REGULATION OF THE DIGITAL ECA

DECREE NO. 12,880/2026 AND GUIDANCE FROM THE BRAZILIAN DATA PROTECTION AGENCY (ANPD)

BERARDO LILLA
BECKER SEGALA E DANIEL

INTRODUCTION

On March 18, 2026, Decree No. 12,880/2026 (“Decree”) was published, regulating Law No. 15,211/2025 (known as the “Digital ECA”), aimed at protecting children and adolescents in the digital environment, which entered into force on March 17.

The Decree operationalizes obligations set forth in the Digital ECA and introduces additional requirements for providers of information technology products or services directed at, or likely to be accessed by, children and adolescents.

On March 20, 2026, the Brazilian Data Protection Agency (ANPD) also published:

i. a regulatory and enforcement implementation roadmap for age assurance solutions and

ii. preliminary guidance on reliable age assurance mechanisms, anticipating key interpretative parameters for the application of the new framework.

In this material, we highlight the main points for your business’s alignment with the new framework.

1. CENTRAL ROLE OF THE ANPD

The Decree reinforces the central role of the ANPD, which will be responsible for detailing a significant portion of the rules through future regulation, as well as supervising compliance with the Digital ECA and enforcing sanctions.

The publications issued on March 20 signal an immediate regulatory response, with the early release of interpretative parameters on age assurance mechanisms and the definition of a structured implementation roadmap.

Further guidance and interpretative documents are also expected, particularly regarding the scope of application of the Digital ECA and the concept of “likely access.”

2. NATIONAL POLICY FOR THE PROTECTION OF CHILDREN AND ADOLESCENTS IN THE DIGITAL ENVIRONMENT

The Decree formally establishes a National Policy aimed at promoting and protecting the rights of children and adolescents in the digital environment. To this end, an Intersectoral Committee will be created, ensuring coordinated action among different ministries and the participation of civil society.

3. PREVENTION OF EXCESSIVE, PROBLEMATIC OR COMPULSIVE USE

The Decree defines mechanisms that may encourage excessive, problematic or compulsive use of digital services by children and adolescents, including the concealment of natural stopping points (such as infinite scrolling), automatic content triggering, time-based rewards, and excessive notifications.

It also introduces a threefold typology of prohibited manipulative practices, transforming what was previously an open-ended clause into legally actionable categories:

- **Obstruction:** conduct that makes it difficult or prevents users from interrupting use, canceling services, or modifying preferences through excessively complex or disproportionate pathways;
- **Exploitation of cognitive vulnerabilities:** use of emotional pressure, artificial urgency, biased choices, or age-inappropriate stimuli to induce decisions contrary to the child's best interests;
- **Harm to the exercise of rights:** practices that conceal, fragment, or hinder access to privacy controls, parental supervision tools, or consent and revocation mechanisms.

4. SPECIFIC OBLIGATIONS FOR AI PROVIDERS

The Decree establishes specific obligations for AI service providers capable of generating content and interacting with users through natural language, such as conversational agents and large language models.

These services must:

- clearly disclose that interactions are automated;
- implement measures to prevent behavioral manipulation;
- assess algorithmic risks to the safety and well-being of children and adolescents; and
- adopt safeguards to protect their physical, mental, and psychosocial development.

5. IMPROPER, INAPPROPRIATE, AND PROHIBITED CONTENT AND SERVICES

The Decree distinguishes between different categories of content, each with specific legal consequences:

- **Improper or inappropriate content:** content that poses risks to psychosocial development or mental health. Access is not prohibited but is conditioned on content rating compliance, default safety measures, and effective parental control tools;
- **Prohibited content:** content whose provision to minors is expressly forbidden by law. Access must be effectively prevented through robust age verification.

  For more sensitive categories—such as pornography, online betting, and lotteries—stricter requirements apply, including the prohibition of account creation by minors and the obligation to identify and remove such accounts.

  The ANPD is also expected to regulate minimum requirements for preventing children and adolescents' exposure to advertising related to prohibited products.

Pornographic content

The Decree adopts a functional definition of pornographic content, considering not only the content itself but also the platform's purpose and business model. It includes explicit sexual content, as well as previews, thumbnails, titles, descriptions, and AI interactions involving sexual content.

