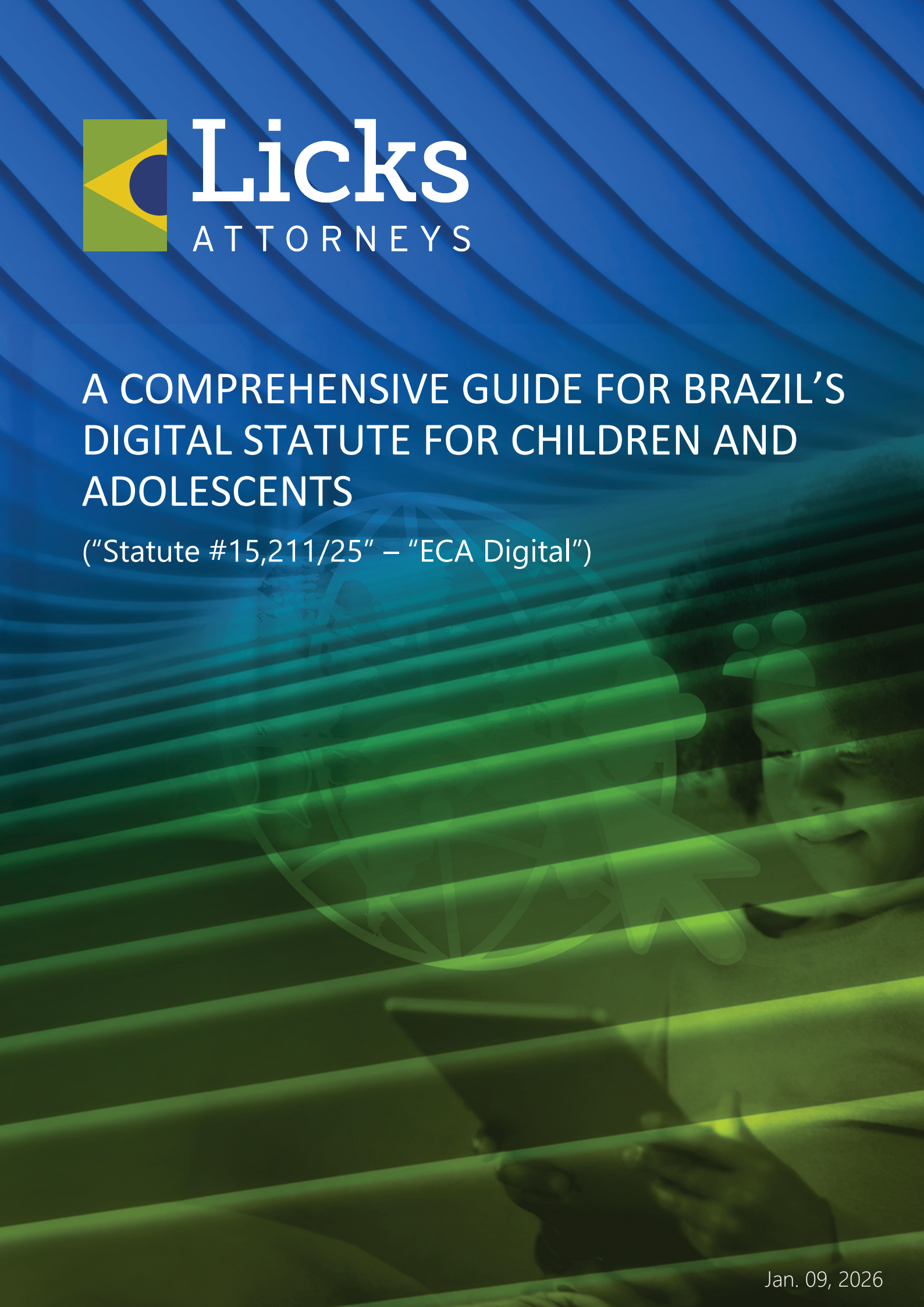
Licks
ATTORNEYS

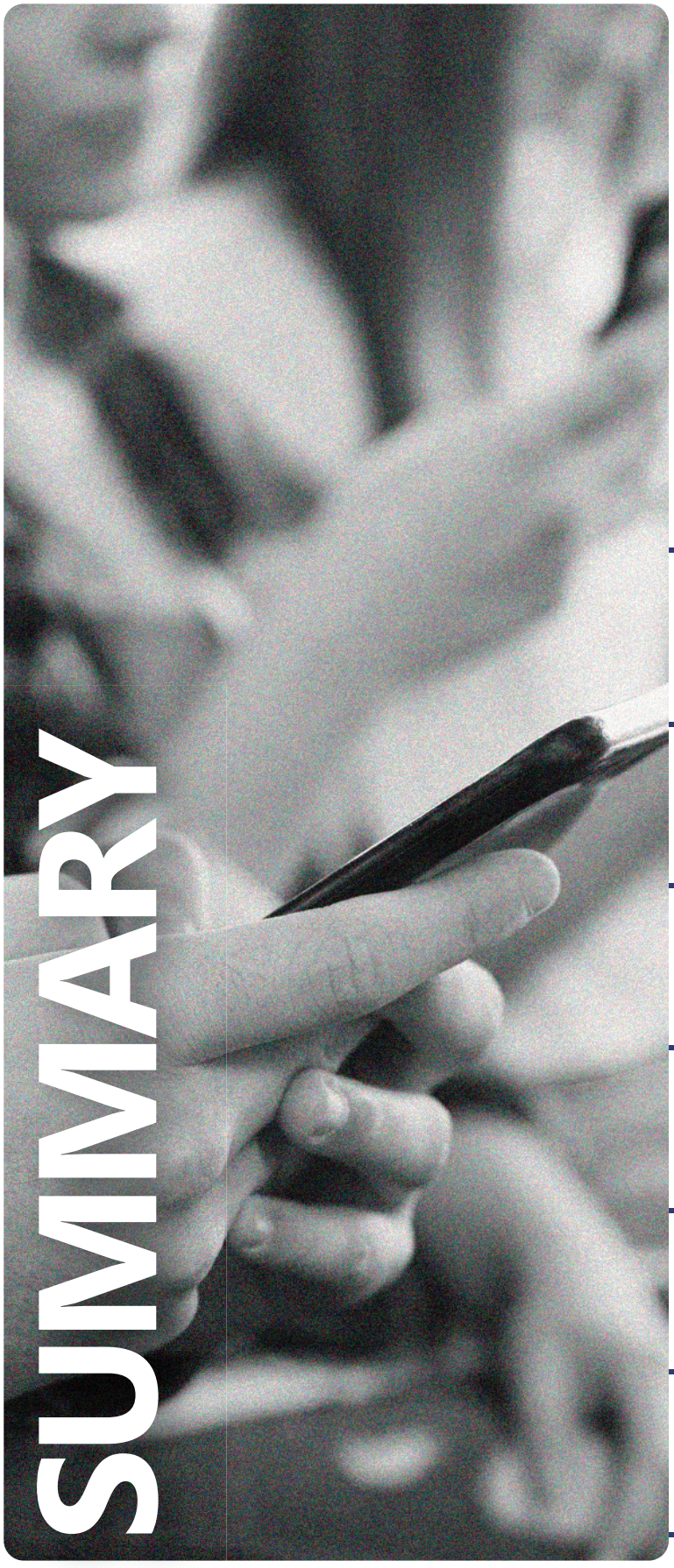
A COMPREHENSIVE GUIDE FOR BRAZIL'S DIGITAL STATUTE FOR CHILDREN AND ADOLESCENTS

("Statute #15,211/25" – "ECA Digital")



Jan. 09, 2026

Licks ATTORNEYS



SUMMARY

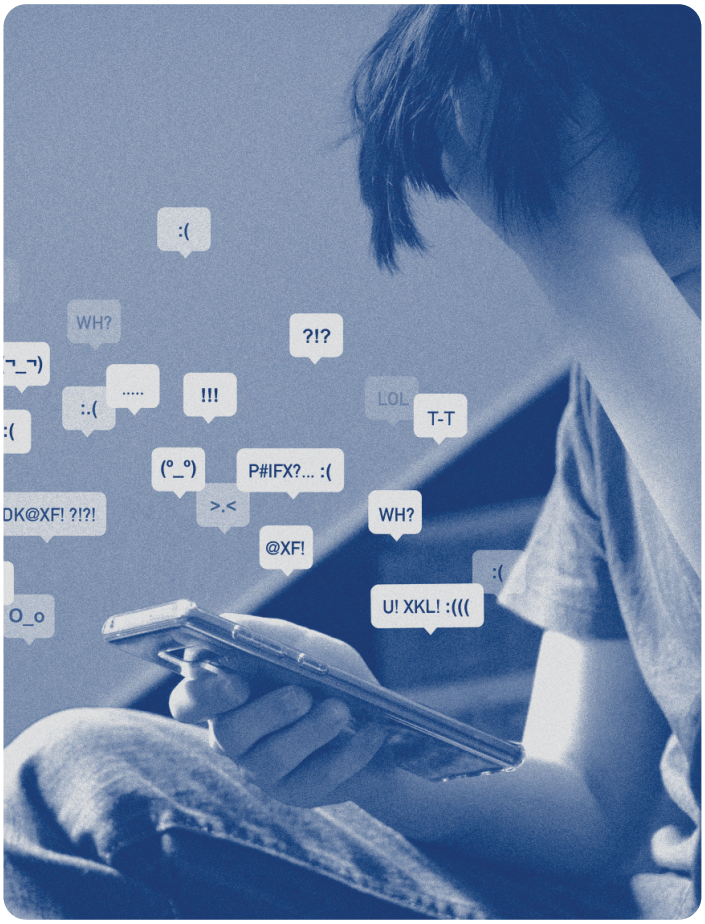
01 INTRODUCTION

In September 2025, Brazil passed the Digital Statute for Children and Adolescents ("Statute #15,211/25" – "ECA Digital"), which establishes a comprehensive set of rules for the protection of minors in the digital environment. The new rules, which will come into force on March 17, 2026, will apply to ***all providers of information technology products or services directed at or likely to be accessed by children and adolescents*** (hereinafter referred to as ***"in-scope providers"***).

The ECA Digital expands the scope of protection granted to minors under Brazilian law by extending to the digital environment the principles and rights originally established by the Statute for Children and Adolescents' Rights (Statute #8,069/90). The enactment of the ECA Digital represents a landmark in Brazil's regulatory landscape, reinforcing the country's commitment to creating a safer and more responsible digital ecosystem for minors. By introducing stringent obligations on age verification, parental controls, and content moderation, the Statute aims to mitigate risks such as exposure to harmful content.

Beyond its social relevance, the law will significantly impact the technology and digital services market, imposing new compliance requirements and operational adjustments. Companies operating in Brazil will face a complex regulatory framework that demands robust governance, transparency, and proactive risk management, reshaping business models and compliance strategies across the industry.

This guide aims to outline the key provisions of the Statute, detailing, in a structured and organized manner, its most relevant rules. It offers an overview of the new regulatory framework and highlights certain measures that digital platforms operating in Brazil will need to implement to ensure compliance.



02 BACKGROUND

Bill #2,628, which originated ECA Digital, was proposed in late 2022 by Senator Alessandro Vieira. It was approved by the Senate in December 2024 and subsequently forwarded to the House of Representatives.

The bill gained significant momentum in August 2025, after influencer Felipe Bressanim Pereira, known as "Felca", released a viral video denouncing the sexualization of minors on social media.[1] The video reached millions of views, garnered nationwide attention, and substantially influenced the debate on minors' online protection, effectively accelerating the legislative process.

