# Effective Protection, Not Mere Compliance: The ANPD's New Approach to Child Safety Online

24.09.2026 4 min read

**Authors**

**Felipe Palhares**

**Fernanda Villela**

**Related areas**

Data Privacy and Cybersecurity

**Topics**

Data Privacy and Cybersecurity ANPD Digital Statute of the Child and Adolescent BMA Review

On 17 August 2026, Brazil's National Data Protection Authority (*ANPD – Agência Nacional de Proteção de Dados*) ordered a gaming platform to suspend its livestreaming feature for users in Brazil. The decision was one of the most significant enforcement actions taken under the new Digital Statute for Children and Adolescents (*ECA Digital – Estatuto da Criança e do Adolescente*).

When it came into force in March 2026, the ECA Digital established a new framework for protecting children and adolescents in the digital environment. The statute applies not only to products and services directed at minors but also to those likely to be accessed by them, and places responsibility for enforcement with the ANPD.

Whether the ANPD's decision was proportionate remains open to debate. The suspension was ordered in the context of an investigation launched after the Agency became aware of allegations that users had been encouraged to engage in self-harm or suicide through activities on the platform.

In its preliminary assessment, the ANPD found evidence suggesting that certain livestreaming features could pose significant risks to children and adolescents. In the Agency's view, the safeguards in place were not sufficient to prevent or mitigate those risks.
Based on that assessment, the ANPD's Inspection Department (*SFI – Superintendência de Fiscalização*) ordered the temporary suspension of the platform's livestreaming feature and similar video-sharing features for users in Brazil. The suspension will remain in place until the company can demonstrate that it has implemented technical safeguards, security measures, and governance processes that the Agency considers appropriate to address the identified risks.

The most significant aspect of the decision is not the suspension itself, but the legal interpretation underlying it. The ANPD addresses concerns about proportionality by making the measure conditional on the implementation of appropriate technical safeguards, security measures, and governance processes, and by emphasizing that the suspension is reversible.

The case offers an important glimpse into the ANPD's expectations regarding effective compliance with the ECA Digital. In its analysis, the Agency expressly states that a platform may violate the ECA Digital not simply because its service presents risks, but because the safeguards it has implemented may be insufficient to prevent, detect, and mitigate risks associated with the design and operation of the service.[1]

The standard adopted by the ANPD under the ECA Digital seems to be different from that found in many other regulatory regimes, where demonstrating accountability is often enough. Under the Agency's approach, compliance is inherently contextual and depends on the nature of the product or service and the specific risks it creates for children and adolescents. Encryption illustrates the point. A safeguard that may be highly effective in one context can become less protective in another if it operates as a barrier to measures needed to address identified risks. In such circumstances, the burden shifts to the platform operator to implement safeguards that can be shown to provide an equivalent or higher level of protection.

The implication is that companies cannot treat compliance with the ECA Digital as a standardized box-ticking exercise. The ANPD's approach goes beyond formal legal compliance to encompass the entire lifecycle of digital products and services, from design and development through deployment and operation. For companies subject to the ECA Digital, compliance is no longer a purely legal function. As the Agency itself explains, it is a "*preventive, continuous, and risk-based duty, the sufficiency of which must be assessed according to the functionalities offered and the severity of foreseeable harms*."[2]

For technology companies, the ANPD's decision signals a need to rethink compliance when products or services are directed at children and adolescents or are likely to be accessed by them. Demonstrating formal compliance or maintaining generic child-protection policies will no longer be enough. The focus is increasingly on whether safeguards are effective in practice and whether they adequately protect the best interests of minors.

The ANPD now expects companies to conduct structured risk assessments, document the decisions underlying the design and operation of specific products and services, and implement safeguards proportionate to the risks identified. Those safeguards must also function as part of an integrated system capable of detecting, containing, and mitigating situations that may affect children and adolescents.

Companies subject to the ECA Digital that understand this new level of expectation and invest early in robust governance structures will be better positioned to face scrutiny from both regulators and the public. Although the challenge is complex, organizations that successfully meet this new standard will benefit not only from reduced regulatory risk, but also from the trust and credibility that come with demonstrating a genuine commitment to protecting children and adolescents online.

**>> Keep scrolling for the next articles in BMA Review #92, or read the full edition as a PDF.**

**NOTES**

1. Nota Técnica n° 1/2026/CGF/SFI/ANPD
2. Nota Técnica n° 1/2026/CGF/SFI/ANPD. Our translation.

› PROFESSIONALS

## Professionals who combine legal insight and market perspective

**Felipe Palhares**

**Fernanda Villela**