ANPD

GUIDELINES

Providers of information technology products or services: scope and general obligations under the Digital ECA

NOV / 2026

ANPD

GUIDELINES

Providers of information technology products or services: scope and general obligations under the Digital ECA

Adenice Araújo de Medeiros
Camila Leite Contri
Carlos Fernando do Nascimento
Diego Carvalho Machado
Eduarda Rodrigues de Almeida Porcino
Guilherme Ferreira Machado
Gustavo Gonçalinho da Mota Gomes
Izabella Alves Jorge Bittencourt
Jeferson Dias Barbosa
Lucas Borges de Carvalho
Maria Carolina Ferreira da Silva
Rodrigo Santana dos Santos
Thiago Guimarães Moraes

Brasília, DF
2026

President of the Republic Luiz Inácio Lula da Silva

Minister of Justice and Public Security Wellington César Lima e Silva

National Data Protection Agency

Director-President Waldemar Gonçalves Ortunho Junior

Directors Iagê Zendron Miola
Lorena Giuberti Coutinho
Miriam Wimmer

Drafting Team Adenice Araújo de Medeiros
Camila Leite Contri
Carlos Fernando do Nascimento
Diego Carvalho Machado
Eduarda Rodrigues de Almeida Porcino
Guilherme Ferreira Machado
Gustavo Gonçalinho da Mota Gomes
Izabella Alves Jorge Bittencourt
Jeferson Dias Barbosa
Lucas Borges de Carvalho
Maria Carolina Ferreira da Silva
Rodrigo Santana dos Santos
Thiago Guimarães Moraes

Review team Camila Leite Contri
Lucas Borges de Carvalho

Graphic Design André Scofano Maia Porto

Desktop publishing Júlia Câmara Cunha

Version 1.0

Digital publication (November 2026)

National Data Protection Agency
SCN, Qd. 6, Conj. A
Ed. Venâncio 3.000, Bl. A, 9th floor
Brasília, DF · Brazil · 70716-900
www.gov.br/anpd

Translation The translation was generated using artificial intelligence and overseen by Lucas Borges de Carvalho and Camila Leite Contri. For direct mentions of the Digital ECA, the English translation prepared by the Ministry of Human Rights and Citizenship (MDHC) was used, with minor adaptations.

Disclaimer The Portuguese version of the Guidelines is the official version. In the event of any discrepancy, misstatement, omission or error appearing in the translation, the Portuguese version shall prevail.

Table of Contents

06 **Introduction**

08 **Providers of information technology products or services**
- 12 Information technology product or service
- 15 Social media
- 18 App store
- 21 Operating systems
- 24 Services with editorial control and copyright protected content

29 **Likely access by children and adolescents**
- 35 Likelihood of use and attractiveness
- 36 Ease of access and use
- 38 Significant degree of risk

42 **Duty of prevention**
- 47 Duty of prevention *(Stricto sensu)*
- 51 Duty of protection
- 52 Duty to inform
- 56 Duty of safety

58 **Notes**

60 **Appendix I** – Summary table – Key concepts

65 **Appendix II** – Summary table – Likely access

67 **Appendix III** – Likely access test

Introduction

The purpose of this document is to provide guidance and establish interpretations regarding the key concepts related to the scope of application of Law No. 15,211, dated September 17, 2025, known as the Digital Statute for Children and Adolescents (Digital ECA). More specifically, these Guidelines seek to answer two central questions: (i) to whom does the Digital ECA apply; and (ii) what are the meaning and implications of the duties of prevention, protection, information, and safety ("duty of prevention") for regulated entities.

To address the first question, we will examine the concept of "providers of information technology products or services directed at children and adolescents or likely to be accessed by them" (Articles 1 and 2, I). This definition is essential for determining which market players are subject to compliance with the legal obligations set forth in the Digital ECA. We will also consider the types of providers established in the Law itself, each with specific obligations: "social networks" (Art. 2, III), "online app stores" (Art. 2, VI), "operating systems" (Art. 2, VII), "providers of services with editorial control" (Art. 39, § 1), and "providers of copyrighted content previously licensed by a responsible economic agent who is not to be confused with an end user" (Art. 39, § 1).

Regarding the second question, we will address the concept of the "duty of prevention" (Art. 5), a central element for properly understanding the regulatory model established by the Digital ECA, which is geared toward risk prevention and the comprehensive and priority protection of children and adolescents. Although the focus of these Guidelines is not the analysis of specific obligations set forth in the Law—such as age assurance, parental supervision mechanisms, and content moderation—it is understood that the "duty of prevention" constitutes the central foundation for the interpretation and application of these and other obligations provided for in the Digital ECA.

Thus, by defining the scope of key concepts in the Digital ECA, these Guidelines aims to provide greater predictability and legal certainty in the application of the Law. Therefore, the goal is to transparently provide guidance and guidelines for regulated entities and to establish interpretations and best practices that can assist in the process of implementing the new regulations.

Providers of information technology products or services

The Digital ECA applies to providers of information technology products or services that are intended for, or likely to be accessed by, children or adolescents in Brazil. Providers of these digital products or services are, therefore, the entities subject to compliance with the obligations set forth in the Law. In general, this definition includes **all providers that offer services or sell products in the digital environment**, as long as the requirements regarding being directed or likely to be accessed by children and adolescents are met.

The Digital ECA stipulates that its application **is independent of the "location, development, manufacture, offering, marketing, and operation" of the service or product** (Art. 1). In this regard, the legal provision follows a premise similar to that adopted in the Brazilian Civil Rights Framework for the Internet (MCI) (Law No. 12,965/2014, Art. 11) and in the General Personal Data Protection Law (LGPD) (Law No. 13,709/2018, Art. 3), in the sense that the provider's physical presence in Brazil—and related factors, such as the manufacture of the product in the country—are not required for Brazilian legal norms to apply. Thus, it is sufficient that a given application, such as a video

game or a social media platform, be available on the internet and likely to be accessed by children or adolescents in Brazil for the provisions of the Digital ECA to apply, even if, for example, the provider is a foreign company or is headquartered in another country.

Another relevant aspect is that the Digital ECA adopts a broad legal concept when identifying these regulated entities. This regulatory framework allows **for the inclusion of providers not expressly mentioned**, such as marketplaces, messaging services, connected devices, and similar services, provided they meet the legal criteria.

Therefore, the **central criterion for identification is functional in nature**, so that the concept encompasses both current and future technologies, even if they are not yet available to the public. Thus, the Law chooses to define providers of information technology products or services based on functions and effects, without tying them to specific technologies, formats, or devices, adopting **a technologically neutral approach** in which this concept is guided **by the purpose and impact of the service or product**, rather than by the technique used or the digital solutions employed.

This demonstrates that **the Digital ECA regulates "what must be ensured"**—that is, the protection of children and adolescents in the digital environment—**rather than, strictly speaking, "the technical means of implementing"** such protection. Therefore, technological neutrality in the definition of providers of information technology products or services is preserved, and regulatory gaps arising from continuous innovation are avoided. The Law is particularly concerned with whether the provider operates in **a context that could pose risks to children and adolescents** and whether it adopts adequate prevention and safety measures.

Finally, the Digital ECA adopts a principle of reasonableness and proportionality in its application. Thus, certain legal obligations must be "modulated according to the degree of influence the provider of the product or service has over the content made available, the number of users, and the size of the provider" (Art. 39). Similarly, these obligations must be applied "in a manner proportional to the provider's ability to influence, moderate, or intervene in the availability, circulation, or reach of content accessible to children and adolescents" (Art. 39, § 2).

