VLK Direito, Inovação & Tecnologia

(Law 15.211/2025)

DIGITAL ECA

WHAT CHANGES IN PRACTICE?

www.vlklaw.com.br

TABLE OF CONTENTS

September 2025

Digital ECA (Law 15.211/2025)
What changes in practice?

1) TO WHOM IT APPLIES

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

- Sufficient probability of use and attractiveness;
- Ease of access and use; and
- 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.

2) WHAT IS CONSIDERED AN IT PRODUCT OR SERVICE

- A product or service provided remotely, electronically, and supplied upon individual request, such as internet applications, computer programs, software, terminal operating systems, internet application stores, and electronic games or similar items 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 as a guiding principle the best interests of the child and the adolescent (protection of their privacy, security, mental and physical health, access to information, freedom to participate in society, meaningful access to digital technologies, and well-being);

- Implement 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 on risks and the security measures adopted;

- Provide information so that children or adolescents 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 way that causes, facilitates, or contributes to the violation of their privacy or any other rights guaranteed to them;

- Assess the content made available to children and adolescents according to their age group, ensuring compatibility with the corresponding age rating, and extensively inform all users of the recommended age group at the time of access;

- Design from the outset and adopt by default configurations that prevent the compulsive use of products or services;

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

- Notify the competent authorities for the initiation of investigations into violations of the rights of children and adolescents within the scope of their services, when applicable;

- Obtain the free and informed consent of parents or legal guardians for the download of applications.

4) ACCESS RESTRICTION MEASURES, COMMUNICATIONS, AND PREVENTIVE POLICIES

All IT products or services shall:

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

  I – sexual exploitation and abuse;
  II – physical violence, cyberbullying, and harassment;
  III – inducement, incitement, instigation, or assistance in practices or behaviors leading to harm to physical or mental health, use of substances causing chemical or psychological dependence, self-diagnosis and self-medication, self-harm, and suicide;
  IV – promotion and commercialization of gambling, fixed-odds betting, lotteries, tobacco products, alcoholic beverages, narcotics, or products prohibited for sale to children and adolescents;
  V – predatory, unfair, or misleading 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 apparent content of exploitation, sexual abuse, kidnapping, and grooming detected in their products or services, 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 representative entities for the defense of children's and adolescents' rights, regardless of a court order.

    - The notification must include, under penalty of nullity, elements that allow the specific identification of the reported content, and anonymous complaints are prohibited;
    - They must respect the right to contest the decision, ensuring the user's right to adversarial proceedings and full defense;
    - Make public and easily accessible the mechanism through which the notification must be submitted by the notifier;
    - Journalistic content and content subject to editorial control shall not be subject to takedown procedures.

- Develop policies for the prevention of cyberbullying and other forms of harassment, with appropriate support mechanisms for victims, as well as educational awareness programs directed at children, adolescents, parents, educators, employees, and support staff regarding the risks, prevention, and response to such practices.

5) DIGITAL EVIDENCE AND REPORTS

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

- IT product or service providers must retain the following data associated with reports of content involving the exploitation and sexual abuse of children or adolescents for six months (Article 15 of the Brazilian Civil Rights Framework for the Internet):

    - Content generated, uploaded, or shared by any user and metadata related to such content; and
    - Data on the user responsible for the content and metadata related to it.

6) AGE VERIFICATION MECHANISMS

- IT products and services must:

    - Adopt reliable age verification mechanisms each time a user accesses content, products, or services that are inappropriate, unsuitable, or prohibited for minors under the age of 18, 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 application 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 signals to internet application providers for compliance with the Law;

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

- Other relevant points:

  - Prohibition of use for other purposes;
  - Social networks may require those responsible for accounts with reasonable evidence of being operated by children and adolescents to confirm their identity, including through complementary verification methods.

7) PARENTAL RESPONSIBILITY AND CONTROL

- IT product and service providers should:

  - Provide settings and tools that support parental supervision, considering the available technology and the nature and purpose of the product or service;
  - Provide information to parents or legal guardians about existing tools for parental supervision and display a warning when they are in effect and about which settings or controls have been applied; and
  - Offer features that allow limiting and monitoring the time of use of the product or service.

