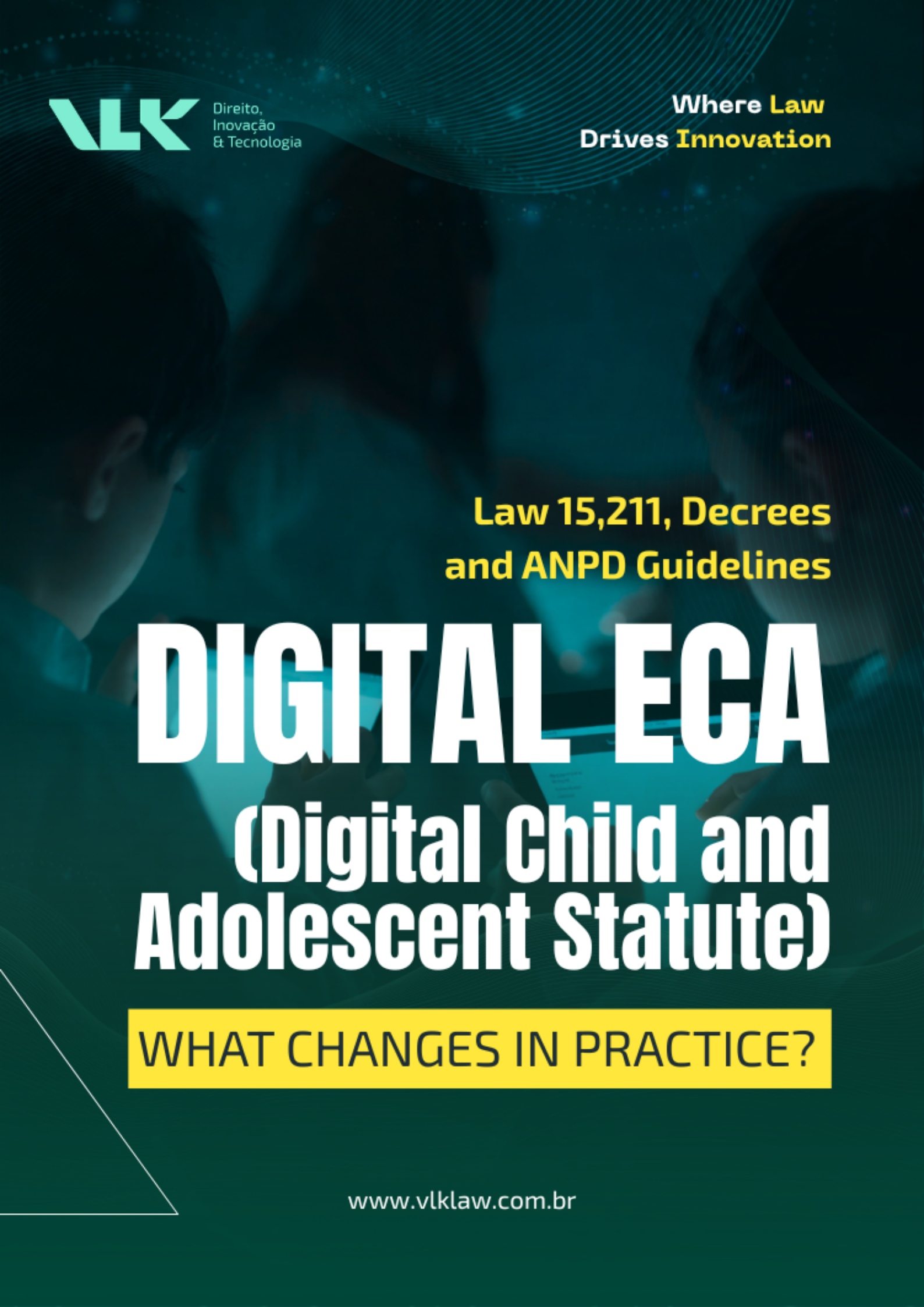

Direito,
Inovação
& Tecnologia

Where Law
Drives Innovation

Law 15,211, Decrees
and ANPD Guidelines

DIGITAL ECA
(Digital Child and Adolescent Statute)

WHAT CHANGES IN PRACTICE?

www.vlklaw.com.br

March 2026

Digital ECA (Law 15,211/2025) and Decrees
What changes in practice?

In September, we published an eBook dedicated to analyzing Law No. 15,211/2025 (Digital child and adolescent statute - Digital ECA), focusing on its main principles and initial regulatory impacts (available in Portuguese here).

With the law's entry into force on March 17, followed by the publication of Decree 12,880/2026 on March 18, issued by the Ministry of Justice (MoJ), and the ANPD's (Brazilian Data Protection Authority) release on March 20 of guidelines and an implementation timeline for reliable age verification mechanisms, **we have updated this material** to reflect the regulatory stage that has effectively been reached.

