Deepfakes and Transparency Obligations

Célia Zolynski*

ANNOTATED TRANSCRIPT

[ZOLYNSKI] First of all, I would like to thank Professor Jane Ginsburg, all the organizers, and the Paris Global Alliance program who made this comparative symposium possible. I'm delighted to be with you today. I propose to share my thoughts from an EU perspective about deepfakes and the current legal framework in the EU, and the potential evolution of this legal framework. This analysis is the result of current research I'm leading for the French Commission of Human Rights about teen intimacy and digital services,[1] a legal study for the French Agency for Food, Environmental and Occupational Health & Safety (ANSES) on the use of social media by adolescents and its health risks,[2] and another study for the Ministry of Culture about deepfakes in the creative sector.[3]

Let's begin with what we are talking about. From this morning's presentations we understand that the very notion of deepfakes is not so clear. There are many definitions of what deepfakes are and what the legal definition should cover. In this regard, the definition proposed by the AI Act is particularly interesting. In accordance with article 3(60) of the EU AI Act:[4]

---

* Professor of Law, Université Paris 1 Panthéon Sorbonne – Co-director of the Paris 1 AI Observatory.

1. CNCDH, *Avis sur la protection de l'intimité des jeunes en ligne*, A-2025-1 (January 2025), https://www.cncdh.fr/publications/avis-sur-la-protection-de-lintimite-des-jeunes-en-ligne-2025-1

2. Célia Zolynski et al., *Mineurs et Réseaux Sociaux: Étude des Dispositifs Légaux Relatifs à l'Usage des Réseaux Sociaux par les Mineurs*, IRJS [SORBONNE INST. LEGAL RSCH.] (Nov. 2025), https://www.anses.fr/system/files/Etude-juridique-IRJS-novembre-2025.pdf [https://web.archive.org/web/20260324230127/https://www.anses.fr/system/files/Etude-juridique-IRJS-novembre-2025.pdf].

3. *Le CSPLA Lance une Mission Relative aux Enjeux pour les Secteurs Culturels et Créatifs des Hypertrucages Générés ou Manipulés par l'intelligence Artificielle*, MINISTERE DE LA CULTURE (FR.), "(June 20, 2025), https://www.culture.gouv.fr/nous-connaitre/organisation-du-ministere/Conseil-superieur-de-la-propriete-litteraire-et-artistique-CSPLA/travaux-et-publications-du-cspla/missions-du-cspla/le-cspla-lance-une-mission-relative-aux-enjeux-pour-les-secteurs-culturels-et-creatifs-des-hypertrucages-generes-ou-manipules-par-l-intelligence-ar [https://perma.cc/2EAE-UTU2].

4. Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and amending Regulations 300/2008, 167/2013, 168/2013,

> 'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful[.]

This is a very comprehensive definition focused on synthetic content.[5] It includes not only deepfakes of people, but any image, text, audio, or video created or manipulated by AI. At least two questions arise from this definition. First, where the text states "audio or video content that resembles existing persons," does that mean that a wholly invented person (a "synthetic person" as Professor [Jennifer] Rothman referenced) would not be a deepfake because it does not correspond to an actual person? The other objects of imitation in the definition, notably "events," however, suggest that the definition is intended to encompass the wholly fabricated as well as imitations based on actual "persons, objects, places, entities or events." To omit the wholly fabricated would mean that the text does not cover a great deal of false and misleading content. Such an omission seems inconsistent with the AI Act's overall goal to promote transparency to limit the risk of public manipulation.[6] Second, does the definition's statement that the content "would falsely appear" imply that a "deepfake" must have been created with a misleading purpose? Given the wording of article 3(60) of the AI Act, we can consider that this provision does not require proof that the producer of the content intended to mislead the public into believing that the content is real.

Beyond that, we need to ask whether deepfakes warrant regulatory attention. How are deepfakes novel or different from other kinds of false representations? Drawing an image or even creating a video does not present the same risk of being confused with reality because the representation is subjective. We understand that it is a representation perceived or constructed by the author. Therefore, the concept of representation brings us back to the classic debate about the relationship with the audience and fiction. Many consider that this debate is renewed with deepfakes, because some believe that hyper-realistic AI-generated or AI-manipulated content could make the public perceive the representation as real, or could prevent the public from taking a critical distance from the object. In other words, deepfakes could blur the line between fiction and reality.

