarily allowed number-independent interpersonal communications services—such as webmail providers and messaging applications—to derogate voluntarily from the confidentiality and data-protection obligations set out in the ePrivacy Directive (2002/58/EC).⁹³ The aim was to permit providers to detect, report and remove CSAM.⁹⁴ The Interim Regulation was originally set to expire on 3 August 2024, but due to delays in adopting permanent legislation, its validity was extended to 3 April 2026. This extension places significant pressure on the EU legislature, as the expiry of the derogation would eliminate the existing legal framework for CSAM-screening practices.⁹⁵

In response, on 11 May 2022 the Commission presented a comprehensive, binding Regulation intended to replace the Interim Regulation. The Commission emphasised that the existing voluntary content-screening practices are fragmented, inconsistent in quality and generate legal uncertainty.⁹⁶ The proposed Regulation therefore aimed to replace the voluntary system with a uniform, mandatory mechanism for service providers, including risk-assessment and risk-mitigation requirements, CSAM detection, reporting obligations, removal of illegal material⁹⁷ and the prevention of online grooming.⁹⁸ The Commission also

⁹³ Rojszczak, M., *Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232*, Computer Law & Security Review, year 56, 2025, p. 2-5.

⁹⁴ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combating child sexual abuse online*, COM(2020) 568 final, Brussels, 2020, p. 1.

⁹⁵ European Parliament, *Legislative Train 12.2025 – New legislation to fight child sexual abuse online*, Legislative Train briefing, 2025, p. 2, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.

⁹⁶ European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, COM(2022) 209 final, Brussels, 2022.

⁹⁷ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU*, online commentary, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

⁹⁸ Eurochild, *Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse*, news article, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.

proposed establishing a new independent EU Centre on Child Sexual Abuse (EUCSA) to support both service providers and authorities.⁹⁹

The proposal was reviewed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), which began assessing it in 2022 and raised several concerns.¹⁰⁰ Supplementary impact assessments found that the proposal did not adequately address challenges inherent in end-to-end encrypted (E2EE) services. While detection of known CSAM is technically feasible, the identification of new material or grooming attempts remains uncertain. Interference with E2EE communication raises serious risks to the fundamental rights protected by Articles 7 and 8 of the Charter of Fundamental Rights—namely, the rights to privacy and data protection.¹⁰¹

The Commission's original proposal would have allowed authorities to require client-side scanning, obliging service providers to examine private messages. This generated extensive professional and civil opposition.¹⁰² The LIBE committee's draft report of 19 April 2023 supported the overall aims of the CSAR but proposed more than 1,900 amendments. These included extending the scope of the Regulation to search engines and other AI-based systems, and limiting CSA detection in E2EE services to metadata analysis only. The report also proposed establishing a victim consultation forum within the EUCSA and allowing voluntary detection practices to continue alongside mandatory measures.¹⁰³

⁹⁹ European Parliament, *Legislative Train 12.2025 – New legislation to fight child sexual abuse online*, *Legislative Train briefing*, 2025, p. 1, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.

¹⁰⁰ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 10, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

¹⁰¹ European Parliament, *Proposal for a regulation laying down rules to prevent and combat child sexual abuse – Complementary impact assessment*, European Parliamentary Research Service (EPRS), Brussels, 2023, p. 3, [https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU\(2023\)740248_EN.pdf](https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU(2023)740248_EN.pdf), 2 March 2025.

¹⁰² ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU*, *online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

¹⁰³ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 10, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

The Council's general approach, adopted on 26 November 2025, further diluted the Commission's original proposal. The Council rejected mandatory detection obligations but made the derogation from the ePrivacy Directive permanent. It introduced mandatory service-provider risk assessments and three risk categories (low, medium and high). High-risk services would be required to implement "risk-mitigation measures," of which scanning would be merely one possible option. Service providers that voluntarily participate in scanning could receive legal certainty and financial or classification advantages.¹⁰⁴ Under the new rules, providers must conduct risk assessments to prevent CSAM and grooming. National authorities oversee this process, holding the power to enforce corrective measures and mandate the removal of illegal content.¹⁰⁵ Trilogue negotiations began at the end of 2025, but adoption of the final text remains uncertain. Since the Interim Regulation will expire again in April 2026, the Commission considers an extension until 2028 necessary; otherwise, current CSAM-screening practices would lack a legal basis.¹⁰⁶