The regulatory environment of the Digital ECA, therefore, has already entered a phase of progressive regulatory implementation. It is no longer merely a law with pending regulations: today, legal provisions, the regulatory decree, preliminary ANPD guidelines with significant institutional weight for monitoring purposes, and a regulatory agenda anticipating new legislative and enforcement measures coexist in a coordinated manner.

The Brazilian model is not limited to an abstract prohibition on children and adolescents accessing digital environments. The regulatory logic adopted is more sophisticated: it is based on a risk-based approach, guided by the best interests of the child and adolescent, and seeks to impose duties of prevention, protection, information, governance, secure design, parental supervision, and age appropriateness that are compatible with the nature, functionality, and risk of each product or service.

At the same time, the new regime does not permit simplistic interpretations. Not every obligation can be resolved with a single technical measure, and age verification, in particular, should not be understood as authorization for excessive data collection, mass surveillance, or the adoption of invasive and disproportionate solutions. The ANPD's preliminary guidelines frame the issue around requirements of proportionality, accuracy, privacy, inclusion, transparency, auditability, and interoperability.

The central question shifts from "whether there will be regulation" to "how to implement, document, and defend—before regulators, consumers, partners, and authorities - a compliance architecture that is technically defensible and proportionate to the risk." It is from this perspective that this eBook should be read: as a tool for regulatory interpretation, risk prioritization, and preparation for compliance.

We hope you enjoy reading it!

Table of Contents

TIMELINE

09/17/2025

- • Publication of Law No. 15,211/2025 (available in Portuguese here) - Digital ECA.

09/18/2025

- Publication of Provisional Measure No. 1,317/2025 (available in Portuguese here), to transform the Authority into the National Data Protection Agency.
- Publication of Decree No. 12,622/2025 (available in Portuguese here), to regulate the Digital ECA and designate the ANPD as the autonomous authority for the protection of children and adolescents in digital environments. The Decree also establishes responsibilities for compliance with court orders for blocking content, assigned to the Brazilian Internet Steering Committee (CGI.br) and Anatel.

02/25/2026

- Conversion of Provisional Measure No. 1,317/2025 into Law No. 15,352/2026 (available in Portuguese here), definitively transforming the ANPD into a regulatory agency.

03/17/2026

- Entry into force of the Digital ECA.

03/18/2026

- Publication of Decree No. 12,880/2026 (available in Portuguese here), to regulate the Digital ECA and establish the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment.
- Publication of Decrees No. 12,881/2026 (available in Portuguese here) and No. 12,882/2026 (available in Portuguese here), which approve a new organizational structure, with changes to commissioned positions and positions of trust within the ANPD and the MJSP, respectively, entering into force 21 days after publication.

03/20/2026

- Publication of ANPD Board Decision Order No. 35/2026 (available in Portuguese here): the ANPD Board approves a timeline defining implementation stages for age verification solutions.
- Publication of ANPD Board Decision Order No. 36/2026 (available in Portuguese here): approves preliminary guidance on age verification for the protection of children and adolescents in the digital environment (available in Portuguese here).

From March/2026

- Publication of preliminary guidelines for the adoption of reliable age verification mechanisms (available in Portuguese here).
- Creation of a dedicated webpage for clarifications regarding the Digital ECA.
- Monitoring of the implementation of age verification solutions, with specific oversight of app stores and operating systems.

From April/2026

- Public consultation (Request for Contributions) for the development of the Guide: "Providers of Information Technology Products or Services: Scope and General Obligations under the Digital ECA.

04/08/2026

- Entry into force of the two decrees that modify the structure of the ANPD and the MJSP.

04/17/2026

- Mandatory inclusion of warning messages on packaging of devices with internet access specifically targeted at children and adolescents.

06/16/2026

- Judicial authorization will become mandatory for monetized or boosted content that routinely exploits the image or daily life of children and adolescents, with an obligation for immediate removal in the absence of such authorization by IT product or service providers.

From August/2026

- Publication of guidance and regulatory parameters on age verification mechanisms, as well as disclosure of monitoring priorities developed to date.

From November/2026

- Adaptation period and monitoring of the implementation of age verification solutions.

From November/2026

- Update of Inspection Regulations and Administrative Sanctions Enforcement.

From January/2027

- Enforcement actions, as provided in the Priority Topics Map for the 2026–2027 biennium (available in Portuguese here).

This multifactor and cumulative approach is relevant and grounded in the linguistic and systematic interpretation of the law. It serves as a proportionality safeguard, ensuring that stricter obligations apply only to services that effectively expose children to significant risks.