Given this phenomenon, it seems important to take into account the context of what the deepfake was intended for, through understanding, as Jennifer Rothman explained this morning, that deepfakes are not a unique phenomenon. We therefore need to take into consideration the various purposes that deepfakes can serve. Several issues of concern should be mentioned here. A number of them appear to be particularly significant. One concerns the potential distortion of the information landscape, with the proliferation of synthetic media content that is now presented as if it were

---

2018/858, 2018/1139 and 2019/2144 and Directives 2014/90, 2016/797 and 2020/1828 [hereinafter "EU AI Act"], art. 3(60), 2024 O.J. (L 1689) 50.

5. Synthetic content refers to any form of media (text, images, audio, or video) that is either partially or fully created or significantly manipulated using artificial intelligence (AI) and machine learning techniques, rather than being captured directly from real-world events.

6. *See* Mateusz Labuz, *Deep Fakes and the Artificial Intelligence Act—An Important Signal or a Missed Opportunity?* 16 POL'Y & INTERNET 783 (2024); *infra* notes 10, 16 and accompanying text.

authentic; indeed, we observe the impact of a saturation of the digital space with the dissemination of a massive amount of inauthentic content which competes for viewers' attention in an already crowded online space. In addition, we need to take into account the massive infringement of individual rights that can result from the production and the sharing of non-consensual intimate images and child sexual abuse material.

Many of the issues surrounding deepfakes were beginning to be discussed years ago but are now more widely recognized. They are highlighted as a main concern by the International AI Safety Report 2025.[7] This report outlines a variety of risks to individuals and to society, such as misinformation, gender-based violence, and erosion of public trust in digital media, among others.[8]

The European authorities decided to tackle several of these issues by adopting the EU AI Act in 2024.[9] In this context, we observe that deepfakes are captured by the various layers of the AI Act (Part I) and that transparency has been considered a cornerstone of the regulation, whose effectiveness however remains limited, which leads to proposals for enhancements aimed at strengthening it (Part II).

I. DEEPFAKES CAPTURED BY THE VARIOUS LAYERS OF THE AI ACT

The AI Act is a regulation that aims to create a single EU market and harmonize rules to promote trustworthy and human-centric AI, based on compliance mechanisms and what we call a logic of risks. The goal is to promote innovation, but also to tackle the level of risks regarding safety and regarding human rights, democracy, and the rule of law. From this perspective, one of the principles of the AI Act is not to consider the technique itself, but its uses. Deepfake regulation is a perfect example of this regulatory approach of raising flags, sometimes red flags, but also of pushing innovation. However, the regulation of deepfakes illustrates how difficult it can be to promote both at the same time, especially considering that deepfake techniques can be used for various purposes and in various contexts.

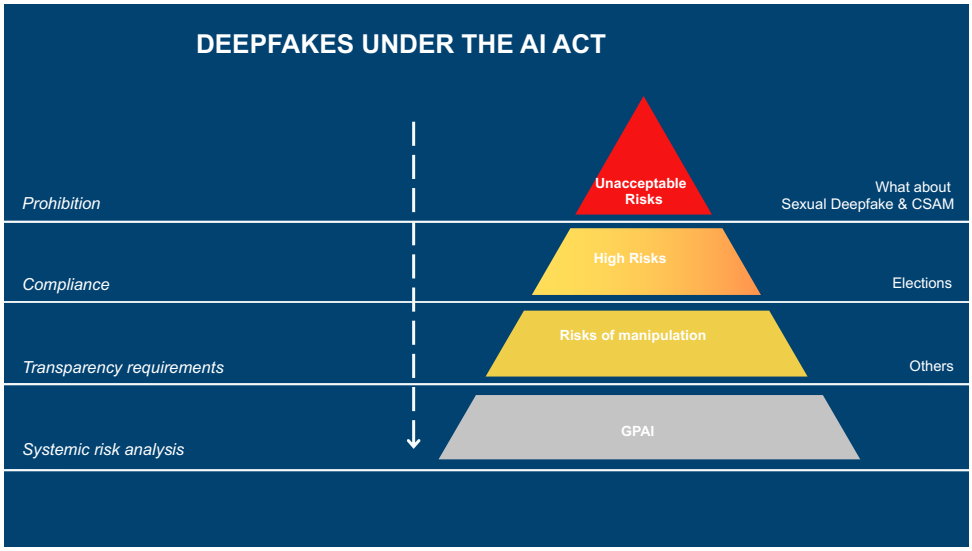
Sometimes deepfakes offer great opportunities that are socially desirable, for education, information, creation, and so on. But they can also cause massive harms, disinformation, fraud, bullying, harassment, and infringement to dignity. Because they

