

DOI: 10.7251/GFP2616179R

UDC: 351.817:347.736/.739(4-672EU)

Pregledni naučni rad

Datum prijema rada:
30. maj 2026.

Datum prihvatanja rada:
10. jun 2026.

In the Shadow of Digital Exploitation: Regulating AI-CSAM within International and European Union Legal Frameworks

Abstract: The advancement of AI and deepfake technology challenges cybercrime frameworks through the emergence of AI-generated child sexual abuse material (AI-CSAM). Employing a legal-doctrinal approach, this study analyzes UN standards, the Budapest and Lanzarote Conventions, and EU frameworks. The research demonstrates that criminal law protection remains justified without identifiable victims, as banning synthetic content abstractly protects children's collective sexual integrity. While the EU pursues a three-pronged legislative strategy, various international declarations have emerged in response. The study concludes that from a legal perspective, effective child protection requires a shift toward systemic prevention, harmonizing global regulations with strict tech developer accountability.

Keywords: CSAM; AI and deepfake risks; international child protection; EU child protection framework.

1. INTRODUCTION

Rapid advances in artificial intelligence (AI) fundamentally transform digital content creation. Deepfake technology can now generate convincing visual depictions of non-existent individuals or events, creating unprecedented challenges for cybercrime regulation, particularly through AI-generated child sexual abuse material (AI-CSAM). Existing legal frameworks increasingly struggle to address synthetic sexual content involving children¹

These technological developments raises new interpretative questions concerning entirely AI-generated content and manipulated material involving real children. These developments require reconsideration of whether criminal law protection dependson identifiable victims or whether it also safeguards children's sexual integrity as an abstract collective legal interest.

Dóra Rengel

*Assistant Professor, PhD
candidate, University of Pécs,
Faculty of Law, Department of
Criminal Law
Doctoral School of Law,
University of Pécs, rengel,
Hungary; dora@ajk.pte.hu*

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

Combating child sexual exploitation remains a central priority at both international and EU levels. This article analyzes the international and EU legal frameworks governing AI-generated CSAM, focusing on conceptual ambiguities, enforcement challenges, and emerging legislative reforms.

2. DEEPFAKES

2.1. The Concept of Deepfakes

To assess AI-CSAM effectively, the underlying conceptual framework must first be clarified. EU law defines deepfakes in the Artificial Intelligence Act (AI Act) as AI-generated or manipulated image, audio, or video content resembling authentic persons, objects, or events and capable of appearing truthful to recipients.² The term combines “deep learning” and “fake” and has become one of the most significant forms of synthetic media.³

Within sexually explicit content involving children, deepfake technology primarily appears in two forms.⁴ First, existing recordings may be manipulated by superimposing the facial or bodily characteristics of real children onto sexually explicit material or by placing benign images into sexualized contexts. Such practices intensify the harm suffered by victims.⁵ Second, AI systems can generate entirely synthetic but hyper-realistic child characters and scenes through text-to-image prompts.⁶

2.2. Statistical Dimensions of the Deepfake Phenomenon

Deepfake proliferation is accelerating rapidly. Estimates indicate that online deepfake content increased from approximately 500,000 items in 2023 to more than 8 million by 2025.⁷

Approximately 98% of all deepfake content is pornographic in nature, demonstrating the overwhelming connection between synthetic media and sexual exploitation.⁸ Europol

² 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] OJ L 2024/1689, art 3(60)

³ Kietzmann, J., Lee, L. W., McCarthy, I. P., Kietzmann, T. C. (2019). *Deepfakes: Trick or Treat*, Business Horizons, 63, 2, pp. 135–146.

⁴ Ganesh, H. K. (2022). *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, pp. 7.

⁵ 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.

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

⁷ Negreiro, M., (July 2025), *Children and deepfakes*, EPRS, European Parliamentary Research Service, PE 775.855, pp. 2, [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.