1) TO WHOM IT APPLIES

To all information technology products or services directed at children and adolescents in the country or likely to be accessed by them, considering:

- Sufficient likelihood of use and appeal;
- Ease of access and use; and
- A significant degree of risk to privacy, security, or biopsychosocial development, especially in the case of those intended to enable social interaction and large-scale information sharing among users in a digital environment.

This multifactorial and cumulative approach is relevant and is grounded in the linguistic and systematic foundations of the law. It serves as a safeguard of proportionality, ensuring that strict obligations apply only to services that actually expose children to significant risks.

2) WHAT IS CONSIDERED AN IT PRODUCT OR SERVICE

- A product or service provided remotely, by electronic means, and supplied upon individual request, such as internet applications, computer programs, software, terminal operating systems, internet app stores, and electronic games or similar products connected to the internet or another communications network.

3) WHAT ARE THE GENERAL OBLIGATIONS FOR IT PRODUCTS AND SERVICES

- Ensure the priority protection of children and adolescents;
- Use their best interests as the guiding principle (protection of their privacy, safety, mental and physical health, access to information, freedom to participate in society, meaningful access to digital technologies, and well-being);
- Include adequate and proportionate measures for privacy, data protection, and security, taking into account the individual's autonomy and progressive development;
- Have mechanisms that enable families and legal guardians to prevent inappropriate access and use by children and adolescents;
- Provide information about the risks and the security measures adopted;
- Provide information so that the child or adolescent and their guardians can make informed choices regarding the possible adoption of less protective settings;
- Refrain from processing the personal data of children and adolescents in a manner that causes, facilitates, or contributes to the violation of their privacy or any other rights guaranteed to them;

- Evaluate content made available to children and adolescents according to their age group, ensuring it is compatible with the respective age rating, and fully inform all users of the recommended age group at the time of access;

- Develop, from the design stage, and adopt by default settings that prevent the compulsive use of products or services;

- Provide mechanisms for reporting violations of the rights of children and adolescents;

- Notify the competent authorities to initiate an investigation into violations of the rights of children and adolescents within the scope of their services, when applicable;

- Free and informed consent from parents or legal guardians for downloading apps.

What changes with the Decree?

- Specific mechanisms must be implemented to prevent excessive, problematic, or compulsive use: hiding natural stopping points, triggering new content without a user's request, offering rewards for time spent using the product, and excessive notifications.

- The concept of manipulative, deceptive, or coercive practices encompasses any design mechanisms (choice architectures, interaction flows, or features) in digital products that unduly manipulate or influence user decisions by exploiting their vulnerabilities, particularly those related to age or cognitive ability.

- The examples cited in the Decree involve actions that create artificial barriers to prevent users from doing something or changing their decisions; that involve the use of psychological techniques (such as emotional pressure or false urgency) to induce children and adolescents to make decisions that are not in their best interest; and that hinder access to basic user rights.

- The terms of use must provide, in Portuguese and in an accessible manner, the age rating assigned to video games and digital applications.

- They must provide mechanisms for reporting violations of the rights of children and adolescents that are accessible, free, effective, and widely publicized to users.

- They must immediately remove content that violates the rights of children and adolescents, without requiring a court order, whenever the report comes from qualified sources (such as the victim themselves, the Public Prosecutor's Office, the police, or recognized entities), ensuring a rapid and prioritized response.

- They must report to the National Notification Screening Center violations involving sexual exploitation, kidnapping, false imprisonment, or the identification of imminent or ongoing risk of serious injury or death to children and adolescents.

- They must give priority treatment and immediately remove, without a court order, any content that violates the rights of children and adolescents.

When read systematically, these obligations should not be treated as a fragmented list of isolated commands, but as foundational duties of product or service governance. For larger economic actors, this means that priority protection, best interests, safety, privacy, information, protective design, and mechanisms for responding to violations must be reflected in product architecture, decision-making processes, internal documentation, risk management, and regulatory accountability. The Decree reinforces this interpretation by strengthening prevention duties, curbing manipulative practices, and requiring proportional measures from the design phase onward and by default.

4) ACCESS RESTRICTION MEASURES, COMMUNICATIONS, AND PREVENTIVE POLICIES

All IT products or services must:

- Adopt reasonable measures to prevent and mitigate risks of access, exposure, recommendation, or facilitation of contact with the following content, products, or practices, from the design phase and throughout the operation of their applications:

  I – sexual exploitation and abuse;
  II – physical violence, systematic online bullying, and harassment;
  III – inducing, inciting, instigating, or aiding practices or behaviors that lead to physical or mental health harm, the use of substances causing chemical or psychological dependence, self-diagnosis and self-medication, self-harm, and suicide;
  IV – promotion and marketing of games of chance, fixed-odds betting, lotteries, tobacco products, alcoholic beverages, narcotics, or products prohibited from being sold to children and adolescents;
  V – predatory, unfair, or deceptive advertising practices, or other practices known to cause financial harm to children and adolescents; and
  VI – pornographic content.

