ISSUE BRIEF

GLOBAL

# Brazil's Digital ECA:
## New Paradigm of Safety & Privacy for Minors Online

Author: Maria Badillo, Future of Privacy Forum
December 2025

FUTURE OF PRIVACY FORUM

# Executive Summary

This Issue Brief analyzes Brazil's recently enacted children's online safety law, summarizing its key provisions and how they interact with existing principles and obligations under the country's general data protection law (LGPD). It provides insight into an emerging paradigm of protection for minors in online environments through an innovative and strengthened institutional framework, focusing on how it will align with and reinforce data protection and privacy safeguards for minors in Brazil and beyond.

This Issue Brief summarizes the Digital ECA's most relevant provisions, including:

- **Broad extraterritorial scope:** the law applies to **all information technology products and services aimed at or likely to be accessed by minors**, with extraterritorial application.
- **"Likelihood of access"** of a technology service or product as a **novel standard,** composed of three elements: **attractiveness, ease of use, and potential risks to minors.**
- Provisions governed by the principle of the "**best interest of the child,"** requiring providers to **prioritize the rights, interests, and safety of minors from the design and throughout their operations.**
- **Online safety by design and by default,** mandating providers to adopt **protective measures by design and monitor them throughout the operation** of the service or product, including **age verification mechanisms** and **parental supervision tools.**
- **Age rating as novelty,** requiring providers to maintain age rating policies and continuously assess their content based on such rating.
- Enforcement of the law is assigned to the **ANPD**, which was transformed into a **regulatory agency with increased and strengthened powers to monitor its compliance**, in addition to its responsibilities under the data protection law.
- Significant sanctions under the Digital ECA, which can range from **warnings and fines up to 10% of a company's revenue to the permanent suspension of activities** in Brazil.

*The author thanks Dr. Desara Dushi and Daniel Hales for their insights and contributions.*

# Table of Contents

## 1. Introduction

On September 17, 2025, Law 15.211 on the protection of children and adolescents in digital environments, known as the "Digital ECA" after its name in Portuguese (*Estatuto Digital da Criança e do Adolescente* – "digital statute of children and adolescents"), was enacted and published in Brazil's Official Gazette. The legislation sets a comprehensive framework for the protection of children online and will become effective six (6) months after its publication. The Digital ECA introduces several safety obligations that expand from the principles and obligations already established under Brazil's Personal Data Protection Law (Law 13.709 – "LGPD"), such as privacy-by-design and special safeguards when processing children's data. This alignment, coupled with the fact that the new legislation will be enforced by Brazil's Data Protection Authority ("ANPD"), marks a significant interplay between both frameworks in advancing the safety and privacy of minors online.

The Issue Brief covers (1) the Digital ECA's broad scope of application, (2) the principle of best interest of the child as its guiding principle for online protection and its meaning under Brazilian law, (3) the core obligations addressed as "preventive measures" under the law and its relationship with data protection principles and obligations, and (4) governance and potential sanctions. Read further for a deeper analysis of the Digital ECA's provisions and what it means for children's online protection in Brazil.

## 2. Scope of Application: All Products and Services *Likely to be Accessed by Minors*

The Digital ECA will apply to all information technology products and services aimed at or likely to be accessed by children and adolescents, regardless of location, development, manufacture, supply, marketing, and operation. The law's definition of an "information technology product or service" (hereinafter referred to as "ITPS") covers **any product or service provided remotely, by request, and connected to the Internet**, including internet apps, computer programs, software, operating systems, and electronic games (Article 1, sec. I). This suggests the law will have a broad extraterritorial scope, becoming applicable to any ITPS regardless of where they are being operated, as long as they can be accessed online by minors located in Brazil.

Moreover, the law will apply to any information technology product or service **aimed at children (anyone under the age of 12) and adolescents (anyone between 12 and 18 years of age)[1] or likely to be accessed by such groups**, even if not explicitly designed for them. Importantly, although Brazilian

[1] As defined by Brazil's Child and Adolescent Statute (*Estatuto da Criança e do Adolescente*).

law distinguishes between these two age groups, the obligations introduced under the Digital ECA seem to be generally applicable, independent of the age group, as long as the services are aimed at or likely to be accessed by minors (understood as anyone under the age of 18).

