PRADO VIDIGAL

Digital ECA

Brazil´s Digital Child and Adolescent Statute

NAVIGATING THE NEW RULES FOR THE ONLINE ENVIRONMENT

Material prepared by **Prado Vidigal Advogados** on September 24, 2025 - Version 1 (English)

Introduction

With the approval of the Digital Child and Adolescent Statute (Federal Law No. 15.211/2025), the regulatory landscape for technology companies in Brazil has recently undergone its most profound transformation since the Brazilian General Data Protection Law (LGPD).

The newly enacted legislation, which establishes the Digital Child and Adolescent Statute ("Digital ECA"), represents one of the most ambitious and extensive legislative initiatives in the world focused on protecting children and adolescents in the digital environment.

In both scope and strictness, the Brazilian Law is more comprehensive than well-established regulations such as the Children's Online Privacy Protection Act (COPPA) in the United States and the provisions of the European Union's General Data Protection Regulation (GDPR) applicable to minors, aligning with, and in some respects exceeding, the standards set by the United Kingdom, such as the Age Appropriate Design Code (AADC) and the Online Safety Act.

For the technology sector, the impacts of this new legislation are multifaceted, requiring a reassessment of operations, product design, and business models.

Scope of application

The Digital ECA uses an expansive "likely access" standard to define its scope of application. This drastically broadens the law's applicability, potentially encompassing a large portion of the digital ecosystem operating in Brazil.

Technical challanges

By expressly prohibiting age self-declaration for services or content with pornographic or otherwise unlawful material, the law creates the need for robust age verification mechanisms.

Business models

The Law directly impacts established monetization and engagement practices. The prohibition of loot boxes in games aimed at, or likely to be accessed by minors, along with the ban on profiling children and adolescents for advertising purposes, requires companies to rethink their revenue strategies and user interaction models.

Severe sanctions

The Law also grants the competent authority (ANPD) the power to oversee its enforcement, monitor compliance, and issue regulations and/or procedures for its implementation, with powers to impose severe sanctions, including fines of up to BRL 50 million, as well as the suspension or prohibition of activities.

A new milestone in digital regulation

With the Digital ECA, the pact of responsibility between digital platforms and the Brazilian society is redefined. Meeting the demands of this new paradigm will take more than adjustments to terms and policies. Instead, it will require a broad, strategic rethinking of products, business practices, operations, and governance.

Who does it apply to?

The Law applies to “any information technology product or service aimed at, or likely to be accessed by, children and adolescents in Brazil.” Paragraph 1 of Article 1 defines this concept based on three cumulative requirements, marked by a notable degree of subjectivity:

01 Reasonable probability of use and appeal

02 Considerable ease of use and access

03 Significant degree of risk to privacy, safety or biopsychosocial development

This broad and subjective definition places the burden of proof on digital companies that claim their activities are outside the scope of the Digital ECA. Ignoring the presence of underage users, a common practice under more lenient regulatory regimes, has now become a legally risky and inadvisable approach.

Attention!

The Digital ECA does not affect only the usual suspects (social networks, video platforms, online games) but may also impact a much broader range of services, from e-commerce platforms to forums and news outlets.

Key Duties and Restrictions

01 Best Interests, Privacy by Design & by Default

Article 3 of the new Law provides that digital products and services directed at, or likely to be accessed by, children and adolescents must prioritize the best interests of minors. Under Article 5, paragraph 2, this includes protecting their privacy, safety, mental and physical health, access to information, freedom to participate in society, meaningful access to digital technologies, and overall well-being. The administrative authority provided for under the Digital ECA may issue recommendations and guidance regarding practices relevant to fulfilling these obligations.

While Article 6 details the types of content, products, and practices that cannot be accessed, exposed, or recommended to minors, Article 7 of the Digital ECA makes the principles of privacy by design and privacy by default an explicit legal obligation for products and services for children and adolescents. It requires providers, “from the conception of their products and services, to ensure, by default, the most protective configuration available with respect to privacy and the protection of personal data.” Paragraph 1 further reinforces that services must, by default, operate “with the highest level of protection for privacy and personal data.”