Due to the widespread social attention sparked by the video, the bill was fast-tracked and approved by the House of Representatives within weeks. The episode's influence was so strong that the Statute became informally known as the "Felca Law." Its approval represents a response to growing public demand for stricter social media regulation, driven by concerns over harmful activities in social media.

[1] https://www.youtube.com/watch?v=FpsCzFGL1LE

03 KEY DEFINITIONS, SCOPE, AND APPLICABILITY

Applicable to any digital product or service that is either **directed at or likely to be accessed by minors**

Definitions

Brazil lacks a comprehensive legislation regulating digital services. Existing regulation is fragmented across instruments such as the Brazilian Internet Act (Statute #12,965/14 or "MCI") and the Brazilian General Data Protection Act (Statute #13,709/18 or "LGPD"). Among other provisions, these statutes establish relevant definitions for key concepts in digital regulation.

As a new framework for online services, the ECA Digital interacts with and complements these existing norms. However, it introduces novel definitions that do not necessarily align with preexisting concepts. Therefore, to fully comprehend the ECA Digital it is first necessary to understand a few concepts created by the Statute:

- **Information technology product or service:** a product or service provided at a distance, by electronic means, and at the individual request of a recipient, such as internet applications, computer programs, software, terminal operating systems, internet application stores, and electronic and similar games connected to the internet or another communications network. This does not include essential functionalities for the operation of the internet, such as open and common technical protocols and standards that allow for the interconnection between computer networks that compose the internet.

- **Social media platform:** an internet application whose main purpose is the sharing and dissemination, by users, of opinions and information conveyed through text or image, sound, or audiovisual files, on a single platform, through connected or articulately accessible accounts, allowing for connection between users.

- **Internet applications store:** an internet application that distributes and facilitates the download, for users of terminals, of internet applications made available or accessible through its platform.

- **Operating systems:** system software that controls the basic functions of hardware or software and allows internet applications, computer programs, applications, or other software to run on it.

- **Parental supervision mechanism:** a set of configurations, tools, and technological safeguards integrated into information technology products or services directed at or likely to be accessed by children and adolescents, which enable parents or legal guardians to supervise, limit, and manage the use of the service, the content accessed, and the processing of personal data performed.

- **Service with editorial control:** an internet application whose main purpose is to make previously selected content available without the use of automated selection means, by a responsible economic agent.

Scope and applicability

The Statute establishes a broad scope of application, encompassing not only products and services specifically designed for minors but also those that are likely to be accessed by them, irrespective of their location, development, manufacture, offering, commercialization, or operation.

The concept of "likely to be accessed" is inspired by the United Kingdom's Age-Appropriate Design Code and the Online Safety Act, both regulating children's use of digital services. Under the ECA Digital, the determination of whether a service or product is "likely to be accessed" is based on three factors:

i. sufficient likelihood of use and attractiveness of the information technology product or service by children and adolescents;

ii. considerable ease of access to and use of the information technology product or service by children and adolescents; and

iii. a significant degree of risk to the privacy, security, or biopsychosocial development of children and adolescents, especially in the case of products or services intended to enable social interaction and the large-scale sharing of information among users in a digital environment.

The Statute's wide scope is a deliberate choice by lawmakers to ensure its effectiveness and guarantee the protection of minors across multiple digital contexts. However, this expansive approach, particularly the broadness of the criteria for determining what is "likely to be accessed", may create challenges for interpretation and enforcement. Until further definitions or regulatory guidance are issued, adopting a conservative approach is advisable to ensure compliance and reduce legal uncertainty.

04 PRINCIPLES

The Statute establishes the foundational principles to be observed in the provision of digital products and services to minors:

- **Priority and full protection:** the Brazilian Constitution and the Statute for Children and Adolescents' Rights mandate that children and adolescents, due to their unique stage of development, must have their rights guaranteed with absolute priority across all areas. This protection is a shared responsibility of families, the State, and society, ensuring not only fundamental rights but also those specific to childhood and adolescence. The ECA Digital updates this scope and establishes that information technology products and services targeted at or likely to be accessed by minors must ensure priority protection of these users and must also incorporate adequate and proportionate measures to ensure a high level of privacy, data protection, and safety.
- **Best interest:** the provision of information technology products and services targeted at or likely to be accessed by minors must be guided by their best interest. For the purposes of the Statute, the expression of minors' best interest means the protection of their privacy, security, mental and physical health, access to information, freedom of participation in society, meaningful access to digital technologies, and well-being.
- **Risk prevention by design:** in-scope providers must adopt reasonable measures from the design stage to prevent and mitigate risks of exposure to harmful content, including content related to sexual exploitation and abuse, physical violence, cyberbullying, incitement to self-harm or substance abuse, gambling, predatory advertising, and pornography.
- **Privacy by design and by default:** in-scope providers must, from the design of their products and services, ensure, by default, the most protective configuration available regarding privacy and personal data protection.

Additionally, the Statute reiterates, in several provisions, the shared responsibility of families, society, and the State for safeguarding and guaranteeing the rights of minors, as enshrined in Article 227 of the Brazilian Constitution.[2]

05 MAIN OBLIGATIONS

General duties

Brazilian legislation on the protection of consumers (Consumer Protection Code, Statute #8,078/90) and minors (Statute for Children and Adolescents' Rights, Statute #8,069/90) provides an extensive and open-ended list of duties and rights that are often broad and vague. The ECA Digital reinforces some of these dispositions, such as:

- Duty of prevention;
- Duty of protection;
- Duty of information;
- Duty of safety;
- Best interest of the minor; and
- Full, special, and priority protection of minors.

The ECA Digital also establishes that in-scope providers must develop configurations that prevent the compulsive use of products or services by children and adolescents from the design stage. Said configurations must be adopted by default. However, the Statute does not provide any objective criteria for of what could be considered "compulsive use".