Accordingly, the **"likelihood of access"** is a novel criterion introduced by the Digital ECA that provides it with a broad scope of application for any provider of an ITPS. The criterion is determined by three elements, including:

> (i) whether the ITPS is **attractive** to minors,
>
> (ii) whether it is easy to **use and accessible**, and
>
> (iii) whether it poses a **significant degree of risk to the privacy, security, or biopsychosocial development** of minors (Article 1).

The wording of the Digital ECA suggests these three conditions must be met cumulatively to consider that an ITPS is "likely to be accessed by minors," and thus under the scope of the legislation. Further regulation and guidance might clarify the meaning of "attractiveness, ease of use and accessibility" under the law, as well as how providers must conduct the three-pronged risk assessment.

For the privacy component of the assessment, it is likely that providers will be required to comply in similar terms under the LGPD—meaning they must disclose the types of personal data to be processed, the potential risks that the processing poses to fundamental rights, and the measures taken to mitigate those risks. In addition, guidance could further clarify the nexus between the degree of risk and the "likelihood of access" criterion, since the legal text suggests that if an ITPS does not pose a significant degree of risk to the privacy, security, and development of minors, then it is not likely to be accessed by minors.

## 3. "Best Interest of the Child:" A Foundational Principle for Online Safety

The obligations provided by the Digital ECA are guided by the underlying principle of acting in the "best interest of the child." This principle is expressly recognized both in Brazil's Federal Constitution, providing that it is the duty of the family, the State, and society to **ensure protection of children and adolescents with "absolute priority,"** and in the Statute of the Child and Adolescent (Law 8.069), indicating children enjoy all fundamental rights and opportunities to enable their overall development and prohibiting any form of negligence, oppression or violence (Articles 3-5). The principle was adopted in national law after Brazil ratified the United Nations Convention on the Rights of the Child in 1990, which is a foundational principle enshrined in the Convention, and is also recognized as a guiding

principle for measures and efforts taken by State parties to implement the instrument, including in digital environments.[2]

Accordingly, the Digital ECA requires organizations to **prioritize the "full and special" protection of children when operating information technology products and services that are likely to be accessed by them**, even if these services are not specifically aimed at minors. In this sense, providers covered by the new legislation must ensure that the use of their products or services is based on the following protections (Article 4):

- The guarantee of minors' full protection;
- The absolute prevalence of their interests;
- The unique condition of a person's biopsychosocial development;
- Safety against intimidation, exploitation, abuse, threats, and other forms of violence;
- Respect for the autonomy and progressive development of the individual;
- Protection against commercial exploitation;
- Compliance with principles to protect people with disabilities;
- Promotion of digital education; and
- Transparency and accountability in the processing of personal data of minors.

Although it remains unclear how these protections will be operationalized in practice, the Digital ECA appears to impose a broad, overarching obligation on all ITPS providers, suggesting that even if a product or service is not specifically designed or aimed at children, providers should assume they may be accessed by them. Consequently, online services must be designed and operated in consideration of minors' developmental needs, autonomy, and rights, ensuring accountability and guaranteeing their full protection.

## 4. "Online Safety" Through A Preventive Approach

The Digital ECA assumes a preventive approach, requiring all suppliers of ITPS to establish **"reasonable" measures, from the design stage and throughout their operations, to prevent and mitigate the risk of access, exposure, recommendation, or facilitation of contact with any of the**

[2] As stated in General comment No. 25 (2021) on children's rights in relation to the digital environment of the United Nations' Convention on the Rights of the Child.

**following content:** material depicting sexual exploitation and abuse; physical violence; virtual intimidation; harassment; practices or guidance for self-harm and suicide; gambling; fixed-odds betting; lotteries; tobacco, alcohol, or other products prohibited for sale to minors; predatory, unfair, or deceptive advertising, or any other form of advertising that might cause financial harm; and pornography (Article 6).

This preventive approach is essentially built on the following obligations: safety and privacy by default, establishing age-rating policies, employing age verification mechanisms and parental supervision tools, and transparency and reporting obligations. Compliance with these obligations must be observed in consideration of the best interest of the child, and the respect for their autonomy and progressive development as guiding principles.