7. Yoshua Bengio et al., *International AI Safety Report,* AI ACTION SUMMIT (2025), https://internationalaisafetyreport.org/sites/default/files/2025-10/international_ai_safety_report_2025_english.pdf [https://web.archive.org/web/20260206184406/https://internationalaisafetyreport.org/sites/default/files/2025-10/international_ai_safety_report_2025_english.pdf].

8. Among harms to individuals caused by fake content, the report lists deepfakes' propensity to: extort, scam, psychologically manipulate, or sabotage targeted individuals or organizations; impersonate authority figures or trusted individuals to commit financial fraud; blackmail individuals for extortion purposes; sabotage individuals in their personal and professional lives, violating rights 'to one's honor and reputation; create abuse through fake pornographic or intimate content overwhelmingly targeting women; and distinctly harm children via AI-generated sexual content. *Id.* at 62–63.

9. EU AI Act, *supra* note 4.

can have non-harmful purposes, deepfakes have not been prohibited per se by the AI Act, even though it was suggested. Nevertheless, the EU authorities have identified the need to preserve the public interest by avoiding specific risks of manipulation and malicious uses. This was one of the main goals of the AI Act, both during its negotiation and at the moment of its adoption in June 2024. The idea was to divide AI into risk levels and to prohibit, among other things, those uses that cause significant harm through manipulation, impersonation, and deception. There was also great concern about the integrity of the information ecosystem and of elections. Considering these risks, deepfakes could be captured by the different layers of the AI Act regulation.[10]



The AI Act recognizes that some deepfakes could be considered in the category of ""high risk,"" a qualification that determines the application of most of the compliance requirements implemented by the regulation. In doing so, the EU legislature recognizes that deepfake technology is not problematic in itself and that deepfakes are not a unique phenomenon. However, certain contexts of use lead us to consider the risk that requires regulation. This is a perfect illustration of the AI Act regulation logic that takes into account the context of the use. The use of deepfakes in an electoral context specifically falls under this category due to their potential for manipulation and the spread of electoral disinformation (considering the dangers to the integrity of votes and democratic processes that we could face). For all other uses, the AI Act imposes transparency requirements to address the risk of manipulating the public exposed to deepfakes.

This raises the question of whether the use of certain types of content should be prohibited. In this regard, it should be noted that the AI Act defines a list of prohibited uses of AI, by identifying so called "unacceptable risks" regarding safety and

10. For critiques of such classifications, see Labuz, *supra* note 6.

fundamental rights. Those are set out in article 5 of the AI Act, which includes no mention of deepfakes.[11] This omission is very controversial and may be revisited considering harmful issues of non-consensual sexual deepfakes and child sexual abuse material (CSAM) [12]. In February 2025, the EU Commission published guidelines to interpret article 5 of the AI Act that mention NCII (Non-Consensual Intimate Imagery) and CSAM as possible prohibited uses.[13] But the conditions necessary to apply the prohibitions of article 5 are very strict, and we are not sure that NCII and CSAM could satisfy all. In considering this, we must promote the evolution of the text to address such harmful uses.

Finally, this whole risk assessment structure is completed by imposing a specific obligation on providers of GPAI (General-Purpose AI) systems and GPAI models that could cause systemic risks,[14] now described by the Safety and Security Chapter of the Code of Practice published by the EU in July 2025.[15] The Code mentions that specific uses of deepfakes such as CSAM and NCII can generate systemic risks. This recognition arrives late, but makes it possible to take such deepfakes into account indirectly.