Furthermore, the regulation and enforcement of the Law by the National Data Protection Agency (ANPD) must be based on a responsive approach, "ensuring differentiated and proportionate treatment for **services of different nature, risk, and business model**" (Art. 34, § 2). This implies applying distinct legal treatment based on the essential characteristics of products and services, as well as their providers, with special consideration given to the risks arising from their impact on children and adolescents. Based on these criteria (nature, risk, and business model), platforms that are strictly educational, professional, or in the public interest may, for example, receive differentiated treatment. Other relevant aspects include whether a particular provider is for-profit or nonprofit, the type of content made available, the design standards adopted, and the presence or absence of targeted advertising.

The analysis in question cannot be conducted in the abstract. It must always be carried out on a case-by-case basis, considering the context and specific characteristics of products, services, and providers, based on the available information and evidence.

Figure 1: Proportionality in the Application of the Digital ECA.

DIFFERENTIATED TREATMENT: PROPORTIONALITY, REGULATORY ASYMMETRY AND A RESPONSIVE APPROACH

The Digital ECA adopts a rationale of reasonableness and proportionality. Legal obligations must be tailored to the provider's context and applied in a manner proportional to the risks, their nature, and the provider's ability to influence the content accessible to children and adolescents (Articles 34 and 39, caput and § 2, of the Digital ECA).

FACTORS FOR ADJUSTMENT

- Nature;
- Risk;
- Business model;
- Degree of interference of the provider of the product or service over the content made available;
- Number of users;
- Size of the provider.

HOW THIS IS REFLECTED IN ITS APPLICATION

Modulated Obligations
The obligations under the Digital ECA are tailored to the provider's specific context, taking into account the factors listed above.

Responsive Approach and Proportional Application
Measures must be proportional to the provider's ability to influence, moderate, or intervene in content's availability, circulation, or reach.

Purpose
To ensure the comprehensive protection of children and adolescents through appropriate, effective, and feasible measures while avoiding unreasonable or disproportionate requirements.

Proportionality does not reduce the provider's responsibility; rather, it guides the form and scope of the expected measures, always with a focus on protecting children and adolescents.

Accordingly, depending on these variables, the obligations set forth in the Digital ECA may apply differently to certain types of products or services and providers, pursuant to Articles 34, § 2, and 39. Such modulation must consider (i) the degree of interference by the provider, (ii) the number of users, and (iii) the provider's size. This analysis must be conducted on a case-by-case basis, taking into account how the provider's products and services operate, the nature of the content, and whether it falls into any of the categories established by law.

In this context, the Law identifies several subcategories of the concept of providers (Art. 2, items I, III, VI, VII, and IX, and Art. 39, § 1), based on the role each entity plays in the digital environment, such as app stores, social networks, and providers of services with editorial control or of copyrighted content previously licensed by a responsible economic agent. These entities have specific obligations set forth in the Law, which are in addition to the general obligations applicable to all providers and help assign responsibilities in the digital environment.

Information technology product or service

The Digital ECA defines an information technology product or service as the "product or service provided remotely, by electronic means, and supplied in response to an individual request" (Art. 2, I). In the same article, the Law lists the following examples of information technology products or services: internet applications, computer programs, software, terminal operating systems, app stores, and electronic games or similar products connected to the internet or another communications network.

The illustrative reference to "internet applications" deserves special mention, as it indicates the central focus and scope of the legal definition. As provided for in the MCI (Art. 5, VII), an internet application is

the "set of functionalities that can be accessed through a terminal connected to the internet"—a definition that encompasses nearly all digital applications, understood as those provided through the storage, processing, or transmission of data over the Internet, thereby distinguishing them from internet connection services, which are typically provided by telecommunications service providers.

Similarly, it should be noted that the terms "product" or "service" refer to the definitions of these terms in the Consumer Defense Code (CDC, Law No. 8,078/1990, Art. 3, §§1 and 2), which are also broad in nature and cover a significant portion of economic activities involving consumer relations.[1] Although these legal definitions may be useful in complementing the interpretation and assisting in the application of the Digital ECA, it should be noted that the Digital ECA has **its own scope and a specific definition** of "information technology product or service," based on **three central elements**:

(i) **remote provision,** without the simultaneous presence of the parties;
(ii) **electronic means,** using equipment and networks for transmission and processing, particularly through internet applications; and
(iii) **individual request,** that is, activation or use of the product or service in response to an individual request from the user, without prejudice to the sharing of its use.

These three elements must necessarily be present for a product or service to be characterized as an information technology product or service, thereby providing a precise definition of which "products" and "services" — or, indeed, "internet applications" — are subject to the provisions of the Digital ECA.

In this regard, the parameters defined in the Digital ECA also help identify situations in which certain activities do not fall within this

framework. Thus, products or services that meet the following criteria are not subject to the scope of the Digital ECA:

(i) **are not provided remotely,** since they involve the simultaneous physical presence of the provider and the recipient, even if electronic tools are used in the service, or the service is provided upon individual request. This category includes, for example, a large portion of commercial activities carried out in brick-and-mortar stores and shopping centers, given that they are provided with the physical presence of the parties involved;

(ii) **are not provided electronically,** such as services whose content is physical or offline, like those provided in brick-and-mortar stores, without any use of applications or terminals connected to the internet. For the purposes of the Digital ECA, services limited to direct contact between the parties by telephone—such as telemarketing—should also not be considered provided electronically, since, in such cases, there is no storage, processing, or transmission of data through digital applications connected to the internet. However, hybrid devices (accessed electronically but with some physical component) are still characterized as being accessed electronically, such as augmented virtual reality devices; or

(iii) **are not provided upon individual request by the user,** as in the case of broadcast transmissions, which are directed at an indeterminate audience without an individual request. It should be noted that the collective, shared, or joint use of a particular information technology product or service does not preclude the characteristic of individual request. It is common for devices to be shared and applications to be subscribed to so that more than one person, including the subscriber, can enjoy their features, such as educational or streaming platforms. In such cases, the Digital ECA remains applicable, as the individual request persists, even if the use is collective.

Finally, it is important to note that the **user's lack of direct payment**, when analyzed in isolation, **does not preclude the application of the Digital ECA's provisions.** This understanding aligns with international experiences and with the well-established interpretation in Brazilian law, namely that **apparent free access does not always negate the economic rationale behind the service offered.** In many cases, the user does not pay in cash for the service or product, or pays only for certain features, but is themselves part of a business model sustained by their data, advertising, or other indirect monetization mechanisms.

Thus, **digital services based on advertising or other forms of indirect remuneration are subject to the Digital ECA,** provided they are supplied remotely, electronically, and upon individual request. The emphasis, therefore, is not on the economic nature of the activity, but on the mode of supply and the functional logic of the connected digital environment.

In summary, situations in which there is no individualized digital provision upon the user's request, in which the simultaneous physical presence of the provider and recipient predominates, or in which the content is disseminated generally and not individually to the public do not, as a rule, fall under the concept of information technology products or services. The analysis, however, must consider the specific characteristics of the offering and the way the product or service is used.