⁸ Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A.-N. (2025). *Social, legal, and ethical implications of AI generated deepfake pornography on digital platforms: A systematic literature review*, Social Sciences & Humanities Open, 12, pp. 13.

further estimates that up to 90% of online content may become synthetically generated by 2026.⁹ Research also demonstrates the growing scale of sexually explicit deepfakes involving minors. One in seven internet users has encountered explicit deepfake content, while approximately 17% of AI-generated sexually explicit **material** involves minors.¹⁰

2.3. AI-CSAM and Criminal Legitimacy

The criminalization of victimless virtual content remains doctrinally controversial. Nevertheless, research demonstrates that virtual CSAM produces tangible societal harm by normalizing child sexual abuse, sustaining market demand, and distorting attitudes toward sexuality. Although empirical research specifically concerning deepfake-CSAM remains limited, analogous studies associate synthetic sexual abuse material with severe psychological harms, including anxiety, depression, and suicidal ideation.¹¹ Further studies suggest that consumption of virtual CSAM may contribute to real-world offending patterns.¹²

3. INTERNATIONAL REGULATION

3.1. The CRC and the Optional Protocol

Global regulation has become increasingly urgent as AI-generated illicit content already constitutes an operational law-enforcement challenge. Europol's "Operation Cumberland" dismantled a network dedicated to distributing synthetic child pornography, involving investigations across 19 countries.¹³

Article 34 of the UN Convention on the Rights of the Child does not expressly refer to technology; however, its prohibition of "all forms of sexual exploitation"¹⁴, supports a technology-neutral interpretation extending to digital and AI-driven abuse.¹⁵ This framework is reinforced by the Optional Protocol, which defines child pornography as any representation of a child engaged in "real or simulated" sexual activity.¹⁶ Nevertheless, synthetic AI-generated content creates doctrinal uncertainty. While "simulated" imagery likely covers

⁹ Orange, E. (2024). *The Impact of Synthetic Content*, In: *AI + The New Human Frontier: Reimagining the Future of Time, Trust + Truth*, Wiley AI, pp. 140.

¹⁰ Ofcom, (2024), *A deep dive into deepfakes that demean, defraud and disinform*, <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform>, 27 May, 2026.

¹¹ Karasavva, V., Noorbhai, A. (2021). *The Real Threat of Deepfake Pornography: A Review of Canadian Policy*, *Cyberpsychology, Behavior, and Social Networking*, 24, 3, pp. 204.

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

¹³ Europol, *25 arrested in global hit against AI-generated child sexual abuse material*, (28 February 2025), <https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material>, 27 February, 2026.

¹⁴ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art. 34.

¹⁵ UN Committee on the Rights of the Child, *General Comment No 25 (2021) on children's rights in relation to the digital environment* (2 March 2021) UN Doc CRC/C/GC/25 art. 7. pp. 81–82.

¹⁶ Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted 25 May 2000, entered into force 18 January 2002) 2171 UNTS 227, art 2.

deepfakes involving real minors, the legal status of entirely synthetic depictions remains contested because no identifiable victim exists.¹⁷ Consequently, the Optional Protocol permits but does not guarantee the criminalization of fully AI-generated CSAM.

However, a significant development occurred with the 2025 Joint Statement on AI and Children's Rights issued by ITU, UNICEF, UNESCO, and other UN bodies. The Statement classifies AI-generated and deepfake sexual content involving children as forms of psychological and sexual violence even where no real child is depicted. It further advocates criminalization of the full AI-CSAM spectrum and promotes "safety by design" measures, including filtering systems, age verification, and human oversight.¹⁸

3.2. Regulation Under the Budapest Convention

Article 9 of the Budapest Convention contains several provisions relevant to AI-CSAM. Paragraphs (2)(b) and (2)(c) introduced the categories of "a person appearing to be a minor" and "realistic images,"¹⁹ thereby anticipating synthetic or manipulated sexual imagery long before the emergence of generative AI. However, the Convention's effectiveness is weakened by the reservation mechanism contained in Article 9(4),²⁰ which permits States Parties to exempt themselves from criminalizing synthetic content.²¹