These broad provisions are frequently interpreted by authorities in an expansive manner to impose obligations on service providers that are not expressly set forth in legislation. A similar enforcement approach is expected regarding the duties and rights specifically referenced in the ECA Digital. In-scope providers should remain attentive, as authorities may attempt to impose specific duties or restrictions not expressly provided for in the law, relying on generic provisions such as the duties of prevention, protection, and safety.

[2] **Brazilian Constitution, Article 227**. It is the duty of the family, the society, and the State to ensure children, adolescents, and young people, with absolute priority, the right to life, health, nourishment, education, leisure, professional training, culture, dignity, respect, freedom, and family and community life, as well as to guard them from all forms of negligence, discrimination, exploitation, violence, cruelty, and oppression.

Risk management

The ECA Digital requires in-scope providers to manage the risks of their resources, functionalities, and systems and their impact on the safety and health of children and adolescents.

Content moderation

The Statute requires in-scope providers to assess the content made available to minors according to age group, ensuring compatibility with the corresponding age rating. It also establishes that such providers must take reasonable measures, from the design stage and throughout the operation of their applications, to prevent and mitigate risks of access, exposure, recommendation, or facilitation of contact with content involving:

- illegal or age-inappropriate content;
- sexual exploitation and abuse;
- physical violence, cyberbullying, and harassment;
- inducement, incitement, instigation to practices or behaviors that lead to harm to the physical or mental health of children and adolescents, such as physical violence or psychological harassment towards other children and adolescents, use of substances causing chemical or psychological dependence, self-diagnosis and self-medication, self-harm, and suicide;
- promotion and commercialization of games of chance, fixed-odds betting, lotteries, tobacco products, alcoholic beverages, narcotics, or products whose sale is prohibited to children and adolescents;
- predatory, unfair, or deceptive advertising practices or other practices known to cause financial harm to children and adolescents; and
- pornographic content.

These types of content are considered to violate the rights of children and adolescents.

The Statute suggests the following prevention measures: *(i)* clear and effective policies for the prevention of cyberbullying and other forms of online harassment, with adequate support mechanisms for victims; as well as *(ii)* the development and availability of educational awareness programs directed at children, adolescents, parents, educators, employees, and support teams regarding the risks and methods for prevention and combat such practices.

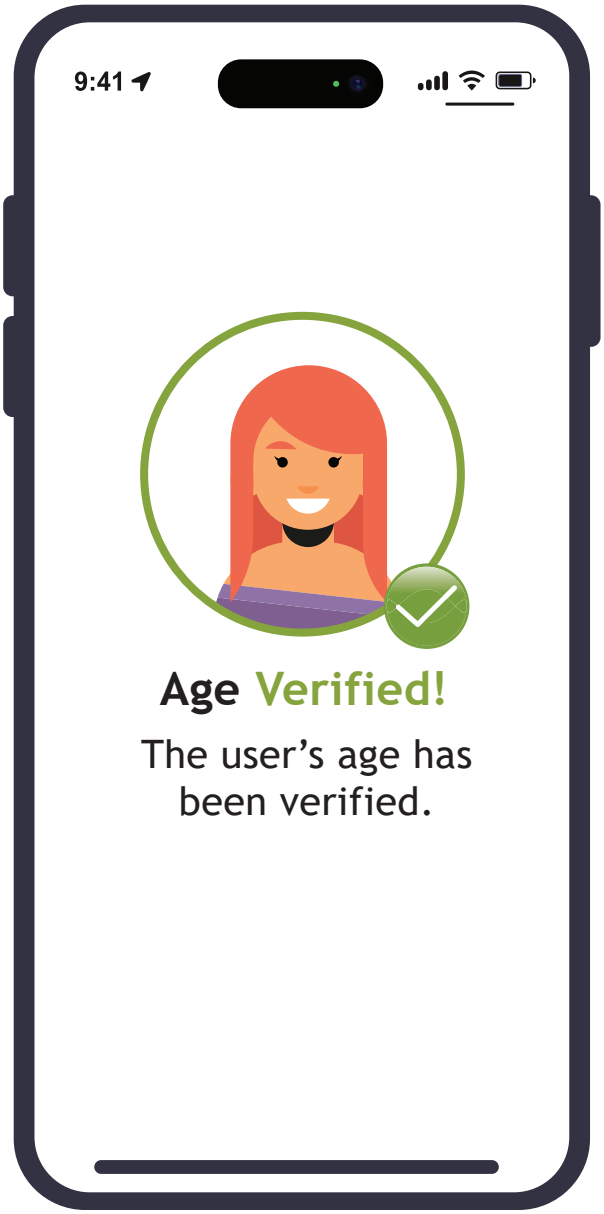
Furthermore, it is the duty of in-scope providers to remove content referred above as soon as they are made aware of the offensive nature of the publication by the victim, their representatives, the Public Prosecutor's Office, or entities representing the defense of the rights of children and adolescents, regardless of a court order *(notice-and-takedown regime)*.

Finally, the ECA Digital creates specific rules for moderating *Child Sexual Abuse Material (CSAM)*. ***Providers of information technology products or services available in the national territory***[3] must remove and report content of apparent exploitation, sexual abuse, kidnapping, and grooming detected in their products or services, directly or indirectly, to the competent national and international authorities, as will be detailed in forthcoming regulations.

Providers must preserve *(i)* the infringing content reported and *(ii)* data of the user responsible for the content and related metadata for 6 months. This period may be extended at the request of law enforcement.

Age verification

The ECA Digital requires in-scope providers to *(i)* extensively inform all users about the indicated age range for the product or service at the time of access, as established by the indicative rating policy, and to *(ii)* adopt mechanisms to provide age-appropriate experiences, which means they should be able to verify the age of their users.



As per the Statute, ***providers of internet application stores and operating systems*** must take security measures to ascertain the age or age range of users. Authorization for the download of apps by minors shall depend on the free and informed consent of parents or legal guardians.

After ascertaining the age of their users, ***providers of internet application stores and operating systems*** must also share age signals via secure Application Programming Interface (API) with providers of internet applications, which must adopt technical and organizational measures to ensure the receipt of the age signals.