Social media

The Digital ECA considers social media platforms to be a type of information technology service provider. In this case, the Law expressly states that such services are subject to its provisions, including the requirement to comply with specific obligations, notably the requirement to link the account of a child or adolescent up to 16 (sixteen)

years of age to the user or account of one of their legal guardians (Art. 24) and the prohibition on creating behavioral profiles of child and adolescent users for the purpose of targeting commercial advertising (Art. 26). Thus, as a general rule, social media platforms should be considered an information technology service directed at children and adolescents or likely to be accessed by this audience.

The Digital ECA defines a social network based on its primary purpose, as follows:

> Art. 2 For the purposes of this Law, the following definitions apply:
> [...]
> III – social network: an internet application whose primary purpose is the sharing and dissemination, by users, of opinions and information conveyed through text or image, audio, or audiovisual files on a single platform, via accounts that are connected or articulately accessible, allowing for connections between users.

The core of the legal definition lies in the characteristics of users' sharing and disseminating opinions and information on a single platform, with interconnected and coordinated interaction between accounts. This prevents other interpersonal communication platforms—such as private messaging services, when used for private interpersonal communications, or closed-group services—from being classified as social networks.

This mode of operation of a social network is typically characterized by direct and widespread positive network externalities, in which the service's benefit grows as the total number of participants increases. In other words, the more people who join the platform, the greater the possibilities for interaction, visibility, and the open and mass circulation of content—which increases the service's appeal.

Classification as a social network depends essentially on the predominant nature of the service, subject to a case-by-case analysis. It must be determined whether its central purpose is to promote **open social interaction, with public contact between users**, and to enable the widespread circulation of content produced or shared, with significant dissemination among user accounts **and without substantial limitations on visibility or recipients.**

This scenario does not apply in the same way to restricted networks, such as corporate, institutional, or closed applications limited to specific groups. In such cases, although communication and sharing occur on the same platform, the predominant logic is not that of open social interaction among multiple, undifferentiated users.

It is worth noting that **classification as a social network under the Digital ECA is based on the activity actually carried out by the provider, and not from its self-declaration or the trade name it uses.** The definition of a social network is based on functional elements, primarily the purpose of sharing and disseminating information through interconnected accounts, regardless of the name adopted by the provider; it is therefore a definition based on function rather than nomenclature.

Furthermore, **Article 19, § 2, of Decree No. 12,880/2026** reinforces this understanding by establishing that the provider's own assessment of its classification is not binding on the ANPD, which may, within the scope of its authority, determine a different classification at any time.

EXAMPLE 1

Maria, a 15-year-old teenager, attends a School of Science and Technology that requires teachers to make content available on a specific platform operated by the institution, which is available on app stores. To access it, the student must log in using her student ID number and a

personal password. Within this platform, there is a student forum—a space where a wide range of information is shared, with a section dedicated to discussion and real-time interactions.

Analysis: · The platform provided by the school does not qualify as a social network for the purposes of the Digital ECA. Although several requirements are present—such as the ability to share and disseminate opinions and information—that is not the platform's primary purpose. As noted, the intent is to facilitate the provision of information to students, and the forum is merely one of the platform's incidental features. Even if this functionality were removed, the platform would still fulfill its intended purposes. Furthermore, it does not qualify as a social network because access to the platform is restricted to students and faculty.

App store

Just like social media platforms, online app stores are expressly treated by the Digital ECA as a type of information technology service provider. In this sense, it is a service that must comply with the provisions of the Law, as it is, as a rule, directed at children and adolescents or likely to be accessed by this audience. It must also fulfill specific obligations, such as providing an age signal to internet app providers or obtaining the free and informed consent of parents or legal guardians for the download of apps by children and adolescents.

The service's primary function is to distribute applications and facilitate their access for end users, connecting them with manufacturers and developers. The legal definition is set forth in Article 2, VI, of the Digital ECA:

> Art. 2 For the purposes of this Law, the following definitions apply:
> [...]
> VI – internet app store: an internet application that distributes and facilitates the download, for terminal users, of internet applications made available or accessible through its platform.

The central point of the definition lies in the store's intermediary role between the end user and the application's developer or provider. In practice, the developer of the product or service enters into an agreement with the store to use its infrastructure for promotion, availability, and distribution. In this context, the app store serves as a repository for accessing the application, organizing its presentation and public availability of the product.

As a general rule, the app store is not to be confused with the apps it distributes. In this regard, it is important to distinguish the intermediary role played by internet app stores from other similar functions, such as in-app purchases made within games or internet applications in general.

It should also be noted that this category of providers (app stores) is distinct from marketplaces. Although they also act as intermediaries and can facilitate access to internet applications (such as digital books and games), marketplaces have **a broader scope, as they involve the provision of various types of products and services, including physical goods, payment processing, and delivery logistics.** For this reason, this category has obligations distinct from those of app stores, as set forth, for example, in Article 18 of Decree No. 12,880/2026.

Similarly, electronic games that may offer additional content, benefits, or features for a fee within their own environment are not classified as app stores. In this scenario, it is merely an ancillary feature of the main service, without the distribution or facilitation of searching

for and downloading other apps. These practices may give rise to relevant obligations under the Digital ECA, but they are not sufficient, on their own, to classify a particular provider as an app store.

The existence of user payment also does not alter this classification. As a subcategory of information technology products or services, the store may operate under free, paid, or hybrid models. The determining factor is the function it performs in the digital chain, not the specific payment method.

Internet app stores occupy a significant position in the protection framework. They form a first layer of agents with responsibilities, among which the following stand out:

- taking proportionate, auditable, and technically secure measures to verify the age or age group of users (Art. 12, I, of the Digital ECA);
- providing age information to internet app providers (Art. 12, III, of the Digital ECA); and
- providing a mechanism to enable the free and informed consent of parents or guardians for the download of applications by children and adolescents (Art. 12, §2, of the Digital ECA).

It is also essential that these environments provide effective safeguards to prevent children and adolescents from entering into contractual or financial transactions without the proper supervision, representation, or assistance of their legal guardians. Failure to do so exposes this demographic to risks of economic exploitation, in potential violation of the imperative to protect children and adolescents from commercial exploitation **(Art. 32 of the Convention on the Rights of the Child; Art. 5, *caput of the ECA*; Art. 4, VI of the Digital ECA)**.

Thus, because they serve as a central hub connecting developers and end users, app stores play a structural role in the implementation of

the Digital ECA. In this regard, it can be stated that, beyond technical intermediation, their role entails duties that are essential to ensuring the priority protection of children and adolescents throughout the entire digital app ecosystem, guided by the principle of their best interests. In particular, these obligations include adopting high standards of privacy, personal data protection, and security on their platforms, as well as establishing age-appropriate restrictions, providing age ratings, and making parental supervision mechanisms available.

Operating systems

An operating system is a type of information technology product or service provider that must comply with the provisions of the Digital ECA because it is, as a rule, likely to be accessed by children and adolescents. It must also fulfill specific obligations, particularly that of providing an age signal to internet application providers.

The operating system is defined by the Digital ECA in the following terms:

> Art. 2 For the purposes of this Law, the following definitions apply:
> [...]
> VII – operating system: system software that controls the basic functions of hardware or software and allows internet applications, computer programs, apps, or other software to run through it.

In simple terms, it is the layer responsible for linking the device's physical components with the applications accessed by the user, which explains its legal significance. The operating system manages the device's resources, organizes the terminal's overall operation, and allows other applications to function in an integrated manner. It manages memory, files, devices, and commands, in addition to establishing the basic conditions for using the device.