The ANPD is expressly empowered to reclassify a provider's self-declared categorization based on the predominant nature or practical effects of the service.

Social media

Platforms that host prohibited content may either:

(i) offer a version without such content, thereby dispensing with age verification; or

(ii) implement effective age verification mechanisms, with self-declaration expressly prohibited.

Loot boxes

Games offering loot boxes must implement age verification or alternatively disable the feature or provide a version without it.

6. OPERATIONALIZATION OF AGE ASSURANCE

The Decree establishes a risk-based and shared-responsibility ecosystem for age assurance. The required level of assurance must be proportional to the risk associated with the content or service, allowing for different technical solutions depending on the context. Implementation will be gradual and subject to further regulation by the ANPD.

The preliminary guidance issued by the ANPD on March 20 provides additional detail on how these mechanisms should be implemented at this initial stage, before the adoption of definitive regulation, reinforcing a risk-based approach and outlining relevant technical parameters.

The Decree introduces the following key concepts:

- **Age assurance:** a broad concept encompassing methods used to verify, estimate, or infer a user's age or age range;
- **Age verification:** a high-reliability form of age assurance based on confirming the accuracy of the declared age, required for prohibited content such as pornography, betting, and loot boxes;
- **Self-declaration:** a simple statement of age by the user, without additional evidence, expressly prohibited for access to prohibited content;
- **Age signal:** a credential or information provided by app stores or operating systems indicating a user's age range without disclosing additional personal data. Even when provided by third parties, the service provider remains responsible, and the most protective outcome must prevail in case of discrepancies.

Consistent with the Decree, the ANPD guidance emphasizes that the choice of mechanism should not be based solely on accuracy, but also on its impact on privacy and data protection. There is a clear preference for solutions that minimize the collection and circulation of personal data, as well as caution regarding more intrusive mechanisms, such as biometric-based solutions.

The guidance also highlights the need for prior risk assessments—both in relation to the service and to the mechanism itself—and confirms that self-declaration alone is not a reliable method.

From a data protection perspective, the implementation of these mechanisms must comply with principles such as data minimization, security, transparency, prohibition of secondary use, and restrictions on tracking users' identity or browsing history, as well as limitations on continuous and unrestricted data sharing. Where identification documents are used, their images must be immediately and irreversibly deleted after extracting the necessary information.

Finally, the Decree authorizes the development of public age assurance solutions integrated with Brazil's digital identity infrastructure (gov.br), which may influence private solutions and foster interoperable models.

7. ADVERTISING AND MONETIZATION

Advertising

Providers must prevent the use of:

profiling techniques;

emotional analysis;

immersive technologies (such as AR/VR) for advertising directed at minors.

Monetization

Content that monetizes or promotes the routine or image of children on a recurring basis requires prior judicial authorization. In the absence of such authorization, the content must be removed.

Content that exposes children and adolescents to degrading or harmful situations may not be monetized or promoted under any circumstances.

8. PREVENTION AND RESPONSE TO SERIOUS VIOLATIONS

The Decree authorizes the creation of a National Notification Screening Center (CNTN) within the Federal Police to centralize the handling of reports of digital crimes against children and adolescents.

9. IMMEDIATE AND PRIORITIZED CONTENT REMOVAL

The Digital ECA establishes priority treatment and immediate removal of content when reported by qualified entities, such as the victim, public authorities, or accredited civil society organizations.

10. TRANSPARENCY AND ACCOUNTABILITY

The Decree adopts a preventive and accountability-driven approach by requiring providers to conduct impact assessments on risks to children's safety and well-being, including risk identification, mitigation measures, and continuous monitoring.

It also requires the disclosure of a summarized version of such assessments in clear and accessible language and allows the ANPD to further regulate their content, frequency, and conditions.

In light of this new regulatory landscape, companies offering digital products and services in Brazil should begin—or accelerate—their compliance efforts.

Our Technology and Digital Business practice is ready to support your organization at every stage of this process.

PAULO LILLA

paulo.lilla@berardo.adv.br

+55 11 99652.3354

CARLA SEGALA

carlasegala@berardo.adv.br

+55 11 99257.1754

ANE CARVALHO

ane.carvalho@berardo.adv.br

+55 11 99613.7624

BERARDO LILLA
BECKER SEGALA E DANIEL