Article 8 requires companies to conduct continuous and rigorous risk management, assessing the impact of their algorithms, features, and recommendation systems on the safety and health of minors. This includes the obligation to actively prevent and mitigate the risks of exposure to harmful content, such as that which incites self-harm, suicide, violence, harassment, and the use of substances that cause chemical or psychological dependency, as prohibited under Article 6.

Under Article 8, item IV, companies must also ensure that, from the design stage, products and services use default settings that prevent excessive or compulsive use. In practice, this may require significant changes to user registration flows and default user settings.

Finally, Article 16, item II, requires the preparation of a “report on the impact, monitoring, and evaluation of personal data protection,” to be shared with the autonomous administrative authority upon request, especially when minors’ data are processed for purposes not strictly necessary for operating the product or service.

02 Age Verification

The prohibition of age self-declaration is arguably the most technically challenging provision. Article 9, paragraph 1, provides that, in order to prevent children and adolescents from accessing content that is inappropriate, unsuitable, or prohibited for minors, providers must adopt “reliable age verification mechanisms at each user access [...], with **self-declaration prohibited**.”

According to the new Law, products, services, or content containing pornographic material, or any other material prohibited under current legislation, must be considered “inappropriate or unsuitable” for minors.

Attention!

This marks a paradigm shift. The common internet model of relying on users to self-declare their age, whether by typing in a birth date or simply clicking 'I am over 18,' is now explicitly prohibited by law.

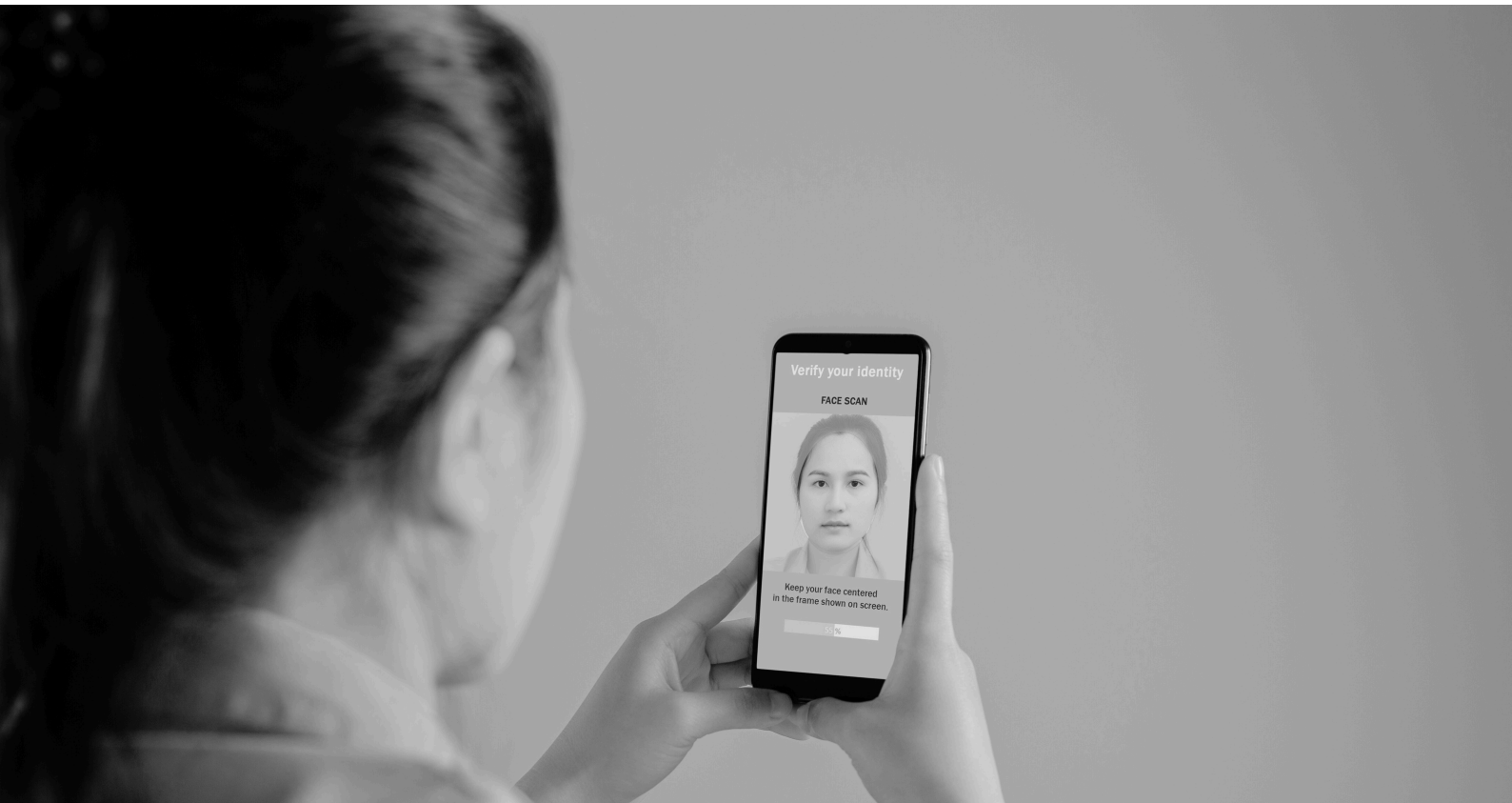
In the context of the UK Online Safety Act, Ofcom (the UK regulatory authority) has issued guidelines listing methods deemed effective, such as open banking validations, photo-based identity verification, facial age estimation, mobile operator age checks, credit card verification, and digital identity services.