- Remove and report to the competent national and international authorities any content involving apparent exploitation, sexual abuse, kidnapping, or grooming detected in their products or services, whether directly or indirectly;

- Remove content that violates the rights of children and adolescents as soon as they are notified of the offensive nature of the publication by the victim, their representatives, the Public Prosecutor's Office, or entities representing the defense of children's and adolescents' rights, regardless of a court order.

  - The notification must contain, under penalty of nullity, elements that allow for the specific identification of the content identified as violating, and anonymous reports are prohibited;
  - They must respect the right to challenge the decision, ensuring the user the right to a fair hearing and a full defense;
  - Make the mechanism through which the notification must be submitted by the notifier public and easily accessible;

  - Journalistic content and content subject to editorial control shall not be subject to the removal procedure.

- Develop policies to prevent systematic online intimidation and other forms of harassment, with adequate support mechanisms for victims, as well as educational awareness programs targeting children, adolescents, parents, educators, employees, and support staff regarding the risks and methods of preventing and addressing these practices.

What changes with the Decree?

Access restrictions:

- Children and adolescents must access digital products, services, and experiences appropriate for their age group, in accordance with the Content Rating Policy issued by the Ministry of Justice and Public Security (MoJ).

- The availability of content, products, or services that are inappropriate or unsuitable for children and adolescents is subject to the following **cumulative** requirements:
  - Compliance with the Content Rating Policy, where applicable;
  - Adoption of technical and organizational security measures by design and by default that are proportionate to the risks for each age group; and
  - Provision of effective parental supervision tools, with blocking features configurable by the legal guardian and other applicable methods.

Note: The Decree preserves room for complementary action by the ANPD, which may determine additional measures whenever it identifies risks relevant to the privacy, security, or development of children and adolescents.

Preventive Policies

- Establishment of the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment ("Policy").
- The ANPD will regulate the minimum default security requirements to curb manipulative, deceptive, or coercive practices in information technology products or services aimed at children and adolescents. The Decree stipulates that, among others, the following practices are covered by this concept:
  - Actions that impede or hinder the user's decision-making process, such as canceling services and modifying preferences;
  - Exploitation of cognitive vulnerabilities;
  - Actions that prevent the exercise of data subject rights, revocation of permissions, parental supervision, and others.

5) DIGITAL EVIDENCE AND REPORTS

- Reports notifying of content involving exploitation, sexual abuse, kidnapping, and grooming of children and adolescents must be sent to the competent authority;

- Providers of IT products or services must retain for 6 months (Art. 15 of the MCI) the following data associated with reports of exploitative content and sexual abuse of children or adolescents:
- Content generated, uploaded, or shared by any user and metadata related to such content; and
- Data of the user responsible for the content and metadata related to it.

What changes with the Decree?

- Reports prepared by providers of internet applications with more than 1 million users, aimed at children and adolescents or likely to be accessed by them, must contain:
    - the number of notifications received; and
    - proportional data on the follow-up given to the notifications received

- The Federal Police is the competent authority for the centralized receipt, processing, screening, and management of reports notifying of content with indications of cybercrimes involving apparent exploitation, sexual abuse, kidnapping, and grooming of children and adolescents.

- The National Notification Screening Center has been established under the Federal Policy to receive these notifications.
- Consequently, it is necessary to review incident response workflows; the chain of custody for information; log governance; and criteria for interaction with authorities.

6) AGE VERIFICATION MECHANISMS

- IT products and services must:
    - Adopt reliable age verification mechanisms each time a user accesses content, a product, or a service whose provision or access is inappropriate, unsuitable, or prohibited for minors under 18 years of age, with self-declaration being prohibited;
    - Mechanisms to provide age-appropriate experiences;

- Public authorities may act as regulators, certifiers, or promoters of technical age verification solutions;

- Internet app stores and terminal operating systems must:
    - Take proportionate, auditable, and technically secure measures to verify age;
    - Allow parents or legal guardians to configure parental supervision mechanisms; and
    - Enable, through an Application Programming Interface (API), the provision of age verification data to internet application providers to ensure compliance with the law.

- There will be regulations establishing minimum requirements for transparency, security, and interoperability for age verification and parental supervision mechanisms.