Importantly, the Explanatory Report to the Budapest Convention provides an important theoretical basis for modern AI-CSAM criminalization. Referring to morphing²² and image manipulation technologies, the Report recognized that synthetic material may legitimize abusive sexual interests, normalize exploitative conduct, and sustain harmful online subcultures. This reasoning shifts criminal law protection beyond identifiable victims toward broader collective legal interests. From a *de lege ferenda* perspective, it supports a reservation-free prohibition of AI-generated child sexual abuse material.²³

3.3. The Lanzarote Convention

As one of the primary instruments of international criminal law enforcement,²⁴ Article 20 of the Lanzarote Convention adopts a broad, technology-neutral definition of child pornography: „any material” that visually depicts:

- a real child;
- a simulated child participating in explicit sexual conduct;

¹⁷ Parti, K., Szabó, J. (2024). *The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe*, *Laws*, 13, 6, pp. 12–13.

¹⁸ Council of Europe; (2021), UNICEF, *Joint Statement on Artificial Intelligence and the Rights of the Child*, pp. 1-5, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_JOINT-2025-PDF-E.pdf 27 May, 2026.

¹⁹ Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185, art 9(2)(b)–(c) (hereinafter: Budapest Convention)

²⁰ Budapest Convention, art. 9 (4)

²¹ Fournier, J. (2010). *Reservations and the Effective Protection of Human Rights*, *Goettingen Journal of International Law*, 2, 2, pp. 439.

²² Aloraibi, A. Q. (2023). *Image Morphing Techniques: A Review*, *Technium*, 9, pp. 41.

²³ Council of Europe, *Explanatory Report to the Convention on Cybercrime* (23 November 2001) paras 101-102.

²⁴ Bitensky, S. H. (2010). *Introductory Note to Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse*, *International Legal Materials*, 49, 6, pp. 1663.

- or realistic representations of the sexual organs of a child for primarily sexual purposes.²⁵

Accordingly, the Convention is capable of covering both deepfake manipulations involving real minors and entirely synthetic AI-generated material. However, Article 20(3) permits States Parties to reserve the right not to criminalize purely simulated content involving non-existent children.²⁶ Consequently, the Convention does not strictly mandate criminalizing entirely AI-generated CSAM involving no real children. Since States may exempt these contents, the Lanzarote Convention fails to guarantee a fully harmonized level of international protection.

It is worth noting, however, that the Lanzarote Committee's 2024 Declaration reaffirmed that AI-generated and deepfake sexual content involving children falls within the Convention's scope through technology-neutral interpretation. The Declaration characterizes synthetic CSAM as facilitating grooming and exploitation and calls upon states to criminalize AI-generated material and strengthen platform accountability and reconsider reservations concerning simulated child pornography.²⁷

4. EU REGULATION

4.1. Directive 2011/93/EU and Its Reform

Directive 2011/93/EU establishes the central EU criminal law framework governing child pornography. Article 2 adopts a broad definition encompassing:

- visual depictions of children engaged in real or simulated sexual conduct;
- representations of children's sexual organs for sexual purposes;
- persons appearing to be children; and
- realistic images.²⁸

This framework potentially covers both virtual, pseudo²⁹- and manipulated child pornography, including deepfakes.³⁰ Nevertheless, the concepts of "realistic image" and "person appearing to be a child" remain interpretatively uncertain.³¹ The proposed Recast Directive may introduce relevant modifications to these definitions, analyzed subsequently. The existing regime also leaves a wide margin of appreciation to Member States: they may

²⁵ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (adopted 25 October 2007, entered into force 1 July 2010) CETS No 201, art 20(2) (hereinafter: Lanzarote Convention)

²⁶ Lanzarote Convention art. 20 (3)

²⁷ Lanzarote Committee, (2024), *Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies*, pp.3-5, <https://rm.coe.int/declaration-on-protecting-children-against-sexual-exploitation-and-sex/1680b25a78>, 22 December, 2026.