In essence, the legislative debate centres on how to balance effective measures against CSAM with full respect for privacy and data-protection rights, as proposals such as encrypted-communication scanning, detection algorithms, mandatory age verification and limits on anonymity risk becoming disproportionate and normalising digital surveillance.¹⁰⁷

6. CONCLUSIONS

The purpose of this study was to examine the gravity of the phenomenon of deepfake child sexual abuse material and to analyse how the European Union's existing and emerging legal frameworks respond to it. Statistical data clearly demonstrate that the volume of AI-generated synthetic sexualised depictions of children has increased at an exceptionally rapid pace in recent years and has now

¹⁰⁴ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU, online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

¹⁰⁵ Eurochild, *Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse*, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.

¹⁰⁶ Moreau, C., *Commission proposes two-year extension to CSAM chat-scanning rules*, Euractiv, <https://www.euractiv.com/news/commission-proposes-two-year-extension-to-csam-chat-scanning-rules/>, 7 January, 2026.

¹⁰⁷ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU, online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

become a particularly dangerous category of criminal activity. This dynamic growth presents new challenges for regulation, given that such material can be produced on a mass scale without necessarily involving real victims, yet remains capable of severely infringing the sexual integrity of children.

The analysis of EU law has shown that the European Union has recognised the specific characteristics of the phenomenon and is attempting to respond to the spread of AI-generated CSAM on multiple levels. With regard to the Recast Directive, the clarification of conceptual boundaries is of primary importance, as the proposal makes clear that both fully synthetic material and deepfake content incorporating the facial features or body parts of real children fall within the Union's definition of child sexual abuse material. The arguments presented demonstrate that although such material may lack an identifiable individual victim, it nevertheless violates the abstract legal interests associated with the sexual integrity and autonomy of children, thereby justifying an EU-level prohibition. Through the Recast Directive, the Union makes explicit that the object of protection is not limited to the bodily integrity of a specific child but extends more broadly to the collective legal interest in safeguarding children's sexual self-determination and development.

At the same time, the study has identified several unresolved issues, particularly in relation to the CSAR. The examination of encrypted communications raises significant fundamental-rights tensions, as it directly affects the rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. Although the protection of children is a paramount EU objective, this does not exempt the legislator from the strict application of the principles of necessity and proportionality.

The analysis also highlights the limited effectiveness of the relevant provisions of the DSA and the AI Act. While both regulations contain rules that may touch upon aspects of AI-generated CSAM, neither provides a direct or comprehensive response to the phenomenon.

A de lege ferenda conclusion emerging from this study is that combating deepfake child sexual abuse material cannot be reduced merely to the introduction of new prohibitions or the expansion of criminal offences. Effective, sustainable and fundamental-rights-compliant regulation requires the coordinated application of criminal-law instruments, platform-governance mechanisms and artificial-intelligence regulation. Such an approach can only succeed if legal responses are developed in dialogue with technology developers, platform providers and civil-society actors. The future direction of EU regulation can be considered coherent and sustainable only if it ensures enhanced protection of

children while preserving the fundamental-rights balance inherent in the EU legal order.