- Other relevant points:
    - Prohibition of use for other purposes;

- Social media platforms may require account holders with reasonable grounds to believe the account is operated by children or adolescents to confirm their identity, including through supplementary verification methods.

What changes with the Decree and the ANPD Guidelines?

- Definition of the following concepts:
  - age assurance: **a general term** referring to procedures designed to verify, estimate, or infer, directly or indirectly, the age or age group of a user, through a set of methods, technologies, and processes, including document analysis, biometrics, and usage patterns, and other technically suitable means.
  - age verification: a **specific age assessment procedure** with a high degree of reliability, as established by the ANPD, based on verifying the accuracy of the age attribute, with the purpose of confirming the accuracy of the declared age or age group through the use of technical or documentary mechanisms
  - self-declaration of age: a method limited to the indication of age, age group, or other personal data provided by the user themselves, without **additional evidence** to confirm the veracity or ownership of the information
- It defines characteristics that age verification techniques must have, such as proportionality between the solution adopted and the associated risk level, prohibition of traceability of identity and access history, requests, and verifications performed by citizens, interoperability between public and private systems and solutions, and others.
- It defines characteristics that age verification techniques must have, such as proportionality between the solution adopted and the associated risk level, prohibition of traceability of identity and access history, requests, and verifications performed by citizens, interoperability between public and private systems and solutions, and others.
- App stores must provide an appropriate channel to allow for the challenge and correction of a specific user's age classification, provided that additional evidence is submitted and a reasoned decision is issued within a reasonable timeframe.
- The Decree makes it clear that the receipt of age signals does not exempt providers of information technology products or services from the responsibility of ensuring the effectiveness of age appropriateness and the protective measures adopted.
- Providers that facilitate or offer the purchase and sale of products and services prohibited for children and adolescents must implement age verification mechanisms during user registration or at the time of purchasing products and services, in order to prevent children and adolescents from completing the transaction.
- They are not required to adopt user age verification mechanisms if they offer age-appropriate children's profiles and parental supervision mechanisms compatible with the age group, service providers with editorial control, copyright-protected content previously licensed by a responsible economic agent who is not to be confused with the end user, and musical or literary content.

Note: The Decree provides that the ANPD will further regulate the matter, with minimum requirements for transparency, security, and interoperability. Furthermore, for corporate groups with

multiple products, significant user bases, or integrated ecosystems, age verification compliance should not be treated as an isolated project, as it will require, at a minimum:

- an inventory of risk areas and scenarios of likely access by children and adolescents;
- definition of internal criteria for selecting mechanisms by service category;
- documentation of proportionality, legal bases, and safeguards;
- governance over data used in the verification process;
- a trail of appeal and review; and
- readiness for monitoring and future oversight by the ANPD

7) PARENTAL RESPONSIBILITY AND CONTROL

- Providers of IT products and services must:
    - Provide settings and tools that support parental supervision, taking into account available technology and the nature and purpose of the product or service;
    - Provide information to parents or legal guardians about existing parental supervision tools and display a notice when they are in effect and regarding which settings or controls have been applied; and
    - Offer features that allow for limiting and monitoring the time spent using the product or service.
- The default settings for parental supervision tools must adopt the highest level of protection available, with:
    - Restrictions on communication with unauthorized users;
    - Limiting features designed to artificially increase, sustain, or extend the use of the product or service, such as automatic media playback or rewards for usage time;
    - Providing tools to monitor appropriate and healthy use;
    - Use of interfaces that allow for immediate viewing and limitation of usage time;
    - Promotion of digital media literacy regarding safe use; and
    - Resources or connections to emotional support and well-being services.
- The tools must allow parents and legal guardians to:
    - View, configure, and manage the child or adolescent's account and privacy settings;
    - Restrict purchases and financial transactions;
    - Identify the adult profiles with whom the child or teenager communicates;
    - Access metrics on total time spent using the product or service;
    - Enable or disable safeguards through accessible and appropriate controls; and
    - Have information and control options available in Portuguese.
- The provider is prohibited from designing, modifying, or manipulating interfaces with the intent or effect of compromising the user's autonomy, decision-making, or choice, especially if this results in the weakening of parental supervision tools or safeguards.

- Children and adolescents have the right to be educated, guided, and supervised by their parents or legal guardians regarding internet use and their digital experience.

- Parents or legal guardians are responsible for exercising active and continuous care through the use of parental supervision tools appropriate to the age and developmental stage of the child and adolescent.

- The restrictions imposed on IT products and services do not exempt parents and legal guardians, or those who financially benefit from the production or public distribution of any visual representation, from taking action to prevent their exposure to harmful situations.

What changes with the Decree?