Although this provision suggests that age verification will rely on the signals to be shared by ***providers of application stores and operating systems***, the Statute establishes that in-scope providers must implement their own mechanisms to prevent improper access of children and adolescents to content inappropriate for their age group, regardless of the signals.

Data collected for the age verification of children and adolescents may be used solely for this purpose, with its processing for any other purpose being prohibited.

Further regulation will establish the minimum requirements for transparency, security, and interoperability for the age assurance mechanisms adopted by ***app stores and operating systems***.

[3] The black letter of the law indicates that this is an obligation directed at providers of products or services available in the national territory, **not only providers of information technology products or services directed at children and adolescents or likely to be accessed by them**. A conservative approach suggests that this obligation covers any providers of information technology products or services available in Brazil, not only those directed at or likely to be accessed by minors.

Parental supervision and controls

The ECA Digital requires in-scope providers to offer accessible and "easy-to-use" settings and tools that "support parental supervision". Information on the existing tools for parental supervision must be displayed in an easily accessible location. According to the Statute, parental supervision tools must allow parents and legal guardians to:

- view, configure, and manage the account and privacy options of the child or adolescent;
- restrict purchases and financial transactions;
- identify the profiles of adults with whom the child or adolescent communicates;
- access consolidated metrics of the total time of use of the product or service and allow the limitation of usage time; and
- activate or deactivate safeguards through accessible and appropriate controls; and have access to information and control options in Portuguese.

Default settings of parental supervision tools must adopt the highest level of protection available, ensuring, at a minimum:

- restriction of communication with children and adolescents by unauthorized users;
- limitation of features designed to artificially increase, sustain, or extend the use of the product or service by the child or adolescent, such as automatic media playback, rewards for time of use, notifications, and other features that may result in excessive use of the product or service by a child or adolescent;
- provision of tools for monitoring the appropriate and healthy use of the product or service;
- use of interfaces that allow for the immediate visualization and limitation of the time of use of the product or service;
- control over personalized recommendation systems, including an option to disable them;
- restriction on the sharing of geolocation and provision of a prior and clear notice about its tracking;
- promotion of digital media literacy regarding the safe use of information technology products or services;
- regular review of artificial intelligence tools, with the participation of specialists and competent bodies, based on technical criteria that ensure their safety and suitability for use by children and adolescents, guaranteeing the possibility of disabling non-essential functionalities for the basic operation of the systems; and
- provision, whenever technically feasible, of resources or connections to emotional support and well-being services, with age-appropriate content and evidence-based guidance, especially in cases of interactions with identified psychosocial risks.

Further regulation will establish the minimum requirements for parental supervision mechanisms.

Privacy implications

The Statute prohibits the use of profiling techniques to direct commercial advertising to minors, as well as the use of emotional analysis, augmented reality, extended reality, and virtual reality for this purpose.

Providers of internet applications are prohibited from monetizing and promoting content that portrays children and adolescents in an eroticized or sexually suggestive manner or in a context proper to the adult sexual universe.

When processing children and adolescents' personal data, especially when carried out for purposes beyond those strictly necessary for the operation of the product or service, the controller must *(i)* map the risks and make efforts to mitigate them; and *(ii)* prepare a Data Protection Impact Assessment (DPIA), to be shared with the ANPD upon request.

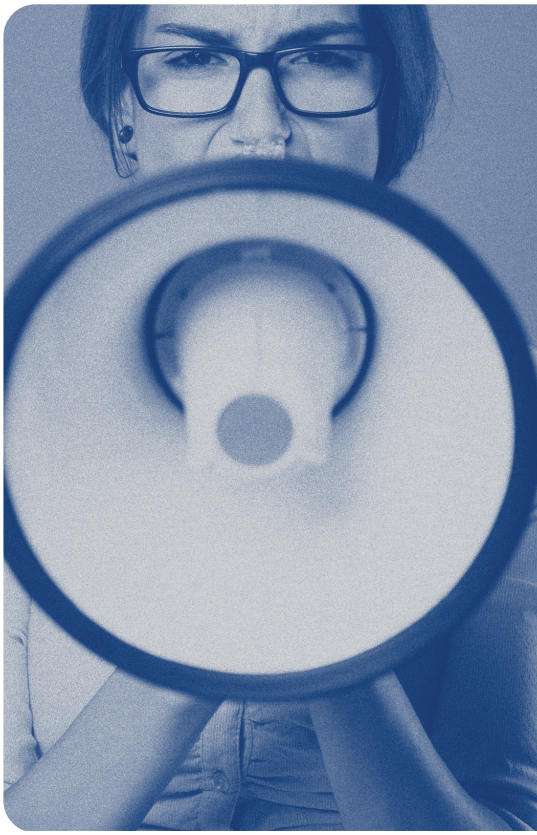
Reporting channels and appeal systems

The ECA Digital requires in-scope providers to make mechanisms available and easily accessible for users to report violations of the rights of children and adolescents. When appropriate, providers must report such violations to competent authorities for the initiation of investigations.

As detailed in the "Content moderation" section, in-scope providers now have the duty to remove content that violates the rights of minors as soon as they are informed of its offensive nature by the victim, their representatives, the Public Prosecutor's Office, or entities representing the defense of the rights of children and adolescents, regardless of a court order (*notice-and-takedown regime*).

The content removal procedure must respect the user's right to challenge the decision, ensuring: *(i)* notification of the removal; *(ii)* justification for the removal, indicating whether the identification resulted from human or automated analysis; *(iii)* the possibility for the user to appeal the measure; *(iv)* easy access to the appeal mechanism; and *(v)* defined procedural deadlines for submitting an appeal and for responding to the appeal.

The ECA Digital also establishes that providers of internet applications must adopt effective mechanisms to identify the abusive use of reporting mechanisms, aiming to prevent their misuse for censorship, persecution, or other illicit practices. In-scope providers must make clear and accessible information available to users about what constitutes improper use of reporting mechanisms and the applicable sanctions.