From a functional perspective, we can identify some of its most relevant elements:

(a) central hardware management core;
(b) boot code, which prepares the device for operation;
(c) drivers, which enable the control of specific devices; and
(d) utility programs, which complement the use of the system.

Together, these elements demonstrate that the operating system plays a fundamental role in the user's digital experience. For example, when a user uses facial recognition to unlock a cell phone, the command issued through the interface activates device features — such as the camera — and relies on the operating system's technical coordination to ensure that the device's data capture, processing, and response occur seamlessly and securely.

Thus, the operating system integrates the user experience from the moment the device is first set up and influences how the user interacts with apps, content, and services. Given this, the responsibilities of operating system providers begin even before the user starts using specific applications. Since these systems come pre-installed on devices and determine how the device functions, a significant portion of the obligations under the Digital ECA falls on them.

As already highlighted by the ANPD[2], together with app stores, operating systems play a foundational role in the implementation of age assurance mechanisms. On the one hand, these systems and stores can ensure structural protection because they enable age verification and the configuration of parental supervision mechanisms on the device itself, rather than solely within isolated internet applications. On the other hand, they enable large-scale protection because the same age assurance mechanism — in particular, the age signal — can be used by various apps accessed by children or adolescents.

However, the implementation of the obligations set forth in the Digital ECA must take into account that there are different types and models of operating systems, including, for example, proprietary operating systems and those based on open-source and free software. Furthermore, while some operating systems are more commonly used by the academic and technical communities or in corporate environments, others are used on a large scale by end users — especially children and adolescents — since they are installed on the majority of mobile devices and personal computers in the country. At this point, we return to what was explained in the previous sections regarding Article 39 of the Digital ECA, which provides for the modulation of legal obligations according to the "degree of interference of the provider of the product or service over the content made available, the number of users, and the size of the provider."

Other provisions of the Law are also relevant to the imposition of obligations on operating systems. It is worth noting that Article 2, § 2, excludes from the definition of information technology products or services "the functionalities essential to the operation of the Internet, such as the open and common technical protocols and standards that enable interconnection among the computer networks that make up the Internet." Furthermore, Article 1, sole paragraph, III, adopts as one of the central elements for defining "likely access" the existence of "a significant degree of risk to the privacy, safety, or biopsychosocial development of children and adolescents" arising from the use of the service.

Together, these provisions form a regulatory framework guided by proportionality, a risk-based approach, and the need for differentiated treatment based on the size and nature of the provider. Thus, for example, operating systems based on collaborative models and open-source software—which are primarily used in tech-

nical communities and have a low likelihood of being accessed by children and adolescents—are not subject to the same obligations as proprietary operating systems used on a large scale by end users, especially children. A similar interpretation regarding the modulation of obligations applies to operating systems used in closed environments where there is little possibility of provider intervention regarding the content made available. This is the case for operating systems installed on Internet of Things (IOT) devices, such as internet-connected home appliances.

Services with editorial control and copyright-protected content

The Digital ECA considers "services with editorial control" and "providers of copyright-protected content previously licensed from a responsible economic agent who is not to be confused with an end user" ("providers of copyright-protected content") to be types of providers of information technology products or services. The definition and reference to these services are set forth in the following provisions of the Law:

> Art. 2 For the purposes of this Law, the following definitions apply:
> [...]
> IX – **service with editorial control:** an internet application whose primary purpose is to make previously selected content available, without the use of automated selection methods, by a responsible economic agent;
> [...]
> Art. 29. To comply with the principle of comprehensive protection, it is the duty of providers of information technology products or services directed at children and adolescents or likely to be accessed by them to 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 rights of children and adolescents, regardless of a court order.

[...]

§ 4 Journalistic content and content subject to editorial control shall not be subject to the removal procedure referred to in the *caput* of this article.

[...]

Art. 39. The obligations provided for in Articles 6, 17, 18, 19, 20, 27, 28, 29, 31, 32, and 40 of this Law shall apply according to the characteristics and functionalities of the information technology product or service, modulated according to the degree of interference of the provider of the product or service over the content made available, the number of users, and the size of the provider.

§ 1 **Providers of services with editorial control and providers of content protected by copyright previously licensed by a responsible economic agent** who is not an end user shall be exempt from complying with the obligations provided in the articles referred to in the *caput* of this section, provided that:

[...]

Decree No. 12,880/2026, Art. 22. Providers of services with **editorial control, of copyrighted content previously licensed by a responsible economic agent who is not to be confused with an end user,** and of musical or literary content, pursuant to the provisions of article 37, sole paragraph, and article 39, § 1, from law n. 15.211, from september 17th, 2025, are exempt from implementing age assurance, provided that:

I – they provide children's accounts or profiles with content appropriate for the age group of the child or adolescent, in accordance with the age rating system, when applicable; and

II – they implement parental supervision, blocking systems, or restrictions on children's and adolescents' access to content, while respecting progressive autonomy and age ratings, where applicable.

Sole paragraph. Providers of journalistic and sports content not subject to content ratings and subject to **editorial control** are exempt from age assurance.

Initially, it is evident that, although they are distinct categories, the Digital ECA treats services with editorial control and providers of copyright-protected content similarly. These categories include, for example, video streaming services or providers of musical or literary content.

In the case of services with editorial control, the main characteristic is the provision of content previously selected by a responsible economic agent, without the use of automated selection methods. The exclusion of automated methods indicates that editorial control presupposes some degree of human evaluation and curation in the process of selecting the content that makes up the service's catalog, as occurs, for example, on video streaming platforms.

In the case of providers of copyright-protected content, the central element is the prior licensing of content made available by economic agents who are not to be confused with end users, such as record labels in the case of music. As with services with editorial control, there is no prevalence of end-user-generated content, which justifies similar treatment under the Digital ECA.

The image below helps illustrate the distinction and the dynamics between the two categories of providers:

Figure 2: Services with editorial control and providers of copyright-protected content.

CRITERION 1 – PROVIDER'S ROLE

SERVICES WITH EDITORIAL CONTROL

Key Question

- Who decides what is published and how it is presented?
- The provider exercises effective editorial control over the selection, organization, presentation, or exclusion of content.

Focus

The service's editorial role.

Examples

Video streaming with a curated catalog; a journalistic or sports service featuring professional editing.

CRITERION 2 – SOURCE OF THE CONTENT

PREVIOUSLY LICENSED COPYRIGHTED CONTENT

Key Question

- Where does the content come from?
- Copyrighted content is licensed, prior to being offered by a responsible economic agent, such as a studio, production company, distributor, record label, or publisher, that is not the end user.

Focus

Origin and licensing chain.

Examples

Film and TV series catalog; music streaming; digital library.

There may be overlap

A service may curate and organize the catalog while also offering previously licensed works.

! The mere hosting or recommendation of content submitted by end users does not, in and of itself, fall under either of these scenarios. Evaluate the specific business model and the provider's role.

Digital ECA, Art. 39, §1 - Decree No. 12.880/2026, Art. 22

Article 39 of the Digital ECA exempts providers of services with editorial control and providers of copyright-protected content from complying with certain legal obligations, provided that specific safeguards are implemented, including compliance with age ratings and the provision of technical mechanisms for parental controls. This is the case, for example, with the exemption from the duty to remove content that violates the rights of children and adolescents as soon as they are notified of its offensive nature (Article 29).[3] This obligation applies to other contexts, particularly services — such as social media platforms — where users freely share content without any prior human curation or licensing of content by economic agents on the part of the platform.