In Article 12, Brazil's Law goes even further by requiring app store and operating system providers to develop mechanisms to verify users' age and transmit an 'age signal' to applications via an API, while still adhering to the principle of data minimization.

The choice of an age verification mechanism involves a delicate trade-off between robustness and privacy. Methods such as uploading identity documents may be effective, but they require collecting critical data that, before the Law, was unnecessary for platform operations.

Alternative techniques, on the other hand, depend on emerging technologies, with results that will not always be 100% effective or secure.

As a result, the obligations set out in the new legislation create a regulatory paradox that service and application providers will find difficult to navigate: the risk that the chosen method to meet strict age verification requirements may be deemed insufficient and/or conflict with other existing rules, particularly in the field of data protection.



03 Advertising, Profiling, and Loot Boxes

The Digital ECA directly impacts central business models in the digital economy, affecting the following activities.

Advertising and Profiling
(Articles 22 and 26)

The Law imposes a broad and explicit prohibition on the creation of behavioral profiles of children and adolescents for commercial advertising purposes.

In addition, the use of immersive technologies such as Augmented Reality and Virtual Reality, as well as emotional analysis, is prohibited for the targeting of advertising to this audience.

This approach goes even further than the Age-Appropriate Design Code (AADC) issued by the ICO (the UK data protection authority), which requires profiling to be disabled by default but does not completely prohibit it where adequate safeguards are in place.

Loot Boxes
(Article 20)

The Digital ECA establishes a ban on loot boxes in electronic games directed at, or likely to be accessed by, children and adolescents, as defined by the age rating system.

This stands among the world's toughest stances on this monetization practice.

In the European Union, the debate is still ongoing, with the European Parliament calling for a common approach that, for now, focuses more on transparency about probabilities than on prohibition. Although some countries, such as Belgium and the Netherlands, have local restrictions, there is still no EU-wide consensus.

What are loot boxes?
Under the Law, loot boxes are defined as: "a functionality available in certain electronic games that allows the player, upon payment, to acquire consumable virtual items or random advantages, redeemable by the player or user, without prior knowledge of their content or any guarantee of their actual utility."

04 Parental Supervision

In Article 12, item II, the Law establishes the duty to provide parental supervision and control tools. Article 17 further requires that such tools be effective, easily accessible and usable.

As set out in Article 17, paragraph 4, and Article 18, these tools must allow parents and legal guardians to exercise detailed and informed control, including, at a minimum, the following functionalities:

Account Management
View and manage account and privacy options.

Financial Control
Restrict or block purchases and financial transactions.

Geolocation Management
Restrict the sharing of geolocation data, which, under the Law, must always be accompanied by a clear notice of tracking.

Usage Time Management
Provide metrics on total usage time and restrict features that encourage excessive use, such as autoplay of videos and infinite content feeds.

Interaction Monitoring
Identify the profiles of adults with whom the child or adolescent communicates.

Control over Recommendations
Disable or control personalized recommendation systems.