Sanctions mentioned by the Statue for users abusing reporting mechanisms include "*among others*": *(i)* temporary suspension of the infringing user's account; *(ii)* cancellation of the account in cases of repeated or serious abuse; and *(iii)* reporting to competent authorities when there are indications of a criminal offense or a violation of rights.

In-scope providers must develop and publish objective and transparent procedures for identifying the abusive use of reporting mechanisms and applying sanctions. These procedures must include, at a minimum: *(i)* technical and objective criteria for characterizing abuse; *(ii)* notification to the user regarding the initiation of an investigation and, if applicable, the imposition of sanctions; *(iii)* the possibility for the sanctioned user to appeal; and *(iv)* defined procedural deadlines for submitting an appeal and for a reasoned response from the provider.

Providers of internet applications must also maintain detailed records of identified cases of abuse and the sanctions applied. These records aim to monitor the effectiveness of the mechanisms adopted and promote the continuous improvement of internal procedures, in accordance with criteria and requirements to be defined by regulation.

Transparency reports

The ECA Digital establishes that ***in-scope providers with over one million underage users in Brazil*** must publish semiannual transparency reports in Portuguese, which must include:

i. the channels for receiving reports and the systems and processes for investigation;

ii. the number of reports received;

iii. the amount of content or account moderation actions, classified by type;

iv. the measures to identify child accounts on social media platforms and illicit activities;

v. the technical improvements for children and adolescents' data protection and privacy;

vi. the technical improvements for verifying parental consent; and

vii. the details of the methods used and the presentation of the results of assessments on impact, identification, and management of risks to the safety and health of children and adolescents.

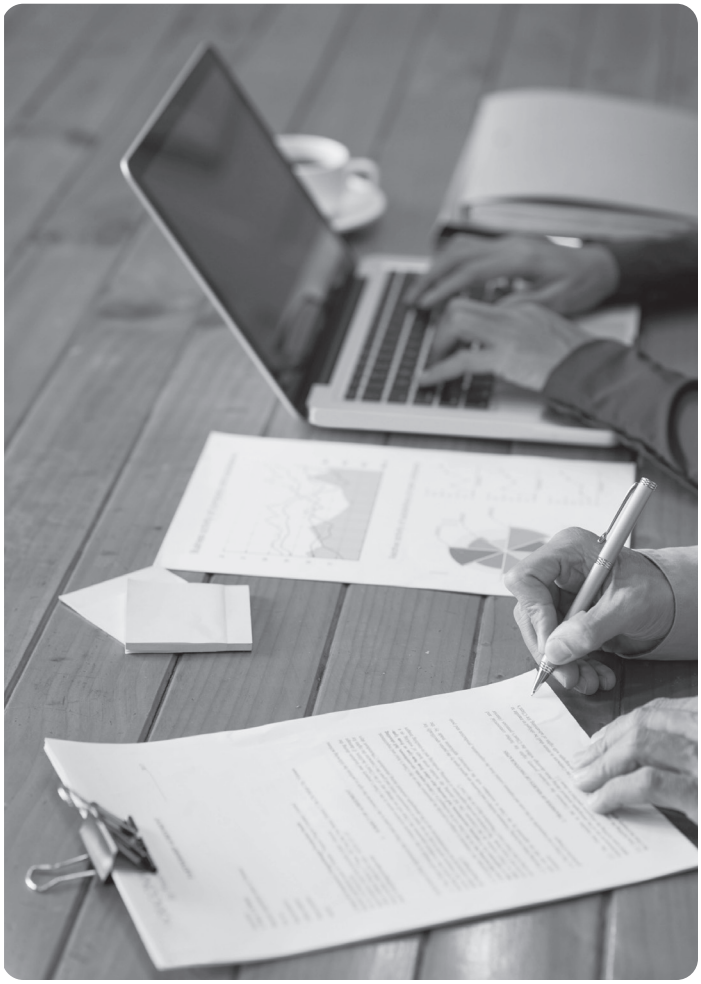
Providers of internet applications shall enable, free of charge, access to data necessary for researching the impacts of their products and services on the rights of children and adolescents and on their best interests, by academic, scientific, technological, innovation, or journalistic institutions, according to criteria and requirements defined in forthcoming regulation. Use of this data for any commercial purposes is prohibited, and compliance with the principles of purpose, necessity, security, and confidentiality of the information must be ensured.

Local legal representation

The ECA Digital requires that in-scope providers maintain a legal representative in the country with the authority to receive judicial and administrative summons, notices, and communications, to respond to Executive, Judiciary, and Public Prosecutor's Office authorities, and to act on behalf of the company before the public administration.[4]

Packaging warning

The ECA Digital establishes that packaging of personal electronic equipment sold in Brazil that allows for internet access must contain a sticker that informs, in Portuguese, parents or legal guardians of the need to protect children and adolescents from accessing websites with improper or inadequate content for this age group.



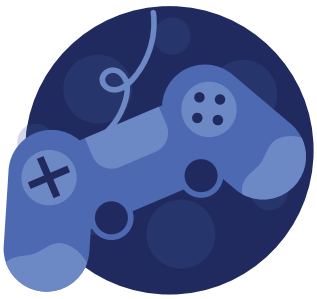
[4] A similar requirement has also been imposed by the Supreme Court ruling on the constitutionality of Article 19 of the Brazilian Internet Act, which is already enforceable and ***applicable to all online service providers with products and services available in Brazil***.

Obligations for specific groups

In addition to the general obligations detailed above, the Statute creates specific obligations for certain groups of providers.

Eletronic Games

Electronic games are regulated in Brazil by Statute #14,852/24 (the "Legal Framework for the Electronic Games Industry in Brazil"). This Framework is now complemented with additional rules created by the ECA Digital.



The ECA Digital establishes that electronic games targeted at or likely to be accessed by minors that include user interaction functionalities through text, audio, or video messaging, or content exchange, must, by default, restrict these interaction features, ensuring consent of parents or legal guardians.