II. TRANSPARENCY: A CORNERSTONE OF REGULATION TO CAPTURE DEEPFAKE RISKS

Under the AI Act, it is therefore important to note that most deepfakes are regulated only by the Act's transparency requirements. The goal is to ensure trustworthiness of AI systems by maximizing transparency as users are exposed to their outputs. This is in

11. EU AI Act, *supra* note 4, art. 5.

12. This will be covered by EU Member States legislation. *See* Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, O.J. (L 1385). For instance, in France, the publication of synthetic intimate imagery (NCII) has been a criminal offense since 2024. CODE PÉNAL, art. 226-8-1 (Fr.). *See* Zolynski et al., *supra* note 2 and CNCDH, *supra* note 1.

13. *See* EUROPEAN COMM'N, *Guidelines on the Definition of an Artificial Intelligence System* (2025), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application [https://web.archive.org/web/20260219200600/https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application]; EUROPEAN COMM'N, *Guidelines on Prohibited Artificial Intelligence Practices Under Regulation (EU) 2024/1689* (Feb. 2025), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act [https://web.archive.org/web/20260219200600/https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act].

14. The AI Act describes "systemic risks": "General-purpose AI models could pose systemic risks which include, but are not limited to, any actual or reasonably foreseeable negative effects in relation to major accidents, disruptions of critical sectors and serious consequences to public health and safety; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content." *See* EU AI Act, *supra* note 4, recital 110.

15. EUROPEAN COMM'N, *Code of Practice on General Purpose AI* (July 2025), https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai [https://web.archive.org/web/20260219185012/https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai]. Under the EU AI Act, they will have to identify and mitigate those risks. *See* Regulation (EU) 2024/1689, art. 55.

order to protect the public from malicious users and disinformation.[16] We need to understand here whether these transparency requirements should be the cornerstone of the regulation. In other words, does such transparency offer sufficient remedies, or should it be considered insufficient to ensure the interests of the public?

My first aim is to identify the questions raised by the AI Act's transparency approach imposing specific requirements to address deepfake risks. My second aim is to determine how transparency could be an effective means of addressing the potential risks we have mentioned, by considering not only obligations of technical transparency, but also the ensemble of governance mechanisms ensuring public access to information through external, independent oversight to build a so-called "*regulation through transparency.*"

A. TRANSPARENCY REQUIREMENTS (HOW AND WHAT FOR?)

Article 50 of the AI Act introduced two levels of transparency requirements that will take effect in August 2026.[17] First, AI providers must design their AI systems, including general purpose ones, to mark, in a machine-readable format that can be detected, outputs as artificially-generated or manipulated.[18] The lengthy AI Act Recitals specify what kind of technical tools can be used, using techniques such as watermarking, for example.[19] The aim here is to facilitate trustworthy detection and identification of AI-generated and manipulated content. In addition, there is a labeling requirement imposed on the deployers of AI systems.[20] They must label deepfakes in such a way that the public can be informed of the synthetic nature of the content. Under article 50(5), information must be provided in a clear and distinguishable manner at the latest at the time of the first interaction of exposure.[21]

Because these provisions could be quite difficult to implement for these actors, guidelines and a code of conduct will be published to better define such requirements, helping deployers and providers of GenAI systems to detect and label AI or manipulated content.[22] These texts, which are considered soft law in European Union law, will

16. Labuz, *supra* note 6, at 791 ("The very basic idea of transparency obligations in relation to deep fakes is to enable the recipients to make informed choices on displaying the material and spot that the epistemic value of the material displayed has changed. It is therefore expected that appropriate markings will serve as a warning to users and a safeguard against dis- and misinformation.").

17. EU AI Act, *supra* note 4, art. 50.

18. *Id.* art. 50(2).

19. *Id.* recital 133.

20. *Id.* art 50(4) (defining a deployer as "a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity").

21. *Id.* art. 50(5).

