



17.9.2024

## NOTICE TO MEMBERS

**Subject: Petition No 1256/2023 by Lorena Portabales Rodríguez (Spanish) on Artificial Intelligence and child pornography**

### 1. Summary of petition

The petitioner expresses concern about Artificial Intelligence in relation to child pornography. According to her, a clear example of this is that a number of artificial intelligence systems have been created that allow faces or bodies of different people to be replaced or for data from a database to be used to generate an image that looks real and is difficult to distinguish from an original one. This could lead to a greater distribution of child pornography, which would not constitute a criminal offence it would not be real but created through artificial intelligence. The petitioner considers that measures should be taken to prevent this by inserting a filter into artificial intelligence algorithms prohibiting the creation of pornographic images or videos.

### 2. Admissibility

Declared admissible on 25 March 2024. Information requested from Commission under Rule 233(5), former Rule 227(5).

### 3. Commission reply, received on 6 August 2024

#### The Commission's observations

The Commission shares the concerns expressed by the petitioner that the latest advancements in Artificial Intelligence (AI) may lead to the spread at scale of deep fakes, including most disturbingly deep fake content featuring child pornography or naked images of women and minors. The right to dignity, privacy and safety of all individuals are enshrined in EU and national legislation and must be respected offline as well as online and regardless of whether AI is used or not.

In this regard, it should be noted that the production and dissemination of child sexual abuse material, including realistic material generated through artificial intelligence, is a criminal offence in the EU under Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography<sup>1</sup>. On 6 February 2024, the Commission presented a proposal for a revision of the Directive<sup>2</sup>, which reinforces such criminalisation by updating the definition of child sexual abuse material, to ensure that it explicitly covers all possible technological developments, including AI-generated content, in a sufficiently technology-neutral and hence future-proof way. Furthermore, the proposal for a Regulation to prevent and combat child sexual abuse<sup>3</sup> would require companies to systematically assess and mitigate the risk of child sexual abuse on their services (i.e., by implementing ‘child safety by design’) and, if prevention is not sufficient, to detect, report, remove and block online child sexual abuse material, including material produced through AI.

In relation to the misuse of AI for the generation of non-consensual naked imaged, it is relevant to mention Directive (EU) 2024/1385 on combating violence against women and domestic violence<sup>4</sup>, which was adopted on 7 May 2024. This Directive is the first legal EU-instrument that deals with these types of violence in a holistic manner. It does so by providing a set of minimum standards regarding the criminalisation of certain forms of violence (both online and offline), provide support and protection to victims, enhances prevention and the access to justice. The Directive applies also to child victims and has special attention to needs of child victims without prejudice to *lex specialis* rules on child sexual abuse material. This Directive amongst others requires Member States to criminalise the sharing of intimate material, meaning material depicting the intimate parts of a person or a person engaged in sexual activities, without the permission of the depicted person. This includes the creation of such intimate content through AI or photoshop, the so-called ‘deep fakes’ and their consequent dissemination. However, the prohibition to create and share deep fakes only applies to deep fakes depicting a person engaged in sexual activities. According to this Directive, Member States must foresee measures for the prompt removal of such content or disabling access to such content.

In addition, the EU co-legislators reached a political agreement on the Artificial Intelligence Act (AI Act)<sup>5</sup>, the first comprehensive regulation for AI worldwide. The Act was voted by the European Parliament on 13 March 2024 and entered into force on 1 August 2024. It aims to address risks to health, safety and fundamental rights,

---

<sup>1</sup> 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, OJ L 335/1, 17 December 2011.

<sup>2</sup> Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast), COM/2024/60 final, 6 February 2024.

<sup>3</sup> 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, 11 May 2022.

<sup>4</sup> Directive (EU) 2024/1385 of the European Parliament and of the Council on combating violence against women and domestic violence, OJ L, 2024/1385, 24 May 2024.

<sup>5</sup> 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) (Text with EEA relevance), OJ L, 2024/1689, 12 July 2024.

while supporting innovation and the development and uptake of trustworthy AI in the EU. The new rules are horizontal in scope and follow a risk-based approach with proportionate requirements depending on the level of risks posed by the various AI applications.

For deep fakes, the AI Act envisages transparency obligations to avoid the risk of manipulation and deception. Deployers of generative AI systems will need to clearly label ‘deep fakes’ that appreciably resemble people as well as certain types of AI-generated text published on matters of public interest. In addition, providers of generative AI systems will have to implement technical solutions such as watermarks and other methods to ensure the content generated or manipulated by AI is marked and detectable as such in an effective and reliable manner as far as technically feasible.

The AI Act also prohibits certain particularly harmful and abusive practices. This includes AI systems that exploit vulnerabilities of children with the objective or the effect of materially distorting children’s behaviour in a significantly harmful manner. AI systems that deploy purposefully manipulative or deceptive techniques with the objective or the effect of materially distorting the behaviour of a person or groups of persons in a significantly harmful manner will also be banned. The prohibitions will become applicable six months after the Act’s entry into force, i.e. from 2 February 2025.

The Commission will issue guidelines to provide legal certainty and concrete examples of applications that could be covered by these prohibitions. In preparing the guidelines, the Commission will analyse whether AI applications that create child sexual abuse material could be covered by this prohibition as applications that exploit children’s vulnerabilities and can be used to coerce, force, threaten children or otherwise influence their behaviour in a way that can harm them significantly, including by endangering their safety, physical and psychological integrity and personal development. In preparing the guidelines, the Commission will also analyse whether the AI applications that create nude images of women without consent could be covered by the prohibition for purposefully deceptive and manipulative techniques.

Finally, the Digital Services Act<sup>6</sup>, which entered into force on 16 November 2022, also includes provisions to identify and mitigate the risks stemming from the spread of deep fakes on online platforms operating in the EU, as well as flagging mechanisms. Tiered due diligence obligations imposed on the providers of intermediary services range from content moderation policies and notice mechanisms to complaint-handling systems, risk assessments, mitigation measures and possible sanctions to tackle the illegal dissemination of deep fakes.

## Conclusion

The Commission recommends the PETI Committee to consider these legislative developments when reviewing the petitions. It will also further cooperate with the Committee to ensure the effective implementation of these legal acts and to address the misuse of AI for the generation of these most unacceptable forms of deep fakes.

---

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>