In addition, the Statute prohibits the offering of loot boxes in electronic games targeted at or likely to be accessed by minors.

Social media platforms

According to the ECA Digital, social media platforms must ensure that users or accounts of children and adolescents up to sixteen (16) years old are linked to the user or account of one of their legal guardians.

If their services are improper or inadequate for children and adolescents, social media platforms must adopt adequate and proportional measures to:

i. inform all users in a clear, prominent, and accessible manner that their services are not appropriate;

ii. monitor and restrict, within the limits of their technical capabilities, the display of content that has the evident objective of attracting children and adolescents; and

iii. continuously improve their age verification mechanisms to identify accounts used by children and adolescents.

If there are well-founded indications that an account is used by a child or adolescent in non-compliance with the minimum age requirements provided for in legislation, social media platforms must suspend the user's access and ensure the launching of a swift and accessible procedure in which the legal guardian may present an appeal and prove the age by appropriate means.

Social media platforms must establish specific rules for the processing of children and adolescents' personal data, defined in a concrete and documented manner and based on their best interests.

Finally, the ECA Digital prohibits social media platforms from creating behavioral profiles of child and adolescent users based on the collection and processing of their personal data, including data obtained in age assurance processes, as well as group and collective data, for the purpose of directing commercial advertising.

Providers of content inappropriate for minors

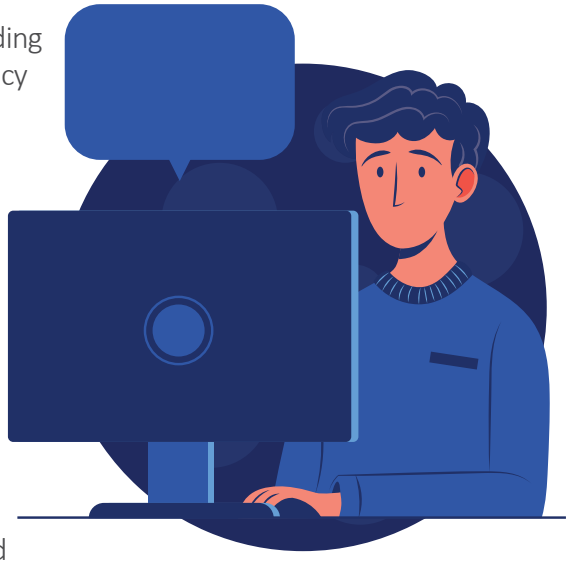
The ECA Digital establishes that providers of information technology products or services that make available content, products, or services whose offer or access is improper, inadequate, or prohibited for persons under 18 years old must adopt effective measures to prevent access by children and adolescents.

To comply with this requirement, providers must implement reliable age verification mechanisms at each access, and self-declaration of age is not permitted. For the scope of this rule, "inappropriate" content, products, or services are defined as those containing pornographic material, as well as other any other content prohibited under current legislation.

Providers that make pornographic content available must also prevent the creation of accounts or profiles by children and adolescents.

Providers of services with editorial control and providers of content protected by copyright

Providers of services with editorial control and providers of content protected by copyright previously licensed from a responsible economic agent who is not an end-user are exempted from complying with most of the obligations detailed herein (content moderation, parental supervision mechanisms, prohibition of providing loot boxes, reporting channels, remove content after notification, transparency reports and appointment of local representative), provided that they:



i. observe the indicative age rating norms of the Executive Branch, when they exist, or, in their absence, the criteria of age appropriateness and clear signaling of potentially harmful content to children and adolescents, as per applicable regulation;

ii. offer transparency in the age rating of the content;

iii. provide easily accessible technical parental mediation mechanisms that allow parents or legal guardians to exercise control over the way children and adolescents use the service, in order to enable the restriction of: (a) content, by age group; (b) processed personal data; (c) interaction with other users; and (d) commercial transactions; and

iv. offer accessible channels for reporting content that is non-compliant with the assigned rating or that violates the rights of children and adolescents, as per applicable regulation.

06 ENFORCEMENT

Centralized governance

The Brazilian Data Protection Agency ("ANPD") has been designated as the primary regulatory authority responsible for overseeing compliance with the ECA Digital and issuing complementary regulations on child safety matters. Enforcement of the obligations provided for in the ECA Digital will take into consideration the product or service's *(i)* characteristics and functionalities, *(ii)* degree of interference over the content made available, *(iii)* number of users, and *(iv)* size.

Established in 2019, the ANPD initially focused on privacy and data protection, enforcing the Brazilian General Data Protection Act ("LGPD"). In 2025, the ANPD became an independent regulatory agency with full technical, administrative, and financial autonomy, similar to other strategic regulators in Brazil.

In addition to being empowered to oversee compliance with the ECA Digital, the ANPD is preparing to expand its mandate to include AI governance. Given these developments, the Agency is currently in a restructuring phase to improve its capacity to effectively regulate, monitor, and enforce compliance.

Recent milestones illustrate this transition:

- On October 15, 2025, the Brazilian Government launched two public consultations regarding the rights and the protection of minors on the internet. The consultations, now closed, aimed to gather input to support the development of new regulations for the ECA Digital.
    - **Age verification on the internet:** The first consultation sought contributions on technical and legal parameters for implementing safe and efficient age verification mechanisms, addressing key challenges in their development and deployment.
    - **National Policy for the Protection of the Rights of Children and Adolescents in the Digital Environment:** Recognizing the growing risks and potential harms of digital technologies on minors' rights, this consultation had two main goals: (i) gather supporting information to develop new regulations for the ECA Digital, and (ii) develop a national policy on the matter.

