

AI, Child Online Safety, and the Digital Governance Challenge

www.360geopolitica.org

Artificial intelligence is transforming online child protection. While AI offers new tools for detection and investigation, it is also making child sexual exploitation more sophisticated, scalable, and difficult to police. Governments, technology companies, and law enforcement agencies now face a dual challenge: counter AI-enabled abuse while ensuring that regulatory responses do not undermine privacy, cybersecurity, and fundamental rights.

German authorities illustrate the scale of this shift. The Federal Criminal Police Office (BKA) recorded more than 20,000 child sexual abuse victims in 2025, with online offenses continuing to rise. Investigators report significant growth in cyber grooming, non-contact sexual abuse, and the livestreaming of abuse conducted across borders. Digital technologies increasingly enable offenders to target children remotely, complicating investigations and reinforcing the transnational nature of these crimes.

AI is accelerating these trends by lowering technical barriers for offenders. Generative AI can create convincing fake identities that predators use to establish trust through personalized conversations, while image-generation tools can manipulate innocuous photographs into child sexual abuse material or regenerate existing illegal content, making detection and attribution more difficult. Consequently, law enforcement must address both the expanding volume of illegal material and the challenge of distinguishing authentic evidence from AI-generated content.

Governments are responding with stronger digital regulation. Australia has restricted social media access for children under 16, while the European Union is developing a common age-verification framework for online services. These initiatives seek to reduce children's exposure to harmful content and strengthen enforcement of age restrictions across digital platforms.

Yet age verification remains highly contested. Privacy advocates and cybersecurity experts warn that centralized systems requiring identity documents, biometric information, or facial recognition could create attractive targets for cybercriminals and expand surveillance capabilities. Others argue that assigning identity verification to large technology companies would further concentrate digital power while enabling greater data collection. There are also concerns that identity infrastructure introduced for child protection could later be repurposed for broader forms of digital control.

Beyond privacy, many child protection specialists argue that age verification addresses symptoms rather than underlying causes. Organizations such as UNICEF emphasize that many online risks stem from platform design itself. Recommendation algorithms that amplify sensational content, engagement-driven features such as infinite scrolling, and advertising models that prioritize user attention can expose children to harmful material regardless of age restrictions. Without addressing these structural incentives, access controls alone are unlikely to provide a comprehensive solution and may even push minors toward less regulated online environments.

These debates reflect a broader digital governance challenge. Policymakers must simultaneously protect children, strengthen law enforcement, preserve privacy and anonymity, and prevent excessive concentration of power within a small number of technology companies. Effective governance therefore requires more than identity controls. It also demands platform accountability, privacy-preserving technologies, international cooperation, and regulatory frameworks capable of addressing both AI-enabled criminal activity and the commercial incentives that shape digital ecosystems.

Colombia's Digital Governance Gap and the Online Recruitment of Children illustrates how digital governance has become a national security issue. While illegal armed groups historically relied on territorial control to recruit

children, recruitment increasingly begins online. Social media platforms provide opportunities to identify vulnerable minors, establish contact, manipulate them through grooming techniques, disseminate propaganda, and facilitate recruitment long before any physical encounter occurs.

Colombia's regulatory framework has not kept pace with this evolution. Existing legislation addresses internet access, cybersecurity, and data protection but imposes few obligations on digital platforms to prevent criminal exploitation of minors and lacks effective mechanisms governing children's access to social media. The result is a significant protection gap that allows criminal organizations to exploit platform algorithms, private messaging services, and online communities with limited oversight.

These vulnerabilities are reinforced by weak state presence in conflict-affected regions, persistent poverty, and the territorial expansion of illegal armed groups and organized criminal networks. Since 2022, these actors have consolidated forms of local governance in several regions while increasingly exploiting digital platforms to expand recruitment. The Colombian government's reluctance to adopt stronger digital governance measures is also shaped by political considerations.

During the *Total Peace deal*, the Petro's administration has sought negotiated arrangements with illegal armed groups and criminal organizations, reducing incentives to pursue more robust regulatory or enforcement measures that could disrupt those compromises. Analysts argue that these groups also retain significant influence over national and local political dynamics as demonstrated during the 2026 legislative and presidential elections where they implemented the vote-

pistole to favor the Petro-Iván Cepeda's government political movement.

International experience demonstrates that governments are increasingly treating children's online safety as a matter of public policy rather than solely parental responsibility or political deals. Australia has adopted mandatory age restrictions for social media, while Spain has combined stronger regulation with digital literacy initiatives. Although these approaches differ, both recognize that digital platforms have become critical components of child protection policy.

For Colombia, however, the challenge extends beyond online safety. Social media platforms have become part of the country's broader security environment. International organizations have documented their use by armed groups to recruit children, spread propaganda, normalize violence, and facilitate criminal activity. As recruitment increasingly shifts into digital spaces, the absence of effective platform regulation directly affects both child protection and national security.

The central policy question is therefore whether Colombia will continue relying on fragmented regulation or adopt a comprehensive digital child protection strategy that combines platform accountability, risk monitoring, targeted age safeguards, and preventive interventions.

In an era where recruitment increasingly begins online, digital governance is no longer simply a technology issue—it is a matter of child protection, public security, and state capacity and responsibility.

360° geopolitica.