²⁸ Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L 335/1., art. 2(c). (hereinafter: Directive 2011/93/EU)

²⁹ Burke, D. D., Doval, C. N. (2025). *Redefining child pornography in an age of technological advancement: The concept of avoidable harm*, Washington Journal of Law, Technology & Arts, 20, 3, pp. 49.

³⁰ Negredo, L., Herrero, Ó. (2016). *Child pornography on the Internet*, Papeles del Psicólogo / Psychologist Papers, 37, 3, pp. 218.

³¹ Rigotti, C., Gkioka, C. P., Do Rosario Da Graça, S., Lannier, S. (2025). *Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors*, New Journal of European Criminal Law, pp. 17.

exempt child-appearing adults and decriminalize personal use of „realistic” content.³²

To address these shortcomings, the European Commission introduced Proposal COM(2024) 60 final to recast Directive 2011/93/EU. The proposal significantly broadens the concept of child sexual abuse material by expressly including:

- individuals appearing to be children;
- realistic digital or artificially generated images;
- virtual representations and avatars; and
- instructional content relating to child sexual abuse or online solicitation³³

The Recast Directive therefore explicitly criminalizes deepfake and AI-generated abuse while tightening existing exemptions.

4.2. The Proposed EU Chat Control Regulation

Alongside substantive criminal law reform, the European Commission proposed the “Chat Control” Regulation in May 2022 to impose direct obligations upon digital service providers. The proposal seeks to establish harmonized EU mechanisms for detecting, reporting, and removing CSAM while creating the European Centre to Prevent and Combat Child Sexual Abuse (EUCSA).³⁴ The proposal introduces mandatory risk-assessment and detection obligations for hosting services and encrypted messaging platforms such as WhatsApp and Signal.³⁵ Its precursor, the Interim Regulation, allowed a voluntary derogation from the confidentiality rules of Directive 2002/58/EC to detect, report and remove CSAM.³⁶

However, it generated significant criticism concerning privacy and fundamental rights, particularly regarding client-side scanning and potential infringements of Articles 7 and 8 of the EU Charter.³⁷ Conversely, the EU Council’s position, adopted on 26 November 2025, rejected mandatory detection, introducing a risk-category framework where client-side scanning remained an optional alternative.³⁸ By spring 2026, the legislative process reached a crisis point: the European Parliament rejected extending the Interim Regulation on 26 March 2026, and the Interim Regulation lapsed on 3 April 2026.³⁹

³² Directive 2011/93/EU, art 5(7)–(8).

³³ Rigotti et al., op. cit., note 33, pp. 17–20.

³⁴ 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, 2022/0155(COD), 11 May 2022 (hereinafter Chat Control)).

³⁵ ASSEDEL (European Association for the Defense of Rights and Freedoms), (2026), *Regulation to Prevent and Combat Child Sexual Abuse (CSAR), policy analysis*, pp. 1, https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February, 2026.

³⁶ European Commission, Proposal for a Regulation ... combating child sexual abuse online, COM(2020) 568 final (10 September 2020), pp. 1, (hereinafter: Interim Regulation).

³⁷ Negreiro, M., (January 2026), *Combating child sexual abuse online*, EPRS | European Parliamentary Research Service, PE 738.224, pp. 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.

³⁸ ASSEDEL (European Association for the Defense of Rights and Freedoms), (2026), *Balancing Protection and Privacy in EU, online commentary*, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

³⁹ Breyer, P., *Chat Control: The EU’s CSAM scanner proposal*, <https://www.patrick-breyer.de/en/posts/chat-control/>, 1 May, 2026.