- On October 21, 2025, the ANPD published a study on age verification mechanisms for children and adolescents in the digital environment. Part of its "Technologic Radar" series, the study provides an overview of current practices, key concepts, and future perspectives, drawing on insights from data protection authorities, child protection agencies, experts, and national legislation, including the ECA Digital.
- On November 28, 2025, the ANPD launched a public consultation, now closed, to clarify concepts within the ECA Digital. The consultation aimed to identify provisions with terminology that may cause doubts or ambiguities, ensuring a clear and uniform understanding of the Statute and ultimate promoting its safe and effective application.

- In December 2025, the ANPD initiated a proceeding to monitor compliance with ECA Digital. The proceeding targets 37 companies offering technology products or services likely to be accessed by children and adolescents in Brazil, aiming to map technical, legal, and organizational measures adopted by them to align with the Statute. Through this process, ANPD seeks to evaluate the maturity of compliance across sectors, identify challenges in implementing protections for minors in the digital environment, and leverage the collected data to support future regulatory decisions.

- On December 22, 2025, the ANPD published an amendment to its Regulatory Agenda for the 2025–2026 biennium. Among other provisions, the Agenda establishes that the ANPD must initiate, **by the end of 2026**:

  - **The development of guidance aimed at clarifying the scope of key concepts related to the application of the ECA Digital**, addressing:

    - The concepts of "information technology product or service" and "likely to be accessed";

    - Specific rules for providers of services with editorial control and providers of content protected by copyright; and

    - Guidance on the duties of prevention, protection, information, and safety, which unfold into general obligations to be fulfilled by providers of information technology products or services.

  - **The revision of the rules governing supervisory activities and the administrative sanctioning process within the ANPD**, in order to update these rules, originally designed considering only the particularities of privacy and data area, to reflect ANPD's new responsibilities involving the protection of minors and specific parameters established by the ECA Digital; and

  - **The proposal of a regulatory solution based on requirements for the use of age verification mechanisms**, considering business models, risks to children and adolescents, and safeguards for personal data processing, based on regulation to be issued by the Executive Branch.

- On December 23, 2025, ANPD published its Priority Topics Map for the 2026–2027 biennium. Among other provisions, the Map establishes that ANPD must:

  - Conduct, **in the first half of 2026**, monitoring activities regarding **compliance of in-scope providers with the ECA Digital**;

  - Conduct, **in the first half of 2027**, 15 supervisory activities to **verify the adoption, by in-scope providers, of the most protective configuration available, by design and by default, regarding minors' privacy and personal data protection, including parental supervision tools**;

  - Conduct, **in the first half of 2027**, 15 supervisory activities to **verify the adoption, by in-scope providers, of measures to prevent children and adolescents from accessing content that is inappropriate, unsuitable, or prohibited by law, including age verification mechanisms**.

Sanctions

Non-compliance with legal obligations established in the ECA Digital may result in the application of the following sanctions (the last two require a court order):

i. warning, with a deadline of up to thirty (30) days for the adoption of corrective measures;

ii. a simple fine, of **up to 10% of the revenue** of the economic group in Brazil or, in the absence of revenue, a fine from R$ 10.00 (ten reais) to R$ 1,000.00 (one thousand reais) per registered user, limited, in total, to **R$ 50,000,000.00** (fifty million reais) per violation;

iii. temporary suspension of activities; or

iv. permanent ban.

Decentralized enforcement

In addition to the ANPD's oversight, enforcement of the ECA Digital will also involve other actors operating concurrently and in a decentralized manner. The main stakeholders are:

- **Public Prosecutors' Offices:** although not a regulator per se, Public Prosecutors' Offices are key enforcers of collective rights. They can launch investigations that may evolve into civil class actions before the Judiciary. As a result of these lawsuits, infringing companies may face severe penalties, ranging from paying damages to product modification or prohibition of the product or activity.

- **Consumer Protection Agencies (SENACON and PROCONs):** SENACON is the consumer protection agency at federal level, while PROCONs operate at the state and municipal levels. These agencies are empowered to enforce consumer rights by handling complaints, conducting inspections, and ensuring compliance with consumer protection laws. They play a crucial role in safeguarding consumer interests across various sectors, including in the digital environment. They can impose fines based on consumer regulation and submit recommendations for other authorities requesting measures.

- **National Council for the Rights of Children and Adole scents ("CONANDA"):** CONANDA is a national deliberative body responsible for formulating policies and guidelines to protect the rights of children and adolescents in Brazil. In the context of digital platforms, CONANDA works to ensure compliance with laws protecting minors from harmful content, exploitation, and other online risks. Upon detecting any irregularity or non-compliance, CONANDA can submit recommendations for other authorities requesting measures.

- **Users:** users also play an active role in enforcement by reporting violations, filing complaints with PROCONs or Public Prosecutors' Offices, and/or filing individual or collective lawsuits requesting that service providers take certain measures or be held liable for damages.

07 PENDING REGULATION

Although the ECA Digital introduces several new obligations, it still leaves significant gaps that will require future regulation. The Statute expressly anticipates further complementary rules to address critical issues, including:

- The measures that in-scope providers must adopt to prevent and mitigate risks related to access, exposure, recommendation, or facilitation of contact with content that violates the rights of children and adolescents;
- The minimum transparency, security, and interoperability requirements for age verification and parental supervision mechanisms to be implemented by operating systems and app stores;
- The guidelines and minimum standards for parental supervision mechanisms to be observed by in-scope providers;
- The proceedings to be adopted by social media platforms for suspending accounts when there are reasonable indications that they are operated by a minor in violation of minimum age requirements established by law, as well as mechanisms to allow legal guardians to appeal and prove age through appropriate means;
- The submission of reports by in-scope providers to competent authorities when identifying violations of children's and adolescents' rights, including content related to exploitation, sexual abuse, kidnapping, and grooming; and
- The criteria for providers of internet applications to enable access to data required for research on the impacts of their products and services on the rights and best interests of children and adolescents, by academic, scientific, technological, innovation, or journalistic institutions.

Rio de Janeiro • Sao Paulo • Brasilia • Curitiba • Tokyo
www.lickslegal.com | info@lickslegal.com