



Video Games & Multi-media | EU response | All Europe Countries | International | USA | Artificial Intelligence

The Commission Opens Official Probe Into X Over AI Chatbot's Role in Deepfake Content

The European Commission opened a new formal investigation into social media platform X, formerly Twitter, over concerns that the company failed to prevent its AI chatbot from generating illegal explicit content.

The European Commission opened new formal proceedings into social media platform X (formerly Twitter) on Monday, citing concerns that the company may not have adequately assessed and mitigated risks linked to its AI features — including the potential generation and spread of illegal sexually explicit content.

The investigation, announced on January 26, 2026, will examine whether X properly assessed risks before deploying Grok, the AI chatbot developed by xAI, including Grok-related image-generation and editing functionalities, and whether X's design and operation of its recommender systems contributed to the dissemination of harmful or illegal material, in a way that could breach the EU's Digital Services Act (DSA).

The new probe runs alongside — and partly extends — an [ongoing Commission investigation launched in December 2023](#), which scrutinises X's approach to systemic risk management, content recommendation, and the handling of illegal content under the DSA framework for very large online platforms.

Commission officials are now focusing on whether X carried out and submitted adequate risk assessment documentation for Grok functionalities that materially affect the platform's risk profile and whether it implemented effective safeguards to prevent and mitigate the spread of illegal content. Key concerns include non-consensual sexually explicit deepfakes — including so-called “nudification” or digital undressing of images of real

people — as well as content that may amount to child sexual abuse material (CSAM).

The controversy intensified after reports and watchdog research suggested that Grok was used to generate large volumes of sexualised imagery over a short period, including documented cases involving non-consensual edits targeting women, public figures and, in some instances, minors — prompting widespread criticism and renewed scrutiny of platform safeguards.

The [new investigation will assess](#) X's compliance with DSA obligations for very large online platforms, including requirements to identify and mitigate systemic risks, introduce proportionate and effective safeguards for new product features, and provide the Commission with an ad hoc risk assessment report ahead of deploying Grok functionalities that critically affect X's risk profile.

Earlier in January 2026, ahead of the formal opening of proceedings, the Commission ordered X to preserve Grok-related documentation until the end of 2026, in a step designed to secure evidence relevant to the inquiry. X has said it tightened restrictions around certain Grok image-editing or generation capabilities following public criticism, and that it has taken steps to reduce the circulation of violative content. The Commission's investigation will test whether such measures were adequate and timely under the DSA's risk-mitigation requirements.

"Sexual deepfakes of women and children are a violent, unacceptable form of degradation. With this investigation, we will determine whether X has met its legal obligations under the DSA, or whether it treated rights of European citizens - including those of women and children - as collateral damage of its service", said Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy in a written statement.

The probe may involve formal requests for information, interviews and on-site inspections. If infringements are ultimately established, the Commission can impose interim measures, order corrective actions, and levy fines of up to 6% of global annual turnover. On 5 December 2025, the Commission had [issued another fine of €120 million to X for breaching its transparency obligations](#) under the Digital Services Act (DSA). The breaches, then included the deceptive design of its 'blue checkmark', the lack of transparency of its advertising repository, and the failure to provide access to public data for researchers.