REFERENCES

BOOKS AND ARTICLES

1. Boştăn, I., Consolidating the Role of AI in the Economy and Society: Combatting the Deepfake Phenomenon Through Strategic and Normative Approaches – The Case of Romania in the EU Context, *Economies*, year 13, 5/2025, p. 1–24.
2. Buri, I.; van Hoboken, J., The Digital Services Act (DSA) proposal: a critical overview, Discussion paper, Digital Services Act (DSA) Observatory, Institute for Information Law (IViR), University of Amsterdam, 2021, p. 1-43.
3. Burke, D. D.; Doval, C. N., Redefining child pornography in an age of technological advancement: The concept of avoidable harm, *Washington Journal of Law, Technology & Arts*, year 20, 3/2025, p. 44-66.
4. Charisi, V.; Chaudron, S.; Di Gioia, R.; Vuorikari, R.; Escobar Planas, M.; Sanchez, I.; Gomez, E., Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2022, p. 1-87
5. Christensen, L.; Moritz, D.; Pearson, A., Psychological Perspectives of Virtual Child Sexual Abuse Material, *Sexuality & Culture*, year 25, 4/2021, p. 1353–1365.
6. Ducret, M.; Wahal, E.; Gruson, D.; Amrani, S.; Richert, R.; Mouncif Mougache, M.; Schwendicke, F., Trustworthy Artificial Intelligence in Dentistry: Learnings from the EU AI Act, *Journal of Dental Research*, year 103, 11/2024, p. 1–6.
7. Dushi, D.; Berdufi, N.; Karagianni, A., The legal framework and legal gaps for AI generated child sexual abuse material, *Computer Law & Security Review*, 59/2025, Article Number 106094.
8. Furizal; Ma'arif, A.; Maghfiroh, H.; Suwarno, I.; Prayogi, D.; Kariyamin; Lonang, S.; Sharkawy, A.-N., Social, legal, and ethical implications of AI generated deepfake pornography on digital platforms: A systematic literature review, *Social Sciences & Humanities Open*, Year 12, 2025, p. 1-25.
9. Ganesh, H. K., Protecting Children Through Deepfake Child Pornography: A Moral, Legal, and Philosophical Discussion on the Intersection of the

- Evolution in Law and Technology, *American Criminal Law Review*, 60/2022, p. 1-15.
10. Genç Geleç, B., Regulating digital platforms: Will the DSA correct its predecessor's deficiencies?, *Croatian Yearbook of European Law and Policy*, year 18, 2022, p. 25–60.
 11. Gsell, Florence, The Digital Services Act (DSA): A General Assessment, In: von Ungern Sternberg, Antje (ed.), *Content Regulation in the European Union – The Digital Services Act*, TRIER Studies on Digital Law, year 1, Verein für Recht und Digitalisierung e.V., Institute for Digital Law (IRDT), Trier, 2023, p. 11-332
 12. Karasavva, V.; Noorbhai, A., The Real Threat of Deepfake Pornography: A Review of Canadian Policy, *Cyberpsychology, Behavior, and Social Networking*, year 24, p. 203–209.
 13. Kietzmann, J.; Lee, L. W.; McCarthy, I. P.; Kietzmann, T. C., Deepfakes: Trick or Treat?, *Business Horizons*, year 63, 2/2019, p. 135–146.
 14. Kim, B.-J.; Jeong, S.; Cho, B.-K.; Chung, J.-B., AI Governance in the Context of the EU AI Act, *IEEE Access*, 2025, p. 144126-144142.
 15. Klimek, L., European responses criminalising online solicitation of children for sexual purposes, *Balkan Social Science Review*, 6/2020, p. 7–21.
 16. Lendvai, G. F., Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából, *Gondolat Kiadó*, Budapest, 2023, ISBN 978-963-556-465-1.
 17. Luan, T., A Survey on Deepfake Detection Technologies, *International Journal of Emerging Technologies and Advanced Applications*, 2/2025, p. 1-9.
 18. Makhrib, Z. F.; Karim, A. A., Digital Watermark Technique: A Review, *Journal of Physics: Conference Series*, year 1999, 2021, p. 1-10.
 19. Masood, M.; Nawaz, M.; Malik, K. M.; Javed, A.; Irtaza, A.; Malik, H., Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward, *Applied Intelligence*, 1/2022, p. 3974–4026.
 20. Negredo, L.; Herrero, Ó., Child pornography on the Internet, *Papeles del Psicólogo / Psychologist Papers*, year 37, 3/2016, p. 217-223.
 21. Novelli, C.; Casolari, F.; Rotolo, A.; Taddeo, M.; Floridi, L., Taking AI risks seriously: a new assessment model for the AI Act, *AI & Society*, year 39, 2024, p. 2493–2497.
 22. Parti, K.; Szabó, J.; The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe, *Laws*, year 13, 6/2024; Laws 78.
 23. da vidimPataki, M., Algoritmusok egynyelvű és különböző nyelvek közötti fordítások és plágiumok megtalálására, PhD dissertation, Pázmány Péter