- Under the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment, the aim is to seek funding to develop technical solutions for parental supervision, as well as for security and age verification purposes, in addition to guiding families on the need for parental supervision solutions.
- Providers of IT products or services are now responsible for avoiding designs that hinder the use of parental controls or manipulate decisions, and must ensure clear, simple, and effective access to privacy settings, supervision, and the exercise of rights.

8) PROTECTION OF PERSONAL DATA

- Controllers of children's and adolescents' personal data, especially when processed for purposes other than those strictly necessary for the operation of the product or service, must assess the risks and make efforts to mitigate them, and prepare an impact and monitoring report to be shared upon request by the ANPD;

- The use of profiling techniques for targeting commercial advertising is prohibited, as is the use of emotional analysis, augmented reality, extended reality, and virtual reality for this purpose;

- The creation of behavioral profiles of child and adolescent users based on the collection and processing of their personal data - including data obtained through age verification processes, as well as group and collective data - for the purpose of targeting commercial advertising is prohibited;

- Control over personalized recommendation systems, including an option to disable them;

- Restrictions on the sharing of geolocation data and the provision of clear advance notice regarding tracking;

- Parents and legal guardians must have the means to view, configure, and manage the account and privacy settings of the child or adolescent;

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

What changes with the Decree?

- Self-declaration, including other personal data provided by the user, is not considered sufficient, requiring the use of additional evidence or mechanisms to validate the accuracy and ownership of the information.
- Providers of IT products or services now have a duty to ensure, from a privacy perspective, that controls such as privacy settings, consent, and revocation of permissions are accessible in a clear, simple, and effective manner, with practices that conceal, fragment, or hinder the exercise of these rights being prohibited, including within the scope of parental supervision.

9) SOCIAL MEDIA

- Definition: an internet application whose primary purpose is the sharing and dissemination of opinions and information on a single platform through interconnected or linked accounts, allowing users to connect with one another;
- They must ensure that users or accounts belonging to children and adolescents up to 16 years of age are linked to the user or account of one of their legal guardians;
- For inappropriate or unsuitable services: inform users that their services are not appropriate; monitor and restrict, to the extent of their technical capabilities, the display of content that is clearly intended to attract children and adolescents; and continuously improve their age verification mechanisms to identify accounts operated by children and adolescents.
- For hybrid services, superapps, or platforms with integrated social layers, the scope for regulatory reassessment by the ANPD regarding the functional classification of the service as a social network remains relevant.

What changes with the Decree?

- Social networks that make available content, products, or services prohibited for children and adolescents, or that engage in advertising related to them, must:
  - Create versions without such content, in which case age verification will not be required; or
  - Adopt effective age verification mechanisms, with self-declaration prohibited.
- Within the scope of its authority, the ANPD may reassess and determine the classification of services as social networks.

10) ARTIFICIAL INTELLIGENCE

- Regular review of artificial intelligence tools, with the participation of experts and competent authorities, based on technical criteria that ensure their safety and suitability for use by children and adolescents, guaranteeing the possibility of disabling features not essential to the basic functioning of the systems;

What changes with the Decree?

- Interactions with systems (including AI) that generate or simulate sexual content are also considered pornographic, which entails specific obligations as indicated in item 12 of this document.

11) ELECTRONIC GAMES

- Loot boxes targeted at children and adolescents or likely to be accessed by them, as determined by age rating, are prohibited;

- Electronic games that include features for user interaction via text, audio, or video messages or content exchange, whether synchronous or asynchronous, must implement measures for content moderation, protection against harmful contacts, and parental control over communication mechanisms;

- By default, limit user interaction features to ensure the consent of parents or legal guardians.

What changes with the Decree?

- The Age Rating for video games must indicate the presence of content that is inappropriate, unsuitable, or prohibited for each age group, as well as risks related to:
    - features that enable interaction with other users;
    - loot boxes, the presence of which is prohibited in video games intended for children and adolescents or likely to be accessed by them;
    - the presence of stimuli that induce excessive engagement;
    - microtransactions;
    - practices that exploit users' vulnerability or cognitive biases; and
    - impacts on the safety and health of children and adolescents.

- Video games with loot boxes must require age verification of users. These games may offer versions without loot boxes or completely disable this feature for children and adolescents.

12) EROTIZATION

- Internet service providers are prohibited from monetizing or promoting content that depicts children and adolescents in an eroticized or sexually suggestive manner or in a context typical of the adult sexual sphere.

What changes with the Decree?

- Any interaction with systems (including automated or AI-based systems) that involves the creation, exchange, or simulation of sexually explicit content, nudity with sexual connotations, or material of an erotic nature is considered pornographic content.