### 4.1. Privacy and Protection by *Default* (Including Explicit Prohibitions)

The Digital ECA has a significant data protection component that expands on the protections provided by the LGPD to protect minors online. As a general rule, the law requires providers to **refrain from any processing that could facilitate or contribute to the violation of children's privacy or other fundamental rights** (Article 7, § 2º). Similar to the Digital ECA, the LGPD sets out a special protection for children's data, requiring all processing of personal data to be performed in the child's best interest and with specific and distinguishable consent from one of the parents or legal guardian (LGPD Article 14).

The Digital ECA complements this protection by establishing explicit **prohibitions on using data collected for age verification for any other purpose** (Article 13) and **profiling for targeted advertising, emotional analysis, and for augmented, extended, and virtual reality interfaces** (Articles 22 and 26). The profiling prohibition for children under the online safety legislation is significant, considering the LGPD does not expressly prohibit this practice, although it recognizes the right to review decisions based on profiling.

Furthermore, the Digital ECA requires providers of ITPS to operate on the **"highest level of protection possible"** and provide children and guardians with clear, accessible, and adequate information about choosing less protective settings (Article 7, § 1º). This obligation supports requirements under the LGPD, particularly, the principle of **privacy by design and by default.** This principle, implicitly recognized in the data protection legislation as a security and good governance measure, instructs processing agents to adopt technical and administrative measures to protect personal data from unauthorized access or unlawful processing from the design phase of a service or product (LGPD Article 46, § 2). Notably, under the Digital ECA, implementing protective settings by default becomes a core obligation aimed at improving online safety and preventing any processing that may violate children's privacy.

Suppliers are also required to establish **default settings to prevent "compulsive use"** of ITPS by minors (Article 8, sec IV). While the Digital ECA does not define "compulsive use," this might be constructed on further guidance based on similar elements of the likelihood of access criterion, considering elements like the ease of use and attractiveness, and potential addictiveness of a product or service. Compulsive use seems to be a recurrent concern throughout the legislation: for instance, the statute prohibits reward (loot) boxes[3] in video games (Article 20) and requires parental supervision tools to be configured in a way that can disable similar functions, such as rewards based on usage time and automatic media playback (Article 17, § 4, II).

## 4.2. Content Assessment Must Be Based on Age Rating Policies

Under the legislation, suppliers of ITPS are required to offer 'age-appropriate' content in consideration of both children's "progressive autonomy" and the diversity of Brazilian "socio-economic contexts." In this sense, the Digital ECA requires providers to **maintain an age rating policy and assess their content based on that rating** (Article 8, sec II). Suppliers must "extensively inform" users about the age rating policy *at the time of access* to the product or service (Article 8, sec V). Notably, the law does not explicitly mention how such policies should be constructed and enforced, although this might be subject to further guidance from the competent authority.

The Digital ECA also introduces an **obligation to conduct risk and impact evaluations of minors' access to harmful content**. For instance, the law requires suppliers to carry out risk assessments of the potential impact of their content on the safety and health of minors, and to establish systems and processes to prevent access to illegal, pornographic, or "clearly" inappropriate content for minors (Article 8, sec I and III). In addition, it requires controllers to map out risks and mitigation efforts, and to prepare **data protection impact assessments** whenever the **processing of minors' data is carried out for purposes other than those strictly necessary for the operation of the product or service** (Article 16).

## 4.3. Age Verification Mechanisms

Under the Digital ECA, providers of products or services with content inappropriate for minors must adopt effective measures to prevent their access through age verification mechanisms. Notably, the law **prohibits age verification through self-declaration** and mandates providers of internet application

[3] Reward boxes are defined as a "functionality available in certain electronic games that allows the player to acquire, upon payment, consumable virtual items or random advantages, redeemable by the player or user, without prior knowledge of their content or guarantee of their effective usefulness" (Article 2, sec. IV).

stores and terminal operating systems to put **proportionate, auditable, LGPD-compliant, and technically secure age verification mechanisms** in place. For this purpose, providers must enable age signals to internet application providers through secure Application Programming Interfaces (API), which must be shared exclusively for compliance purposes and for implementing technical safeguards. The law expands the protection provided under the LGPD, requiring age signals to be shared in accordance with the principle of **data minimization** and **prohibiting any continuous, automated, and unrestricted sharing of minors' data** (Article 12, sec II, § 1).

Importantly, providers of **ITPS are responsible for implementing their own mechanisms to prevent access to inappropriate content** for minors through their platforms regardless of measures adopted by internet application stores and operating systems (Article 14). Age verification obligations similarly do not exempt other agents in the digital ecosystem from their responsibilities, and all agents are jointly liable for ensuring comprehensive protection for minors online (Article 15).