05 App Stores and Operating Systems

Article 12 of the Law assigns direct responsibilities with significant technical impact to app store providers (such as Google Play Store and Apple App Store) and operating system providers, requiring them to:

Age verification

Implement secure and proportionate technical measures to verify users' age or age group, always in compliance with the data minimization principles of the LGPD.

Age signal

Provide a secure API that enables the transmission of an "age signal" to third-party applications.

Parental consent

Require parents' or guardians' free, informed, and unambiguous consent before children and adolescents can download applications.

06 Association of Accounts on Social Networks

For social networks, Article 24 establishes one of the most challenging obligations from an operational standpoint. Providers must ensure that the accounts of children and adolescents up to 16 years old are formally associated to the account of one of their legal guardians. This measure aims to create a digital bond that facilitates parental supervision and monitoring.

Paragraph 1 of this Article further imposes the duty to actively monitor and restrict the display of content that may attract children and adolescents on platforms inappropriate for minors, in addition to continuously enhancing age verification mechanisms.

07 Content Removal

Article 29 introduces a notice and takedown rule, requiring providers to remove content that violates the rights of children and adolescents (as defined in Article 6) as soon as they are notified by the victim, a parent or guardian, the Public Prosecutor's Office, or child protection entities, regardless of a court order. Article 27 further establishes the duty to remove and report to the authorities any detected content involving exploitation, sexual abuse, abduction, or grooming of minors.

08 Transparency and Accountability

Article 31 requires providers subject to the Digital ECA with more than 1 million registered underage users in Brazil to prepare and publish, on a semiannual basis and in Portuguese, detailed reports on their protection activities. These reports must include the following information:

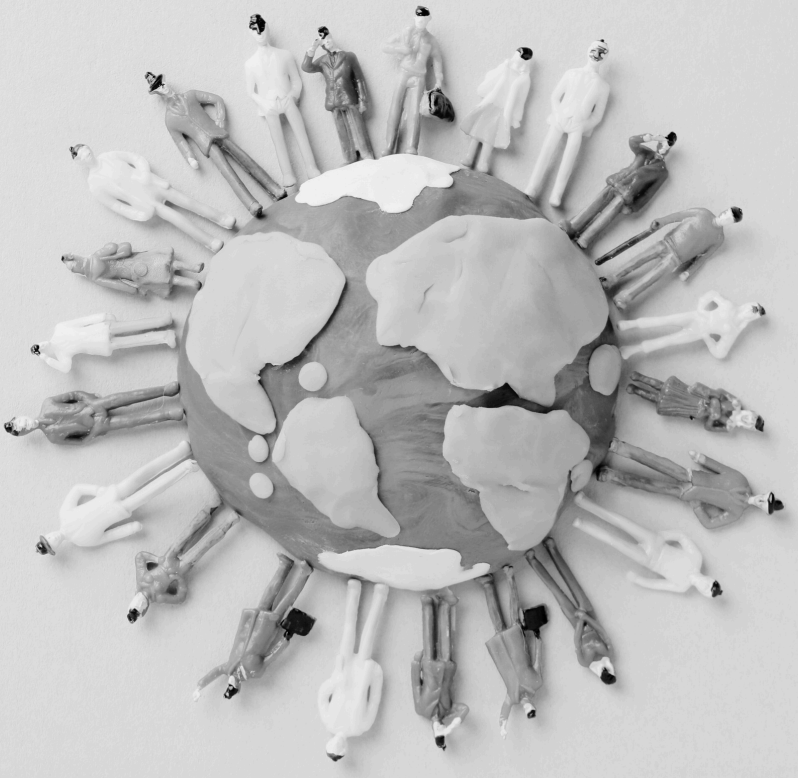
- **Reporting Channels**: details on the available channels for submitting complaints, along with the systems and procedures used for their investigation.
- **Content Moderation:** volume of reports received and actions taken to moderate content or accounts, detailed by category.
- **Technical Protection Enhancements:** details on the technical enhancements implemented to protect the personal data and privacy of children and adolescents.
- **Parental Consent**: technical enhancements for verifying parental consent.
- **Risk Management**: detailed disclosure of the methodologies applied and the presentation of the outcomes of impact assessments, including the processes for identifying, evaluating, and mitigating risks to the safety and health of children and adolescents.