- The definition of pornographic content takes into account the purpose and model of the service, covering content with nudity or explicit sexuality.

- Content with an educational, artistic, informational, or health-related context, as well as books/audiobooks (without images) and audio-only content.
- As a primary obligation, providers of IT products or services that make this type of content available must implement effective age verification, preventing access by children and adolescents, including to previews.

- The ANPD may reclassify content or services as pornographic based on their nature or practical effects.

- Pornographic content must remain hidden by default and may only be accessed upon effective age verification; a simple self-declaration is insufficient

13) TRANSPARENCY REPORT

- Applicable to providers of applications aimed at children and adolescents or likely to be accessed by them that have more than one million registered users in this age group with an internet connection within the national territory.

- They must prepare semi-annual reports, in Portuguese, to be published on their website, including:
    - Channels available for receiving complaints and the systems and processes for investigating them;
    - Number of complaints received;
    - The number of instances of content or account moderation, by type;
    - Measures adopted to identify children's accounts on social media;
    - Technical improvements for the protection of personal data and privacy;
    - Technical improvements to verify parental consent; and
    - Details of the methods used and the presentation of the results of impact assessments, identification, and management of risks to the safety and health of children and adolescents.

- Provide, free of charge, access to data necessary for conducting research on the impacts of their products and services on the rights of children and adolescents and on their best interests, prohibiting the use of such data for any commercial purposes and ensuring compliance with the principles of purpose, necessity, security, and confidentiality of information.

What changes with the Decree?

- The disclosure of a summary version of the impact reports in clear and accessible language is mandatory.

- The ANPD may regulate the reports, defining minimum content, frequency, and rules for preparation, review, and sharing.

- Data from the reports may be shared with qualified institutions for public interest research purposes, provided they meet technical and governance criteria and have no commercial purpose.

- It is also the ANPD's responsibility to accredit these institutions through a public notice, requiring criteria such as research for the public interest, technical qualifications of the team, submission of a research plan, absence of commercial purposes, and adoption of governance and information security measures.

14) REGULATORY ASYMMETRY

- The ANPD may issue recommendations and guidelines regarding the relevant practices provided for in the Law, taking into account regulatory asymmetries, the functionalities and risk level of each product or service, as well as technological developments and applicable technical standards;

- Adopt a responsive approach, ensuring differentiated and proportionate treatment for services of distinct nature, risk, and business model.

What changes with the Decree?

- A risk-based regulatory approach is adopted, in which obligations now vary according to the level of risk to children and adolescents, meaning that the concrete application of the Digital ECA's obligations is unlikely to be uniform for all stakeholders.

- The ANPD has regulatory authority to define technical criteria (e.g., age verification, classification, categorization of services), which reduces divergent interpretations and asymmetries across sectors.

15) ENFORCEMENT AND SANCTIONS

- Provisional Measure (MP No. 1,317/25) (available in Portuguese here) transformed the Brazilian Data Protection Authority (ANPD) into a regulatory agency with new powers for monitoring, enforcement, and sanctioning under the Digital ECA;

- The MP increases the ANPD's budget and establishes an administrative structure, including a specific career path for senior-level analysts with new positions;

- Without prejudice to other civil, criminal, or administrative sanctions, the penalties are:
    - Warning, with a deadline of up to 30 (thirty) days to implement corrective measures;
    - A simple fine of up to 10% of the economic group's revenue in Brazil for its most recent fiscal year or, in the absence of revenue, a fine ranging from R$ 10.00 (ten reais) to R$ 1,000.00 (one thousand reais) per registered user of the sanctioned provider, limited, in total, to R$ 50,000,000.00 (fifty million reais) per violation;

  - Temporary suspension of activities; and
  - Prohibition on conducting business activities.

- In the case of a foreign company, its subsidiary, branch, office, or establishment located in the country shall be jointly and severally liable for payment of the fine.

- Decree No 12,622/2025 (available in Portuguese here) regulates the law and assigns to Anatel (Brazilian National Telecommunications Agency) the responsibility for receiving and distributing blocking orders to telecommunications service providers.

- The Decree grants Brazilian Internet Steering Committee (CGI.br) and Anatel the authority to define the most appropriate techniques for complying with blocking orders.

What changes with the Decrees?

- The Brazilian Data Protection Authority now officially plays a central and more structured role in regulation and oversight, with institutional reinforcement resulting from the new regulatory framework (Decree No. 12,881/2026), expanding its operational and technical capacity to supervise compliance with the rules.

- There is a consolidation of joint action between the ANPD, the Ministry of Justice, and other agencies, such as the Federal Police, through the National Notification Screening Center.

16) LABELS ON ELECTRONIC DEVICES

What changes with the Decrees?