- Katolikus Egyetem, Információs Technológiai Kar, Multidiszciplináris Műszaki Tudományok Doktori Iskola, 2012.
24. Patel, Y.; Tanwar, S.; Gupta, R.; Bhattacharya, P.; Davidson, I. E.; Nyameko, R.; Aluvala, S.; Vimal, V., Deepfake Generation and Detection: Case Study and Challenges, *IEEE Access*, 11/2023, p. 143296–143323.
 25. Rigotti, C.; Gkioka, C. P.; Do Rosario Da Graça, S.; Lannier, S., Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors, *New Journal of European Criminal Law*, 2025, p. 3-26.
 26. Rojszczak, M., Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232, *Computer Law & Security Review*, year 56, 2025. p. 1-14.
 27. Sandoval, M. P.; de Almeida Vau, M.; Solaas, J.; Rodrigues, L., Threat of deepfakes to the criminal justice system: a systematic review, *Crime Science*, year 13, 1/2024, p. 1-16.
 28. Schuett, J., Risk Management in the Artificial Intelligence Act, *European Journal of Risk Regulation*, year 15, 2/2023, p. 367–385.
 29. Sorbán, K., A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről, *Belügyi Szemle*, 10/2020, p. 81–104.
 30. Temir, E., Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism, *Selçuk İletişim Dergisi*, 2/2020, p. 1009–1024.
 31. Veszelszki, Á., Deepfake: kételkedés a kételyben, In: Aczél, P.; Veszelszki, Á. (eds.), *Deepfake: a valótlan valóság*, Gondolat Kiadó, Budapest, 2023, p. 13–31.
 32. Weikmann, T.; Greber, H.; Nikolaou, A., After Deception: How Falling for a Deepfake Affects the Way We See, Hear, and Experience Media, *The International Journal of Press/Politics*, 1/2025, p. 187–210.
 33. Whittaker, L.; Mulcahy, R.; Letheren, K.; Kietzmann, J.; Russell, R.; Bennett, B., Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda, *Technovation*, 1/2023, p. 1–17.
 34. Wilman, Folkert, The Digital Services Act (DSA) – An Overview, working paper, European Commission, 2022, p. 1-21.
 35. Zhang, T., Deepfake generation and detection, a survey, *Multimedia Tools and Applications*, 81/2022, p. 6259–6276.
 36. Zverev, V.; Bushkov, V.; Khrushkov, B.; Sarychev, V.; Ostaltsev, O.; Prokopovych-Tkachenko, Y., Artificial intelligence and cybercrime: New challenges and prospects for legal regulation, *Contemporary Issues in Artificial Intelligence*, 1/2025, p. 1-8.

LEGAL RULES

1. Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 326, 26.10.2012.
2. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011.
3. European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, Brussels, 2022.
4. European Commission, Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number independent interpersonal communications service providers for the processing of personal and other data for the purpose of combating child sexual abuse online, COM(2020) 568 final, Brussels, 2020.
5. 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.
42. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Official Journal of the European Union, L 2024/1689, 12.7.2024.

NETWORK RESOURCES

1. ASSEDEL (European Association for the Defense of Rights and Freedoms), Balancing Protection and Privacy in EU, online commentary, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.
2. ASSEDEL (European Association for the Defense of Rights and Freedoms), Regulation to Prevent and Combat Child Sexual Abuse (CSAR), policy analysis, 2026, https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February, 2026.