The age assurance requirement was expressly exempted by Decree No. 12,880/2026 (Art. 22), subject to the availability of children's accounts or profiles and the implementation of parental supervision, blocking systems, or access restrictions for this audience. The exemption from the obligation to adopt the age assurance mechanisms provided for in that article, however, does not exempt the provider from the duty to adopt the most protective settings by default (Article 7 of the Digital ECA) or from the other obligations under the Digital ECA.

Likely access by children and adolescents

The term "likely access" broadens the scope of application of the Digital ECA beyond services directed—that is, explicitly aimed at—children and adolescents. In this sense, it is an essential element for defining the scope of the Law and determining which providers are subject to its legal provisions.

"Likely access" to a given product or service is established when **three requirements are cumulatively met**, as provided in the sole paragraph of Article 1 of the Digital ECA. See below:

> Article 1. This Law provides for the protection of children and adolescents in digital environments and applies to any information technology product or service directed at or likely to be accessed by children and adolescents in the country, irrespective of its location, development, manufacture, provision, marketing, and operation.
>
> Sole paragraph. For the purposes of this Law, the following situations are considered likely accessed by children and adolescents:
> 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, safety, or biopsychosocial development of children and adolescents, especially in the case of products or services intended to enable social interaction and large-scale information sharing among users in a digital environment.

It is important to note that a given information technology product or service will not be characterized as "likely to be accessed" by children and adolescents if only one or two of the requirements are present in a specific case. Thus, for example, a service will not be considered "likely to be accessed" if, although attractive and easily accessible, its use does not pose significant risks to the privacy, safety, or biopsychosocial development of children and adolescents. Therefore, all three requirements must be met simultaneously.

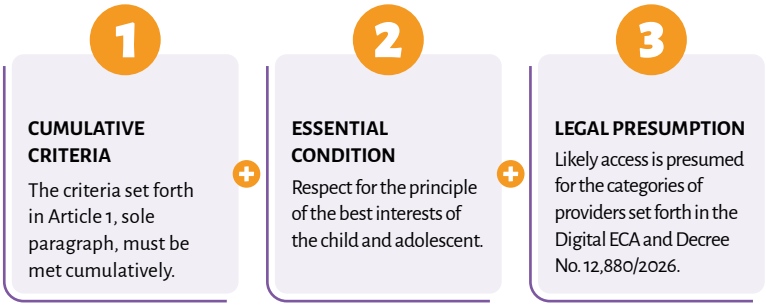
Nevertheless, this interpretation cannot be used to unjustifiably restrict the scope of application of the Digital ECA, particularly in situations where significant risks to children and adolescents have been identified. In this regard, the provisions of the sole paragraph of Article 1 of the Digital ECA must always be applied **in accordance with the principle of the best interests of the child and adolescent** (Article 5, § 2). This means **that interpretations contrary to this principle—and which have the direct or indirect effect of undermining the application of Digital ECA provisions** protecting privacy, safety, mental and physical health, access to information, freedom of participation in society, meaningful access to digital technologies, and the well-being of children and adolescents—**must not be accepted.**

To reinforce the above, it is worth noting that **certain types of information technology products or services have been deemed by the Digital ECA and Decree No. 12,880/2026 to be targeted at or likely to be accessed by children or adolescents.** This is particularly the case for the following providers, which are specifically mentioned and subject to specific obligations defined in the aforementioned regulations: social

media platforms, app stores, operating systems, services with editorial control, video games, adult content providers, systems capable of generating content and interacting with users based on natural language instructions, and e-commerce platforms that facilitate the purchase and sale of products and services prohibited for children and adolescents.[4] In all these situations, there is a **legal presumption that the service or product is likely to be accessed** by children and adolescents and is therefore subject to the provisions of the Digital ECA. Thus, as a general rule, conducting a "likely access" test is unnecessary for providers who already fall within the presumed categories listed above, since the legislation itself — whether the Digital ECA or Decree No. 12,880/2026 — already classifies them as products or services targeted at or likely to be accessed by children and adolescents.

This presumption may only be rebutted with proper justification and in situations where, given the specific circumstances of the case, one or more of the requirements set forth in Article 1, sole paragraph, of the Digital ECA are not met, while observing the principle of the best interests of the child and adolescent and the other interpretive criteria outlined in these Guidelines.

Figure 3: *Analysis of "likely access" for the purposes of applying the Digital ECA.*



In any case, **any self-assessment by the provider is not binding on the ANPD**, which may, based on legal criteria, reach a different conclusion and determine compliance with the Digital ECA's standards. In fact, the legislative intent was to **prevent the application of the Law from depending solely on the provider's own declaration or on formal classifications of the target audience**. Instead, the analysis must consider the product's or service's **actual suitability** for use by that audience, as assessed based on its functional characteristics. What matters is the combination of **the product's characteristics and actual conditions of use**, not merely the provider's indication of who its intended recipients are. It is worth noting that the measures adopted by the provider to comply with the obligations under the Digital ECA and Decree No. 12,880/2026 — such as age assurance mechanisms — cannot be considered sufficient to rule out any of the requirements set forth in the sole paragraph of Article 1 of the Law. There is a logical sequence between determining whether the provider falls within the scope of the Law and the fulfillment of its obligations. First, it must be determined whether the product or service is directed at children and adolescents or is likely to be accessed by them. Based on this determination — and as a result of it — legal obligations arise, including the obligation to verify users' ages. Age assurance therefore constitutes compliance with a legal obligation that follows the determination of the Law's applicability, rather than a factor that precludes likely access.

For these reasons, the analysis of likely access must consider the characteristics of the product or service regardless of the measures adopted to comply with the law. A different interpretation would lead to a circular argument: compliance with a legal obligation would remove the provider from the scope of the regulation that imposes it, which would authorize the elimination of the measure itself and, consequently, reestablish the conditions for likely access.

The scenario in which a service or product is directed at children and adolescents arises when the provider explicitly states that its product is intended for a child and adolescent audience (in the terms of use of the product or service, in its description, among other places). By doing so, the provider assumes the duty to ensure the priority protection of these users and the prevalence of their best interests, and must comply with the rules of the Digital ECA.

In many other cases, products and services are not formally intended for children and adolescents, but their design, language, features, engagement mechanisms, and conditions enable access by this audience, posing significant risks to their rights. In these scenarios, the application of the Digital ECA — through an analysis of the concept of "likely access" — **cannot be set aside due to technicalities or attempts to ignore real-world situations in which a given platform is, in fact, used by children and adolescents,** even if it was not designed or targeted at this audience.

The presence of certain factors — **by way of example** — can aid in the analysis of the requirements set forth in Article 1, sole paragraph, of the Digital ECA. This involves verifying the existence of **relevant evidence** that a given service **meets the criterion of "likely access,"** given its appeal, ease of access, and significant risks to children and adolescents. In this regard, a given service is **more likely** to **meet the criterion of "likely access"** when **one or more of the following illustrative situations are identified:**

- the availability of products or content of interest to children and adolescents;
- the use of design elements that are attractive to children and adolescents;
- the display of advertising targeted at children and adolescents;

- similarity to services considered to be "likely to be accessed" by the Digital ECA and Decree No. 12,880/2026; and actual access or use by children and adolescents, based on available evidence, including data from the platform itself or from independent research and studies.