In addition, Paragraph 1 of Article 31 requires these providers to grant free access to data for academic, scientific, technological, innovative, or journalistic research on how their products and services affect the rights of children and adolescents. Confidentiality of the information must always be preserved, and the commercial use of such data is prohibited.

09 Obligation to Maintain a Representative in Brazil

Article 40 of the Digital ECA requires all providers subject to the new Law to appoint and maintain a legal representative in Brazil.

This representative must have full authority to receive legal notices, summons, and administrative communications, ensuring that foreign companies are held accountable before Brazilian authorities and courts.



Online Protection of Minors in Comparative Law

	 Digital ECA	 COPPA	 AADC & Online Safety Act	 Online Safety Act
Age of Protection	Minors under 18	Minors under 13	Minors under 18	Minors under 18
Scope of Application	Services “directed to” or “likely to be accessed” by children and adolescents.	Services “directed to children” or with “actual knowledge” of collecting children’s data.	Services “likely to be accessed” by minors under 18.	Broad in scope. Focus on “harmful content for minors.”
Age Verification	Self-declaration is not allowed for 18+ content, and platforms must use “reliable mechanisms.”	Age verification is not required, but parental consent must be obtained before collecting data from a user known to be under 13.	Requires “highly effective age assurance” for harmful content (e.g., pornography).	Requires “reasonable measures” to prevent minors from accessing restricted (18+) content.
Advertising	Explicit prohibition of profiling children and adolescents for advertising purposes.	Restricted by the requirement of parental consent for data collection.	Profiling must be disabled by default.	An “Online Privacy Code” is under development, which will address the matter in a specific manner.
Loot Boxes	Prohibition in games directed to, or likely to be accessed by, minors.	Not regulated at the federal level.	In discussion.	Receive age ratings of 15+ or 18+ (gambling simulation).

Supervision and Sanctions

Article 34 provides for the creation of an "autonomous administrative authority for the protection of the rights of children and adolescents in the digital environment," which, pursuant to Decree No. 12.622 of 2025, will be the Brazilian National Data Protection Agency (ANPD).

The designation of an autonomous and specialized entity is a critical factor. This distinguishes it from models where oversight is dispersed among various agencies or relies exclusively on the initiative of the judicial system. The ANPD now assumes primary responsibility for overseeing compliance with the Law throughout the national territory and, crucially, the power to issue supplementary rules and regulations.

Therefore, the existence of an authority whose function is to actively supervise compliance with this specific Law creates a proactive oversight environment. This requires companies to maintain a robust and continuously updated compliance program, rather than adopting a merely reactive posture.

Sanctions under the Digital ECA

The authority's powers are backed by a strict and wide-ranging sanctioning framework, set out in Article 35. Sanctions follow a progressive scale:

01 — Warning
Accompanied by a timeframe to implement corrective measures.

02 — Simple Fine
May reach up to 10% of the economic group's revenue in Brazil in the previous fiscal year, capped at BRL 50 million per violation.

03 — Suspension of Operations

04 — Prohibition of Activities

Under Article 35, Paragraph 5, the most severe sanctions, such as suspension and prohibition of activities, which may effectively remove a service from the market, require a court decision.

Pursuing Compliance

The Digital Child and Adolescent Statute is not merely another regulatory layer. It represents a paradigm shift in how the responsibility of companies within the digital ecosystem is conceived and enforced in Brazil. The Law demands a holistic approach that goes beyond the legal department, embedding legal, ethical, technical, and product design considerations at the heart of operations.

Conversely, there is a strategic opportunity for companies that lead this transition. Those that genuinely embrace the principles of the Law, investing in the creation of digital environments that are evidently safe, positive, and empowering for young audiences, will be able to turn a heavy compliance obligation into a powerful brand differentiator.

Attention!

Compliance deadline: **March 17, 2026** (pursuant to Provisional Measure No. 1.319/2025).

The path to compliance with the Digital ECA is undoubtedly complex, with many legal and technical nuances. Given such context, the deadline appears to be rather tight in light of the adjustments that will be required from the companies affected by its provisions.

At Prado Vidigal, we are fully prepared to support your organization in ensuring compliance with Brazil's new digital regulatory framework.

PRADO VIDIGAL

Contact us

Access our website