4.3. The 2026 Amendment to the AI Act: The Omnibus VII Package

In March 2026, the Council adopted its negotiating mandate within the Digital Omnibus (Omnibus VII) package.⁴⁰ The proposal would amend Article 5 of the AI Act by classifying systems capable of generating synthetic CSAM or non-consensual intimate imagery as prohibited AI practices. This approach introduces an *ex ante* regulatory model targeting not only explicitly abusive software but also systems whose harmful outputs are reasonably foreseeable and insufficiently safeguarded. The proposal expressly requires technical protections, including prompt filters, refusal training, output controls, and data-scrubbing mechanisms.⁴¹ On 7 May 2026, the European Parliament and the Council of the European Union reached a provisional agreement on amendments to the AI Act, including an explicit ban on AI-generated CSAM.⁴²

5. CONCLUSION

This research demonstrates that modern technologies challenge the criminal justice system, requiring updated legal frameworks. Statutes must shift from traditional camera-recorded imagery toward „content” and „visual representation”, as AI-generated materials trigger the same harmful societal effects as authentic recordings.

Consequently, criminal law protection can no longer be confined to identifiable victims. While deepfakes violate specific minors’ dignity, purely machine-generated content attacks an abstract legal interest: the collective protection of children’s sexual integrity. To close regulatory gaps, the EU deploys a three-pronged legislative strategy:

- Substantive law: The Recast Directive overhauls definitions to criminalize synthetic CSAM.
- Platform regulation: Chat Control imposes detection obligations on digital networks.
- Source intervention: The Digital Omnibus VII package (complementing the AI Act) prohibits illicit image-generating AI applications.

Ultimately, *ex post* sanctions are insufficient. Effective child protection requires integrating criminal law with preventive, „safety by design” technological safeguards. Tech developers must ensure automated safety filters, age verification, and data exclusion *ab initio*, balanced by continuous human oversight to prevent over-censorship.

⁴⁰ Council of the European Union, (13 March 2026), *Council agrees position to streamline rules on artificial intelligence*, <https://www.consilium.europa.eu/en/press/press-releases/2026/03/13/council-agrees-position-to-streamline-rules-on-artificial-intelligence/>, 18 March, 2026.

⁴¹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – Mandate for negotiations with the European Parliament*, 7322/26, 13 March 2026.

⁴² Council of the European Union and European Parliament, (7 May 2026), *Artificial Intelligence: Council and Parliament agree to simplify and streamline rules*, <https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/>, 29 May 2026.

LITERATURE

Monographs, Articles

- Aloraibi, A. Q. (2023). Image Morphing Techniques: A Review, *Technium*, 9, pp. 41–53.
- Bitensky, S. H. (2010). Introductory Note to Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, *International Legal Materials*, 49(6), pp. 1663–1682.
- Burke, D. D., Doval, C. N. (2025). Redefining child pornography in an age of technological advancement: The concept of avoidable harm, *Washington Journal of Law, Technology & Arts*, 20(3), pp. 44–66.
- Dushi, D.; Berdufi, N.; Karagianni, A. The legal framework and legal gaps for AI generated child sexual abuse material, *Computer Law & Security Review*, 59, Article Number 106094.
- Fournier, J. (2010). Reservations and the Effective Protection of Human Rights, *Goettingen Journal of International Law*, 2(2), pp. 437–462.
- Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A.-N. (2025). Social, legal, and ethical implications of AI generated deepfake pornography on digital platforms: A systematic literature review, *Social Sciences & Humanities Open*, 12, pp. 1–25.
- Ganesh, H. K. (2022). 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, pp. 1–15.
- Karasavva, V., Noorbhai, A. (2021). The Real Threat of Deepfake Pornography: A Review of Canadian Policy, *Cyberpsychology, Behavior, and Social Networking*, 24(3), pp. 203–209.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., Kietzmann, T. C. (2019). Deepfakes: Trick or Treat, *Business Horizons*, 63(2), pp. 135–146.
- Klimek, L. (2020). European responses criminalising online solicitation of children for sexual purposes, *Balkan Social Science Review*, 6, pp. 7–21.
- Negredo, L., Herrero, Ó. (2016). Child pornography on the Internet, *Papeles del Psicólogo / Psychologist Papers*, 37(3), pp. 217–223.
- Orange, E. (2024). The Impact of Synthetic Content, In: *AI + The New Human Frontier: Reimagining the Future of Time, Trust + Truth*, Wiley AI.
- Parti, K., Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe, *Laws*, 13(6), 67. <https://doi.org/10.3390/laws13060067>
- Rigotti, C., Gkioka, C. P., Do Rosario Da Graça, S., Lannier, S. (2025). Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors, *New Journal of European Criminal Law*, pp. 3–26.
- Zverev, V., Bushkov, V., Khrushkov, B., Sarychev, V., Ostaltsev, O., Prokopovych-Tkachenko, Y. (2025). Artificial intelligence and cybercrime: New challenges and prospects for legal regulation, *Contemporary Issues in Artificial Intelligence*, 1, pp. 1–8.