Figure 4: *Non-exhaustive evidence for the "likely access" test.*

IMPORTANT

The evidence presented in these Guidelines is provided solely for illustrative and auxiliary purposes. It does not constitute additional legal requirements, nor does it replace or modify the three cumulative requirements set forth in Article 1, sole paragraph, of the Digital ECA. Thus, the presence or absence of any of this evidence, by itself, does not determine whether a product or service is (or is not) considered likely to be accessed by children and adolescents.

The conclusion must always result from a joint analysis of the three legal requirements set forth in the Digital ECA.

Finally, the "likely access" criterion also prevents gaps in dynamic environments, where business models, interfaces, and features change rapidly. Products and services may change their profile, incorporate new features, alter their marketing methods, and reach audiences not previously anticipated. Thus, the applicability of the Law depends on the specific manner in which the service or product operates, its potential to attract children, and the possible consequences and risks to the child audience.

A complete flowchart for the "likely access" test is available in Appendix III of these Guidelines.

Next, we will analyze each of the requirements for characterizing "likely access."

Likelihood of use and attractiveness

The likelihood of use and the appeal of a product or service are related to user motivation and explain why certain products and services are able to capture and hold the attention of children and adolescents. Appeal is related to the ability of **the design, content, and presentation strategies** of a given information technology product or service to spark the interest of children and adolescents.

Thus, the likelihood of use and appeal are related to **the characteristics and engagement mechanisms of a given product or service that make its use desirable for children and adolescents,** even if they are not specifically targeted at or are formally prohibited for this audience.

These characteristics and practices warrant attention because they can increase initial interest, return frequency, and usage time among children and adolescents. In contexts of information asymmetry between providers and users, design elements and service features can contribute to making the digital environment more inviting.

When analyzing attractiveness, factors such as language, visual aesthetics, themes, characters, rewards, gamification, the use of influencers, engagement dynamics, and other aspects that make the product or service emotionally relevant or particularly appealing to children and adolescents should be considered — even if they are not accompanied by language or visual aesthetics explicitly aimed at children. The analysis therefore depends on the actual experience of children and adolescents, regardless of the commercial intent stated by the provider.

The key point is not the isolated existence of an eye-catching feature, but the actual ability of the combination of elements to increase the potential for initial interest, adoption of the service, or repeat use. When a product or service is designed to increase interest in its use, the likelihood that

it will actually be used by children and adolescents increases. Certain elements, taken in isolation, may seem neutral, but when combined with notifications, rewards, rankings, and personalization, they can increase the frequency of use and return to the service by this population.

The Digital ECA focuses not only on the final content offered, but also on the characteristics of the product or service that may increase its appeal and the likelihood of its use by children and adolescents. Thus, products and services with strong visual, sensory, or behavioral appeal may fall within the scope of likely access even when they have not been formally designed for children or adolescents.

Ease of access and use

Ease of access and use refers to the **technical, operational, and contextual conditions that reduce barriers to accessing and using the product or service.** This criterion involves the technological architecture, delivery mechanisms, interaction interface, operational workflows, and user experience elements that structure the functioning of the product or service, its usability, and other elements that can prevent or reduce practical barriers to access or use by children or adolescents.

This dimension involves the service's delivery infrastructure, usability, and compatibility with widely available devices. Simplified onboarding processes, low technical requirements, and an intuitive user experience reduce barriers to access and increase the actual likelihood of users signing up for, using, and returning to the service.

While attractiveness relates to the characteristics that make the service appealing to this audience, ease of access and use refers to the conditions that reduce practical barriers to entry and use, regardless of the content offered.

The presence of features or adaptations implemented to comply with accessibility laws or standards should not be interpreted, in isolation, as evidence of greater ease of access and use for the purpose of determining likely access. These mechanisms are intended to promote accessibility and inclusion, ensuring equal access for people with disabilities, the elderly, those with reduced mobility, those with low digital literacy, and other groups, and do not, in and of themselves, alter the assessment of the requirement set forth in item II of the sole paragraph of Article 1 of the Digital ECA.

Thus, the analysis of ease of access and use remains focused on verifying the specific conditions that reduce practical barriers to entry and use by children and adolescents, taking into account the architecture, usability, interaction flows, and other elements of the product or service. Consequently, attributes of good usability, accessibility, and inclusive design do not, in and of themselves, constitute evidence of appeal to children and adolescents — which must be assessed through a combination of elements tailored to this audience.

The Brazilian context underscores the importance of this criterion. The widespread use of the internet by children and adolescents and the proliferation of mobile devices make countless digital services accessible.[5] In this context, technical availability on commonly used devices—including cell phones, tablets, and wearable electronic devices—can already constitute a significant factor in reducing barriers to access for children and adolescents. Furthermore, when a service operates smoothly on commonly used devices, with simple user interfaces and few steps required for activation, barriers to use are reduced, making the product or service easier to integrate into the daily lives of children and adolescents.

This requirement pertains to the material conditions of use. The more intuitive and straightforward the path from initial contact to actual use of the service, the less effort is required to access it.

EXAMPLE 2

Tamara, age 10, wants to use a social media platform that is very popular among her classmates. The platform features short videos on professional makeup techniques. When opening the app, there is an option to "Sign in with an email account," using the email address already associated with the mobile device or computer being used. To justify this flexibility, the providers claim that their product is aimed at the specific niche of professionals in the field and not at children.

Analysis · In the described situation, the platform is easily accessible and usable by children and adolescents, thereby meeting the second requirement for "likely access," as provided for in subsection II of the sole paragraph of Article 1 of the Digital ECA. The absence of significant barriers to accessing the platform and interacting with the community facilitates its use. Therefore, the simplified user registration processes result in considerable ease of access to the social network by children and adolescents.

Significant degree of risk

The significant degree of risk to privacy, safety, or biopsychosocial development (Article 1, sole paragraph, III, of the Digital ECA) constitutes a third requirement for characterizing likely access. Unlike the criteria related to attractiveness or ease of access, this aspect considers the protective relevance associated with the use of the product or service and the specific exposure of children and adolescents to foreseeable negative effects.

In this context, risk corresponds to the possibility of negative effects on the privacy, safety, or biopsychosocial development of children and adolescents resulting from the use of a product or service, taking into account the probability of occurrence and the potential severity of the consequences.

Among other possibilities, the Law specifically refers to products and services that enable large-scale social interaction and information sharing (Art. 1, sole paragraph, III, Digital ECA), indicating the existence of a presumption of significant risk in these cases. This reference is illustrative and allows for a broader interpretation: certain technical arrangements and business models may, by their very nature, increase the exposure of children and adolescents to significant risks.

The term "significant" indicates that this is not just any ordinary risk inherent in social life or the use of technology. By way of example, this may include negative impacts on children and adolescents arising from the nature of the service, the content made available, the design standards adopted, the features accessible to children and adolescents, the data processing carried out, the technologies used, and, in general, the effects generated by such use on users' privacy, safety, or biopsychosocial development.

The assessment is contextual and forward-looking. It considers, on a non-exhaustive basis, the probability of negative effects occurring and their potential severity based on the ordinary operation of the product or service, and not merely on exceptional events. It is worth noting that, in the context of a "likely access" analysis, the risk assessment should not be limited to a specific mechanism or an isolated feature of the product or service. This is a comprehensive analysis that must consider the operations of the information technology product or service provider as a whole, including its business model, features, architecture, recommendation and interaction mechanisms, personal data process-

ing flows, usage patterns, engagement strategies, methods of content delivery, and other elements capable of impacting the privacy, safety, or the biopsychosocial development of children and adolescents.