3. Choudhary, A. S., What is Variational Autoencoders? Data Science Blogathon 2025, <https://www.analyticsvidhya.com/blog/2023/07/an-overview-of-variational-autoencoders/>, 22 April, 2025.
4. Elcano Royal Institute, Risk without borders: the malicious use of AI and the EU AI Act's global reach, Analysis, <https://www.realinstitutoelcano.org/en/analyses/risk-without-borders-the-malicious-use-of-ai-and-the-eu-ai-acts-global-reach/>, 10 February, 2026.
5. Eurochild, Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse, news article, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.
6. European Commission, AI Act, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, 14 November, 2025.
7. European Commission, Code of Practice on marking and labelling of AI generated conten, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>, 9 January, 2026.
8. European Commission, Digital Services Act: keeping us safe online, 2025, https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en, 19 December, 2025.
9. European Commission, Supervision of the designated very large online platforms and search engines under the Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>, 10 February, 2026.
10. European Commission, The Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 8 October, 2025.
11. European Commission, The enforcement framework under the Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.
12. European Data Protection Board (EDPB), Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR, 2025, https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf, 10 December, 2025.
13. European Newsroom (ENR), Nudification blocks: The EU's struggle for more safety online, News article, 2026, <https://europeannewsroom.com/nudification-blocks-the-eus-struggle-for-more-safety-online/>, 6 February, 2026.
14. European Parliament, Combating child sexual abuse online, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025,

- [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.
15. European Parliament, Legislative Train 12.2025 – New legislation to fight child sexual abuse online, Legislative Train briefing, 2025, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.
 16. European Parliament, Proposal for a regulation laying down rules to prevent and combat child sexual abuse – Complementary impact assessment, European Parliamentary Research Service (EPRS), Brussels, 2023, [https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU\(2023\)740248_EN.pdf](https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU(2023)740248_EN.pdf), 2 March 2025.
 17. European Parliament, Children and deepfakes, Briefing, European Parliamentary Research Service (EPRS), 2025, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.
 18. Fauchoux, V., Transparency of AI Generated Content: In depth legal analysis of the Draft Code of Practice implementing Article 50 of the EU AI Act, 2026, <https://www.ddg.fr/actualite/transparency-of-ai-generated-content-in-depth-legal-analysis-of-the-draft-code-of-practice-implementing-article-50-of-the-eu-ai-act>, 15 February, 2026.
 19. Harkavy, R., EU moves to criminalise AI generated CSAM, Global Legal Insights, 2025, <https://www.globallegalinsights.com/news/eu-moves-to-criminalise-ai-generated-csam/>, 12 February, 2026.
 20. Internet Watch Foundation (IWF), How AI is being abused to create child sexual abuse imagery, institutional report, 2023, https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf, 18 January, 2026.
 21. Internet Watch Foundation (IWF), What has changed in the AI CSAM landscape?, AI CSAM Report Update, Version 1.1, July 2024, https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf, 5 January, 2026.
 22. Introduction to diffusion models for machine learning. Superannotate 2025, <https://www.superannotate.com/blog/diffusion-models#:~:text=Diffusion%20models%20are%20prominent%20in,distribution%20from%20the%20noisy%20data>, 25 June, 2025.
 23. Moreau, C., Commission proposes two-year extension to CSAM chat-scanning rules, Euractiv, <https://www.euractiv.com/news/commission-proposes-two-year-extension-to-csam-chat-scanning-rules/>, 7 January, 2026.
 24. O'Connor, R., Introduction to Diffusion Models for Machine Learning, Assemblyai 2022, <https://www.assemblyai.com/blog/diffusion-models-for-machine-learning>

introduction#:~:text=Let's%20dive%20in!,Diffusion%20Models%20%2D
%20Introduction,through%20the%20learned%20denoising%20process, 30
June, 2025.

25. Sensity, How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos, 2021, <https://sensity.ai/blog/how-to-detect-a-deepfake/>, 24 June, 2025.
26. U.S. Department of Homeland Security – Homeland Security Investigations, Artificial Intelligence and Combating Online Child Sexual Exploitation and Abuse, Know2Protect campaign, online infographic, https://www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_genai-bulletin.pdf, 3 January, 2026.