- It creates the obligation to include, within 30 days of publication, a specific warning message on the packaging of internet-enabled electronic devices intended for children and adolescents, with the text “This product allows access to the internet. Internet content may pose risks to children and adolescents. Use of this product requires parental supervision.” This does not apply to products already manufactured or imported prior to the date of publication

- The requirement for the warning on packaging applies only to products whose presentation or marketing is **exclusively** directed at children and adolescents and does not apply to products for general use or with a mixed audience.

- The ANPD may issue future regulations regarding how these warnings must be presented (form, content, and deadlines) and may replace or elaborate on this initial model.

17) ARTISTIC ACTIVITIES ARTÍSTICAS

What changes with the Decrees?

- Judicial authorization is now required for content that habitually exploits the image or daily life of children and adolescents when there is monetization or promotion.

- A direct obligation is created for platforms and providers to verify this authorization and immediately remove the content if it does not exist.

- The rule applies only to content whose monetization or promotion occurs 90 days or more after the Decree's publication.

- The dissemination, monetization, or promotion of content that exposes children and adolescents to abusive, humiliating, or degrading situations is expressly prohibited.

18) NATIONAL POLICY FOR THE PROMOTION AND PROTECTION OF THE RIGHTS OF CHILDREN AND ADOLESCENTS IN THE DIGITAL ENVIRONMENT

What changes with the Decrees?

- The Decree establishes the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment, which seeks to promote intersectoral coordination, with mandatory coordination among different agencies and levels of government to ensure integrated and ongoing action.

- It introduces mechanisms such as a three-year plan, guidelines, and integration with other public policies (digital education, combating violence, among others).

- The policy now prioritizes measures from the product design stage (by design), such as safety, age verification, and parental supervision. It also includes digital education, the promotion of research, innovation, and the active participation of children and adolescents in decision-making.

19) NATIONAL CENTER FOR NOTIFICATION TRIAGE

What changes with the Decrees?

- The Decree authorizes the creation of the National Notification Screening Center, designed to centralize the receipt, validation, and handling of reports regarding serious violations against children and adolescents in the digital environment.

- The Federal Police will now be the authority responsible for screening, analyzing, and forwarding notifications to the competent authorities.

- Providers of IT products or services are now required to report certain types of content and serious misconduct (e.g., sexual abuse, grooming) through established reporting channels.

- IT product or service providers that already submit the same notifications to overseas reporting centers, which are accessible to Brazilian authorities, do not need to resubmit them to the Center.

- The Center's operations will be detailed by a Ministry of Justice and Public Security (MJSP) regulation, including internal protocols, communication workflows, coordination with authorities, and a protection system, as well as requirements and deadlines for handling notifications.

20) REGULATION

- Article 37 of the Digital ECA originally allows the Executive Branch (via decrees and acts of the ANPD) to specify how the law will be applied in practice. The article establishes an explicit limit: the regulations cannot result in mass, generic, or indiscriminate surveillance, and prohibits measures that compromise: freedom of expression; privacy; protection of personal data of children and adolescents; and the principle of comprehensive protection.

What changes with the Decrees?

- The Decree implements the regulations provided for in Article 37 of the Digital ECA, detailing technical and operational obligations (such as age verification, secure design, reporting, and governance), incorporating safeguards and a risk-based approach.

21) VACATIO LEGIS

- Six months (a reduction from the initially envisaged one-year period.

What changes with the Decrees?

- The Digital ECA has been in effect since March 17, 2026, and its regulatory Decree has been in effect since March 18, 2026. The following obligations have specific effective dates:
    - April 17, 2026: Obligation to include a warning on the packaging of internet-enabled products intended exclusively for children and adolescents.
    - June 16, 2026: Obligation to require judicial authorization for monetized content featuring recurring appearances by children and adolescents, with immediate removal if such authorization is absent.

- The two decrees amending the structures of the ANPD and the MJSP take effect on April 8, 2026, 21 days after publication.

- As announced by the ANPD, MJSP, and the Presidential Communications Secretariat (available in Portuguese here), the adaptation will be gradual and guided by the ANPD, which will define guidelines and best practices without necessarily imposing a single age verification solution, but requiring technical adjustments based on risk and sector.

Read the full text of the regulations here:

- Digital ECA (**here**)
- Decree No. 12,880/2026 (**here**)
- Decree No.12,881/2026 (**available in Portuguese here**)
- Decree No. 12,882/2026 (**available in Portuguese here**)
- CD/ANPD Decision No. 35/2026 (**available in Portuguese here**)
- CD/ANPD Decision No. 36/2026 (**availabe in Portuguese here**)

Sincerely,

VLK Law