However, the risk analysis conducted as part of the "likely access" test must not be confused with the duty to manage and assess risks, as provided for in Article 8, I, of the Law. A significant degree of risk to the privacy, safety, or biopsychosocial development of children and adolescents serves as the criterion for defining the material scope of application of the Digital ECA. Risk management and assessment, on the other hand, are legal duties of regulated entities (Articles 6, *caput*; 8, I; and 16, sole paragraph, I, of the Digital ECA; Article 47 of Decree No. 12,880/2026) and, therefore, presuppose the applicability of the Law.

Of particular note is the provision in Decree No. 12,880/2026 that imposes on providers of information technology products or services the duty to conduct "an assessment of the impact on children's safety and health, including the identification and analysis of risks, an evaluation of the probability of occurrence and the severity of the potential impact, the management and mitigation of risks, and continuous monitoring of the effectiveness of the measures adopted" (Art. 47). The preparation of risk assessments and impact reports constitutes best practice for gauging the degree of risk in the likely access scenario involved in a given situation and for defining appropriate prevention and mitigation measures.

However, the implementation of risk mitigation measures, on its own, does not preclude the application of the "significant degree of risk" criterion, especially in cases where such measures are part of the mechanism necessary for risk management and are intended to meet the obligations set forth in the Digital ECA. While the duty of prevention and related obligations can be fulfilled through effectively implemented mitigation measures, such measures do not preclude the application of the "significant degree of risk" criterion for the pur-

pose of determining likely access. Thus, for example, the implementation of age assurance measures in compliance with the provisions of the Digital ECA does not preclude the application of the "likely access" criterion (and the Law itself) to the provider, even if it is considered that the implemented measures have mitigated the risks involved.

EXAMPLE 3

Carlos, aged 14, began using a social media platform accessible via a mobile app, which, at first glance, seemed like just another way to make new friends. The platform allowed users to send messages, short videos, and audio clips. Through notifications and personalized recommendations, the service encouraged frequent interactions with other users. The platform did not provide any information about how it operated, despite collecting and storing a large volume of data, including message history, interaction patterns, and usage time. This information was used to power algorithmic personalization mechanisms capable of suggesting new content and connections.

Analysis · The case described highlights significant risks across the three dimensions set forth in Article 1, sole paragraph, III, of the Digital ECA. With regard to privacy and the protection of personal data, it is noted that the provider did not make clear and adequate information available to parents and guardians regarding the social network's operating model, the processing of adolescents' personal data, the scope of the collection and storage of content generated during interactions, and the use of the system for recommendations and personalization. The security aspect, in turn, involves risks arising from adolescents' exposure to unsupervised contact with adults. Finally, biopsychosocial development may also be affected by the encouragement of continuous and prolonged use, posing significant risks to the well-being and health of child and adolescent users.

Duty of prevention

Article 5 of the Digital ECA establishes the "duty of prevention." This general duty is divided into four fundamental duties that underlie the entire Law and guide the actions of providers of information technology products and services, as follows:

> Article 5. Providers of information technology products or services directed at children and adolescents or likely to be accessed by them shall observe the **duties of prevention, protection, information, and safety** provided for in this Chapter and in Law No. 8,078, of September 11, 1990 (Consumer Defense Code), and in Law No. 8,069, of July 13, 1990 (Child and Adolescent Statute), in accordance with the principle of the best interests of the child and adolescent and their comprehensive, special, and priority protection.

Thus, the duty of prevention consists of four dimensions (protection, information, safety, and prevention in the strict sense), which, taken together, anchor the regulatory model established by the Digital ECA. These dimensions complement one another and often overlap, so that a single obligation under the Law or Decree No. 12,880/2026 may fulfill more than one of them at the same time. Default settings at the most protective level, for example, fulfill both the duty of protection and the duty of safety for children and adolescents. The division into four dimensions helps to understand the logic of the regulatory

model, but does not require that each obligation be classified under a single dimension.

This is a model focused on preventing the risk of violations of children's and adolescents' rights — including the rights to privacy and personal data protection, safety, and physical and mental health — and on the comprehensive protection of this population in the digital environment. Rather than only imposing specific obligations, the Digital ECA establishes a model of responsibility guided by risk anticipation, qualified transparency, and the secure organization of digital environments. As a result, the focus shifts from reacting to harm to preventing it, and providers are required not only to comply with regulations but also to demonstrate the measures they have adopted to comply with the law.

This duty also requires documenting and demonstrating the effectiveness of the measures adopted. It must be noted that the risk-based approach itself is grounded in the concept of accountability, and that the Law and its implementing Decree require the implementation of measures that are **effective** in preventing rights violations and promoting the comprehensive protection of children and adolescents (Art. 9, § 1; Art. 32; and Art. 33, §3, Digital ECA; Arts. 15, I and II, 18, 26, §3, 41, sole paragraph, 47, and 49, Decree No. 12,880/2026). Efficacy and effectiveness must be supported by evidence documented by the regulated entities.

In this sense, the **duty of prevention** can be understood as the legal obligation of providers of information technology products or services to **act proactively and diligently** by adopting appropriate, proportionate, and effective measures that, throughout the life cycle of the products and services, prevent or mitigate risks of violations of children's and adolescents' rights and protect their best interests.

Articles 6, 7, and 8 of the Digital ECA objectively express this concept by setting forth the main elements that comprise the duty of preven-

tion for providers of information technology products or services. The text reads as follows:

> Art. 6 Providers of information technology products or services directed at children and adolescents or likely to be accessed by them shall **take reasonable measures, from the design stage and throughout the operation of their applications, with the objective of preventing and mitigating risks of access, exposure, recommendation, or facilitation of contact** with the following content, products, or practices:
> I – sexual exploitation and abuse;
> II – physical violence, cyberbullying, and harassment;
> III – inducement, incitement, instigation, or aid, through instructions or guidance, 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, the use of substances that cause chemical or psychological dependence, self-diagnosis and self-medication, self-harm, and suicide;
> IV – 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;
> V – predatory, unfair, or deceptive advertising practices, or other practices known to cause financial harm to children and adolescents; and
> VI – pornographic content.
> [...]
> § 2 Among the preventive measures provided for in the *caput* of this article include clear, effective policies, appropriate to the Brazilian legislation, for the prevention of cyberbullying and other forms of online harassment, with adequate support mechanisms for victims, as well as the development and availability of educational awareness programs aimed at children, adolescents, parents, educators, employees, and support teams regarding the risks and methods for prevention and combat these practices, in accordance with the regulation.

Art. 7 Providers of information technology products or services intended for children and adolescents or likely to be accessed by them shall, from the design of their products and services, **ensure, by default, the most protective settings available regarding privacy and personal data protection,** considering the individual's autonomy and evolving capacities and justified by the best interests of the child and adolescent.

§ 1 The product or service referred to in the *caput* of this article shall, by default, operate with the highest level of privacy and personal data protection, provided that the provision of **clear, accessible, and adequate information** so that the child or adolescent and their guardians can make informed choices regarding the possible adoption of less protective settings.

§ 2 The providers referred to in the *caput* of this article shall 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 by law, subject to the principles set forth in Article 6 of Law No. 13,709, of August 14, 2018 (General Personal Data Protection Law), and the best interests of the child and adolescent.