22. EUROPEAN COMM'N, *FAQs: Guidelines and Code of Practice on Transparent AI Systems* (2025), https://digital-strategy.ec.europa.eu/en/faqs/guidelines-and-code-practice-transparent-ai-systems [https://web.archive.org/web/20260210150922/https://digital-strategy.ec.europa.eu/en/faqs/guidelines-and-code-practice-transparent-ai-systems]; EUROPEAN COMM'N, *Stakeholder Consultation on Transparency Requirements for Certain AI Systems under Article 50 of the AI Act* (2025), https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-develop-guidelines-and-code-practice-

specify the technical requirements and how to take into account the context of the deepfake. This seems essential considering the various challenges we already can identify with respect to the transparency requirements imposed by the AI Act.

In particular, many limits and challenges have been identified respecting the effectiveness of these new requirements imposed by the AI Act considering that the goal pursued here, as mentioned, is to ensure the trust of the user and the general public and to avoid the risk of manipulation.

Some concerns have already been taken into account by the AI Act itself. For example, the text addresses the need to preserve freedom of expression, freedom of creation, and freedom of science.[23] In this context, the AI Act still requires labeling, but specifies that the label can be adapted so as not to hamper the display or enjoyment of the work.[24] Thus, this is not a total exemption in case of creative or scientific content. This approach prompts the question: What is artistic content? The AI Act provides that the content has to be a work that is *evidently* artistic, creative, satirical, fictional, or analogous. While "evidently" suggests an endeavor to avoid pretextual claims of artistic content, the open-ended phrase "or analogous work" risks expanding the universe of content benefitting from a relaxed labelling requirement.

There are also other limits and challenges to transparency, such as technical ones. The Coalition for Content, Provenance, and Authenticity (C2PA) is currently working on watermarking.[25] In France, for example, the Provenance for Trust initiative aims at proposing to create a coalition of researchers and authentication services including the Journalism Trust Initiative (founded by Reporters without Borders),[26] working with experts on labeling content and detecting AI-generated content, to propose open source technical solutions and specific certification mechanisms for media.

There are a lot of technical challenges to consider, especially regarding the robustness and accuracy of watermarks.[27] More generally, we need to take into account other challenges to reach the goal pursued, such as the limits of label's ability to inform

transparent-ai-systems [https://web.archive.org/web/20260219152742/https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-develop-guidelines-and-code-practice-transparent-ai-systems].

23. For example, deepfakes can be used in video games to create a non-player character using motion picture techniques. In a historical context, deepfakes can be used to produce counterfactual history. *See, e.g.*, LE MONDE SELON L'IA: EXPLORER LES ESPACES LATENTS [THE WORLD THROUGH AI: EXPLORING LATENT SPACES] (Jeu de Paume & JBE Books, 2025).

24. *See* EU AI Act, *supra* note 4, art. 50(4) ("Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.").

25. COAL. FOR CONTENT, PROVENANCE & AUTHENTICITY, https://c2pa.org/ [https://web.archive.org/web/20260221005527/https://c2pa.org/] (last visited Mar. 24, 2026).

26. PROVENANCE FOR TRUST INITIATIVE, https://www.provenance4trust.org/ [https://web.archive.org/web/20260128180453/https://www.provenance4trust.org/] (last visited Mar. 24, 2026).

27. EUROPEAN PARLIAMENT, *Generative AI and Watermarking* (2023), https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf [https://web.archive.org/web/20260204172313/https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf]; EUROPEAN COMM'N, *Stakeholder Consultation*, *supra* note 22.

the public of the nature of the deepfake. This means that we need specific analysis to ensure that the goal pursued can be reached, whereas Article 50 of the AI Act is very general concerning the information to be provided.[28] Here, academics and researchers are of critical importance in identifying appropriate labels and addressing cognitive biases.[29] We also have to address the enforcement problem considering that "malicious actors will simply not adhere to the obligations."[30] Beyond that, it is essential to consider an epistemic issue regarding the impact on public opinion of the dissemination of a massive amount of fake synthetic content even if the deepfakes are labeled as such. In this context, transparency requirements might not be enough to prevent public manipulation.

That is the reason why it is critical to take action for the education and resilience of the public and to consider the relationship between users and the information space, in order to ensure better user agency.[31] Regarding all of this, we need to go a step further to understand if transparency is a sufficient remedy to limit the harmful impact of deepfakes. In order to reach this goal, we need to assess transparency not only as meeting specific technical or legal requirements but also whether it achieves genuine transparency in fact.