For social media platforms, the Digital ECA requires providers to **link the accounts of minors below the age of sixteen (16) to the account of a legal guardian**, and to continuously improve their verification tools to identify accounts operated by children, as well as to implement additional age verification methods, allowing further processing of personal data for this purpose (Article 24, sec III, § 3.).

### 4.4. Parental Supervision Tools

The Digital ECA introduces obligations for suppliers of ITPS to facilitate and enable parental supervision tools. Based on the preventive approach enshrined throughout the legislation, it **requires providers to embed parental supervision tools by default**. Default settings must consider the highest level of protection possible, allowing parents or guardians, as a minimum, to restrict communications with unauthorized users, limit features that increase or sustain the use of the product or service (i.e., restricting automatic media playback, rewards on app, and notifications), regularly reviewing artificial intelligence (AI) tools and disabling non-essential functions, among other features (for an exhaustive list of controls, refer to Articles 17 and 18). At the same time, the Digital ECA requires suppliers to **inform minors when parental supervision tools are in place** through a clear and visible notice.

For age verification and parental supervision tools, the legislation leaves room for the authority to issue guidance and regulations on both mechanisms to indicate minimum transparency, security, and interoperability requirements. Relatedly, the legislation also authorizes the government to act as regulator, certifier, or promoter of age verification and parental supervision tools (Articles 11 and 12, § 3).

### 4.5. Transparency Obligations, Reporting Mechanisms, & Content Removal

A relevant component of the children's online safety law are transparency obligations triggered under certain circumstances. For instance, as noted above, the Digital ECA requires ITPS to provide both minors and guardians with **clear and accessible information about choosing less protective settings than those provided by default, and to disclose to minors in an understandable format whenever parental tools are in place.**

Interestingly, the law also requires providers of ITPS to make information available to parents and guardians about the **risks from access or exposure to their services by minors,** as well as the security measures taken to protect them, **regardless of whether their product is purchased** or not (Article 16). Considering the extraterritorial effect of the law, and the fact that this obligation is applicable regardless of purchase, it appears that any provider of an ITPS aimed at or likely to be accessed by minors is required to make this information publicly available on their website. In practice, this could mean conducting risk assessments and making them public, along with the measures taken to mitigate those risks. However, further guidance on how to perform such assessments and how to report them in a clear and understandable manner for all audiences will be necessary for effective compliance.

Since the Digital ECA is fundamentally aimed at preventing and limiting minors' access to harmful content, including through content removal obligations, it also incorporates safeguards to avoid turning these measures into broader forms of online censorship. In this sense, it requires suppliers to implement **mechanisms to prevent the abuse of content reporting tools and inform users about the consequences of abusing the tools and potential sanctions**, which may include temporary suspension and cancellation of accounts. In addition, suppliers must disclose their procedures for identifying cases of abuse and their assessment when imposing sanctions (Articles 32-33).

The law also introduces **reporting obligations for violations of rights and other "serious violations"** according to a set of requirements to be further developed in secondary regulation. The Digital ECA establishes that **providers must report "serious violations," to national and international authorities and remove any content depicting exploitation, sexual abuse, kidnapping, and grooming** detected directly or indirectly in their products or services. For these purposes, providers are required to retain data and metadata related to the reported violation for at least six (6) months—a period that can be extended whenever there is a request from the competent authority, in accordance with Article 15 of Law 12.965 (*Marco Civil da Internet*).

It is unclear how grooming in text-based communication services should be detected, and it remains uncertain whether any form of communication monitoring would be strictly incompatible with children's privacy rights under both the LGPD and the Digital ECA. However, it is worth noting that the potential

means of identifying this harmful practice in ITPS while preserving the privacy of minors appears to be a subject of broader discussion. Comparable online safety legislation seems to rely on privacy by design settings, user reporting tools,[4] while the industry is increasingly exploring techniques such as signal sharing and keywords, and behavioral pattern detection.[5] This approach is more consistent with the preventive approach adopted by the Digital ECA and privacy protections under the LGPD.