- Default settings for parental supervision tools should adopt the highest level of protection available, with:

  - Restriction on communication with unauthorized users;
  - Limitation of features to artificially increase, sustain, or extend the use of the product or service, such as automatic media playback and rewards for time spent using the product;
  - Provision of tools to monitor appropriate and healthy use;

  - Use of interfaces that allow immediate visualization and limitation of usage time;
  - Promotion of digital media education on safe use; and
  - Resources or connections to emotional support and well-being services.

- The tools should enable 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 profiles of adults with whom the child or adolescent communicates;
  - Access metrics on the total time spent using the product or service;
  - Enable or disable safeguards through accessible and appropriate controls; and
  - Have access to information and control options in Portuguese.

- The supplier is prohibited from designing, modifying, or manipulating interfaces with the purpose or effect of compromising the user's autonomy, decision-making, or choice, especially if it results in the weakening of parental supervision tools or safeguards.

- Children and adolescents have the right to be educated, guided, and monitored by their parents or legal guardians regarding their use of the internet 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 stage of development of the child or adolescent.

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

8) PROTECTION OF PERSONAL DATA

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

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

- The creation of behavioral profiles of children and adolescents based on the collection and processing of their personal data, including those obtained in 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 the option to disable them;

- Restriction on the sharing of geolocation and provision of clear prior notice regarding its tracking;

- Parents and legal guardians must have mechanisms to view, configure, and manage the account and privacy options of children and adolescents;

- Social network 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.

9) SOCIAL NETWORKS

- Concept: internet application whose main purpose is to share and disseminate opinions and information on a single platform through connected or accessible accounts, allowing users to connect with each other;

- 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.

10) ARTIFICIAL INTELLIGENCE

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

11) ELETRONIC GAMES

- Loot boxes aimed at children and adolescents or likely to be accessed by them, according to the age rating, are prohibited;

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

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

12) EROTIZATION

- Internet application providers are prohibited from monetizing and promoting content that depicts children and adolescents in an eroticized or sexually suggestive manner or in a context specific to the adult sexual universe.

13) TRANSPARENCY REPORT

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

- They must prepare semi-annual reports, in Portuguese, to be published on their website, with:

    - Channels available for receiving complaints and the investigation systems and processes;
    - Number of complaints received;
    - Amount of content or account moderation, by type;
    - Measures adopted to identify children's accounts on social networks;
    - Technical improvements for the protection of personal data and privacy;
    - Technical improvements to assess 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.

- Enable free access to data necessary to conduct research on the impacts of its products and services on the rights of children and adolescents and in 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.

14) REGULATORY ASYMMETRY

- The ANPD may issue recommendations and guidelines regarding the relevant practices provided for in the Law, considering regulatory asymmetries, the functionalities and

level of risk 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 different nature, risk, and business model.

15) ENFORCEMENT AND SANCTIONS

- Provisional Measure (MP 1.317/25) transformed the National Data Protection Authority (ANPD) into a regulatory agency with new powers to monitor, supervise, and sanction the Digital ECA;

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

- Without prejudice to other civil, criminal, or administrative sanctions, the penalties are:

    - Warning, with a deadline for corrective measures of up to 30 (thirty) days;
    - Simple fine of up to 10% of the economic group's revenue in Brazil in its last fiscal year or, in the absence of revenue, a fine of R$ 10.00 (ten reais) to R$ 1,000.00 (one thousand reais) per registered user of the sanctioned provider, limited to a total of R$ 50,000,000.00 (fifty million reais) per violation;
    - Temporary suspension of activities; and
    - Prohibition from exercising 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 the payment of the fine;

- Decree 12.622/2025 regulates the law and assigns Anatel the task of receiving and distributing blocking orders to telecommunications service providers.

- The Decree assigns to CGI.br and Anatel the possibility of defining the most appropriate techniques for complying with blocking orders.

16) VACATIO LEGIS

- Six months (reduction from the initially planned period of one year).

See the full text of the Law (here).

Sincerely,

VLK Advogados