B. REGULATION THROUGH TRANSPARENCY (TAKE IT A STEP FURTHER)

Considering these limits and challenges, we need to go a step further to take the public interest into account by promoting not only transparency requirements but also regulation through transparency.

First and foremost, it means involving third parties (regulators, academics, NGOs) in reviewing the transparency measures imposed by the AI Act to be adopted in order to achieve the intended objective—namely, to avoid the risk of public manipulation—and to ensure their effectiveness.

To this end, AI systems and model providers should first publish periodic transparency reports detailing the various measures taken and why they were chosen. This should be supplemented by the periodic publication of risk assessment reports required for providers subject to the AI Act. These reports would describe how providers have identified the systemic risks caused by the generation of deepfakes from their models and what mitigation measures have been taken to effectively limit these

28. Martina J. Block, *A Critical Evaluation of Deepfake Regulation Through the AI Act in the European Union*, 4 EUROPEAN CRIM. L. REV. 184 (2024).

29. EUROPEAN COMM'N, *Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes* (Apr. 2024), https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes [https://web.archive.org/web/20260220131404/https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes].

30. Block, *supra* note 28.

31. *User Empowerment through Media and Information Literacy Responses to the Evolution of Generative Artificial Intelligence (GAI)*, UNESCO (2024), https://unesdoc.unesco.org/ark:/48223/pf0000388547.locale=en.

risks. However, for these reports to be fully effective, the regulator must develop a common methodology for producing them in a way that is fully useful. In addition, access to data should be ensured not only to regulators but also to academics and non-profit organizations in order to evaluate how responsibly these online service providers have been in implementing their transparency obligations.

Furthermore, this regulatory approach based on transparency must extend beyond the AI Act, as the production and dissemination of deepfakes require the development of a systemic regulatory framework in light of massive sharing on online services, especially on social media. In this perspective, beyond the AI Act, it is essential to take into account the new requirements imposed by the Digital Services Act ("DSA") on online platforms that aim at ensuring the safety of the digital space, in particular to limit the impact of deepfakes' virality and algorithmic amplification. To that end, first of all, very large online platforms have to undertake risk analysis and take mitigation measures to limit the systemic risks produced by the use of their services such as threats to privacy, dignity, media pluralism, and health.[32] Such obligations have been set out in the specific context of elections to consider the risks of massive amount of deepfakes for the integrity of election results and democratic debate.[33] The Guidelines of article 28 of the DSA,[34] imposing specific obligations to online platforms accessible to underage end-users, also cover deepfakes.[35] This is especially essential considering that "children are particularly vulnerable to synthetic content, such as deepfakes, which can make them more exposed to harmful online practices like grooming and cyberbullying, as well as child sexual abuse material (CSAM)."[36]

In considering deepfake-related legislation, it is particularly important to monitor the effectiveness of mitigation measures online service providers take to address these risks, for example, for individuals or for democratic debate. In an effort to achieve these goals, the DSA also imposes external and independent audits. Such audits are essential notably to assess the effectiveness of the guardrails implemented by the AI provider, for example, to avoid specific kinds of deepfakes.[37] This is one of the major components of the regulation through transparency by evolving various stakeholders. This appears

32. For example, they must label deepfakes and ensure that this label stays with the content even if the content is shared with other users. *See* Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (hereinafter "Digital Services Act"), arts. 34–35, O.J. (L 277).

33. EUROPEAN COMM'N, *Guidelines for Providers*, *supra* note 29.

34. Digital Services Act, *supra* note 32, art. 28.

35. EUROPEAN COMM'N, *Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online* (July 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519 [https://perma.cc/9SVZ-99C7].

36. EUROPEAN PARLIAMENT, *Children and Deepfakes* (July 2025), https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775855 [https://web.archive.org/web/20251211125034/https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775855].

37. *See, e.g.*, CTR. FOR COUNTERING DIGITAL HATE, *Fake Image Factories* (2024), https://counterhate.com/research/fake-image-factories/ [https://web.archive.org/web/20251229085406/https://counterhate.com/research/fake-image-factories/].

to be a decisive step toward protecting the public interest by preventing manipulation and disinformation.