Relatedly, providers must **put in place mechanisms to report potential violations of the rights of children and adolescents and, where applicable, notify the competent authorities to initiate an investigation** (Article 28). Importantly, under the principle of "comprehensive protection," the Digital ECA mandates providers of ITPS to immediately remove content reported as violating the rights of children and adolescents when reported by the victim, their representatives, the Public Prosecutor's Office, or entities representing minors' interests, without a court order (Article 29).

Lastly, for platforms with more than one million registered users below the age of eighteen (18), providers must prepare and publish in their website semi-annual reports in Portuguese with information about the channels available for filing complaints, the number of complaints received, the amount and type of content moderated, the number of sanctioned accounts, the measures adopted to identify children accounts on social media, technical improvements for privacy and data protection of minors; technical improvements for assessing parental consent, and details of impact assessments and risk management (Article 31).

## 5. Governance & Sanctions

Enforcement is given to an **"autonomous administrative authority"** responsible for monitoring and overseeing compliance with the law. Significantly, on the same day the Digital ECA was enacted, President Lula da Silva issued Preventive Measure 1.317 and Decree 12.622, granting the **Brazilian Data Protection Authority ("ANPD")** the status of autonomous regulatory agency in charge of the protection of children and adolescents online. Through both Executive acts, the ANPD went through a major change in its former administrative nature as an Executive body, becoming an independent regulatory agency linked to the Ministry of Justice and Public Security and endowed with functional, technical, decision-making, and administrative and financial autonomy.

[4] See for instance the EU's Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, and provisions under UK's Online Safety Act.
[5] See for example the findings from the Tech Coalition's Research Paper on Online Grooming: Considerations for Detection, Response, and Prevention of Online Grooming (2022).

Under its new administrative nature and role, the **ANPD is responsible for issuing regulations to implement the Digital ECA**, which must be performed in consideration of regulatory asymmetries, diverse functionalities, and levels of risk of each product or service, as well as technological developments and applicable technical standards.

While the legislation explicitly mandates further regulation on age assurance and parental supervision tools, it also leaves room for other regulations to be developed by the authority. This is relevant considering the Digital ECA introduces **broad and ambiguous language where additional guidance might be necessary for effective enforcement and compliance**—for instance, on additional elements to assess the "likelihood of use" of certain services and products; factors to adequately comply with the principle of "best interest" of the children; and further guidance to assess other concepts such as protecting the "biopsychosocial development" or the Brazilian "socioeconomic context" for age rating policies.

Accordingly, the ANPD will be in charge of imposing sanctions, which may result in warnings (with a 30-day corrective deadline); **fines up to 10% of the economic group's revenue** in Brazil or up to R$50,000,000.00 (approximately USD$9,120,545) per violation; the **temporary suspension** of activities; or the **prohibition of operations** in national territory. For cases where the temporary or permanent suspension of activities is not implemented by the offender, the ANPD can enforce judicial blocking orders to telecommunication service providers, which must perform in coordination with the National Telecommunications Agency and the Brazilian Internet Steering Committee (CGI.br).

## 6. The LGPD & Digital ECA Interplay: A New Era of Online Protection for Minors

With the enactment of the Digital ECA and the assignment of its monitoring to the ANPD, Brazil enters a new era of children's online protection grounded on a strong legal and institutional framework. Since the Digital ECA has a significant data protection component, it is expected that both frameworks will closely interact and mutually reinforce each other. The new online safety legislation can be viewed as an expansion of privacy safeguards laid by the LGPD, translating existing data protection principles and obligations to specific obligations and preventive measures designed to achieve safety for minors online. These include a series of obligations such as introducing services and products with the most protective and private default settings, providing age verification and parental supervision tools, and imposing further restrictions on processing of children's data, including specific prohibitions on profiling for emotional analysis and targeted advertising.

At the same time, by assigning the powers to enforce the Digital ECA in the ANPD, the law extends the agency's supervisory authority to the protection of children online, expanding its role of supervising data protection to encompass a broader mandate to achieve children's online safety. This includes evaluating potentially harmful content online for minors, issuing guidance on novel concepts introduced by the legislation, such as the "likelihood of access" criterion and additional elements to consider in risk assessments that go beyond privacy, such as assessing potential impact on a child's development. Considering the broad scope of the legislation—covering essentially any online product or service likely to be accessed by minors—the ANPD is entering a new regulatory phase in which its active voice and global positioning will be significantly relevant in the protection of minors in digital environments in Brazil and beyond.


Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org