Online Sources

- ASSEDEL (European Association for the Defense of Rights and Freedoms) (2026). Balancing Protection and Privacy in EU. <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February 2026.
- ASSEDEL (European Association for the Defense of Rights and Freedoms) (2026). Regulation to Prevent and Combat Child Sexual Abuse (CSAR). https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February 2026.
- Breyer, P. Chat Control: The EU's CSAM scanner proposal. <https://www.patrick-breyer.de/en/posts/chat-control/>, 1 May 2026.
- Council of Europe; UNICEF (2021). Joint Statement on Artificial Intelligence and the Rights of the

- Child. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_JOINT-2025-PDF-E.pdf, 27 May 2026.
- Council of the European Union (13 March 2026). Council agrees position to streamline rules on artificial intelligence. <https://www.consilium.europa.eu/en/press/press-releases/2026/03/13/council-agrees-position-to-streamline-rules-on-artificial-intelligence/>, 18 March 2026.
- Council of the European Union and European Parliament, (7 May 2026), Artificial Intelligence: Council and Parliament agree to simplify and streamline rules, <https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/>, 29 May 2026.
- Europol (28 February 2025). 25 arrested in global hit against AI-generated child sexual abuse material. <https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material>, 27 February 2026.
- Harkavy, R., (2025), EU moves to criminalise AI-generated CSAM, Global Legal Insights. <https://www.globallegalinsights.com/news/eu-moves-to-criminalise-ai-generated-csam/>, 12 February, 2026.
- Internet Watch Foundation (IWF) (October 2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf, 18 January 2026.
- Lanzarote Committee (2024). Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies. <https://rm.coe.int/declaration-on-protecting-children-against-sexual-exploitation-and-sex/1680b25a78>, 22 December 2026.
- Negreiro, M. (January 2026). Combating child sexual abuse online, EPRS | European Parliamentary Research Service, PE 738.224. [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.
- Negreiro, M. (July 2025). Children and deepfakes, EPRS, European Parliamentary Research Service, PE 775.855. [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.
- Ofcom (2024). A deep dive into deepfakes that demean, defraud and disinform. <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform>, 27 May 2026.
- U.S. Department of Homeland Security – Homeland Security Investigations. Artificial Intelligence and Combating Online Child Sexual Exploitation and Abuse, Know2Protect campaign. https://www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_genai-bulletin.pdf, 3 January 2026.

Legal Sources

- Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3
- Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185 (Budapest Convention)
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (adopted 25 October 2007, entered into force 1 July 2010) CETS No 201 (Lanzarote Convention)
- Council of Europe, Explanatory Report to the Convention on Cybercrime (23 November 2001)
- Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – Mandate for negotiations with the European Parliament, 7322/26, 13 March 2026.
- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L 335/1.
- European Commission, Proposal for a Regulation ... combating child sexual abuse online, COM(2020) 568 final, 10 September 2020 (Interim Regulation).

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, 2022/0155(COD), 11 May 2022.

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted 25 May 2000, entered into force 18 January 2002) 2171 UNTS 227.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L 2024/1689.

UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment (2 March 2021) UN Doc CRC/C/GC/25.



This work is licensed under a **Creative Commons Attribution-NonCommercial 4.0 International License**.