Article 8. Providers of information technology products or services intended for children and adolescents, or that are likely to be accessed by them, shall:

I – **manage the risks** associated with its resources, features, and systems, as well as their impacts on the safety and health of children and adolescents;

II – **evaluate the content** made available to children and adolescents according to their age group, to ensure it is **consistent with the applicable age rating;**

III – provide **systems and processes designed to prevent** children and adolescents from encountering, through the product or service, illegal and pornographic content, as well as other content that is manifestly inappropriate for their age group, in accordance with age rating standards and applicable law;

> IV – develop, from the design stage, and adopt **by default settings that prevent the compulsive use** of products or services by children and adolescents; and
>
> V – **provide comprehensive information to all users regarding the** recommended **age group** for the product or service at the time of access, as established by the age rating policy.

Therefore, the duty of prevention specifically comprises mandatory and preventive measures regarding:

(i) privacy and personal data protection, including the adoption of the most protective model available by default;
(ii) risk management of resources, functionalities, and systems and their impacts on safety and health;
(iii) evaluating and providing content appropriate for users' age groups;
(iv) the development and adoption of design standards that prevent compulsive use; and
(v) the provision of clear, accessible, and appropriate information to users and legal guardians.

In practical terms, the duty of prevention requires the implementation of various protective measures, including, for example, the adoption of age assurance mechanisms (Art. 10) and parental supervision (Art. 16), the establishment of adequate content moderation systems (Articles 28–30), and the publication of semiannual transparency reports (Article 31).

Another relevant aspect to consider is that, as can be inferred from Articles 5 and 7, § 2, the application of the duty of prevention provided for in the Digital ECA may be supplemented by principles and rules set forth in the Child and Adolescent Statute (Law No. 8,069/1990, ECA), the Consumer Defense Code (Law No. 8,078/1990, CDC), and the General Personal Data Protection Law (Law No. 13,709/2018, LGPD).

By way of example, relevant provisions include Articles 70 and 100, sole paragraph, item II, of the ECA, which establish, respectively, the duty of all persons to prevent threats to or violations of children's and adolescents' rights, and that all of its provisions must be interpreted and applied considering the comprehensive and priority protection of children's and adolescents' rights. With regard to the Consumer Defense Code (CDC), Article 8 provides that products and services may not pose "risks to consumers' health or safety, except for those considered normal and foreseeable due to their nature and use, and providers are required, under all circumstances, to provide necessary and adequate information regarding them." Finally, regarding the LGPD, the principles of transparency, prevention, security, and accountability — among others set forth in Article 6 — are worth highlighting.

These and other provisions of the ECA, the CDC, and the LGPD—mentioned here merely by way of example — indicate the existence of a complementary relationship between these laws and the Digital ECA, a relationship that can facilitate and assist in the process of interpreting and applying the new legislation. This complementarity must, however, adhere to the risk-based regulatory approach that characterizes the Digital ECA, in which the obligations of regulated entities are proportionate to the risk that the information technology product or service poses to children and adolescents.

Next, we turn to an analysis of the four dimensions of the duty of prevention.

Duty of prevention *(Stricto sensu)*

The duty of prevention in the strict sense can be understood as the duty of providers to identify, assess, prevent, and mitigate risks to the privacy, safety, and health of children and adolescents. The preventive nature of this duty stems from ex ante action — that is, prior to the occurrence of

harm—both in the design of the product or service and throughout its operation. This proactive approach enables the identification of likely risks and the adoption of appropriate measures to prevent them from materializing. Among the main manifestations of this duty are risk management and the assessment of impacts on the health and safety of children and adolescents, as provided for in Article 8, I, of the Digital ECA and in Article 47 of its implementing decree.

The first step in risk management requires providers to identify the risks that their products or services may pose to the health and safety of children and adolescents. Based on Article 8, I, this analysis must cover three interrelated levels: (i) functionalities, that is, the tools made available to users and the actions they enable, such as private communication via instant messaging; (ii) the resources, that is, the technological components that support these functionalities, such as hardware, computer programs, integrated artificial intelligence models, and end-to-end encryption; and (iii) the systems, understood as the architecture that integrates these components, from the user interface to the operating system.

Once the risks have been identified, it is the provider's responsibility to assess the **likelihood** of their occurrence and the **severity** of the potential impact (Decree No. 12,880/2026, Art. 47). It is recommended that this assessment indicate the level of risk that the product or service poses to children and adolescents (e.g., low, medium, or high) based on clear criteria, in accordance with existing best practices. Subsequently, appropriate measures and safeguards must be adopted to prevent and mitigate these risks.

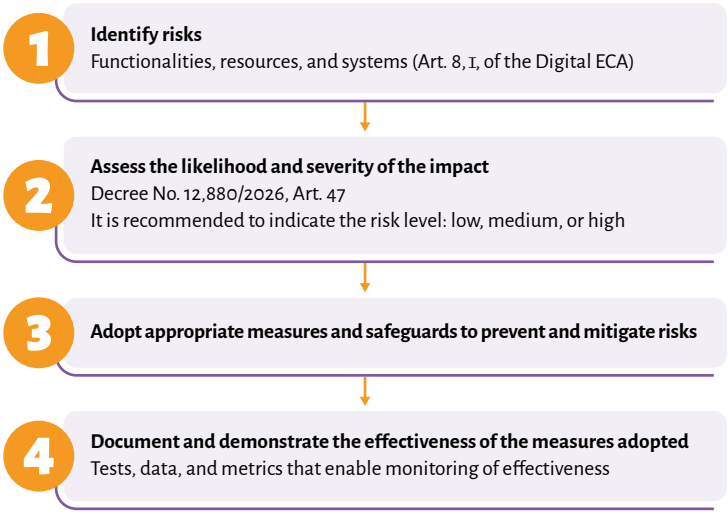
It is also necessary to document and demonstrate the effectiveness of the measures adopted. The Law and its implementing decree require both the implementation of measures that are **effective** in preventing risks and the ongoing monitoring of their effectiveness (Articles 9,

caput; 32, *caput* and § 3, of the Digital ECA; Articles 14, III; 15, II; 18; 26, §3; 41, sole paragraph; 47; and 49, Decree No. 12,880/2026). Thus, the effectiveness of the measures must be supported by evidence documented by the regulated entities. To ensure compliance with this requirement, providers must adequately document the process of implementing the adopted measures, including, for example, (i) tests and data used to assess whether the measures are achieving the expected results; and (ii) metrics that allow for monitoring, over time, the effectiveness of addressing the identified risks.

Certain references may assist in the work of identifying, analyzing, and managing risks. In the field of risk typologies, the European Commission, in its "Guidelines on measures to ensure a high level of privacy, safety, and security for minors online"[6], refers to the "5Cs" model (content, conduct, contact, consumer, and cross-cutting risks) of risks to children and adolescents in the digital environment, proposed by the Organization for Economic Cooperation and Development[7], and also cites the "4Cs" model (content, contact, conduct, and contract). In addition to these classifications, other references provide parameters for identifying and assessing risks, such as the "United Nations Guiding Principles on Business and Human Rights"[8]. According to the document, the results of the assessments should be integrated into the organization's relevant areas and processes—such as product development, design, engineering, and content moderation—so that potential impacts are prevented or mitigated and impacts that have already occurred are remedied.

The flowchart below outlines the steps involved in implementing the duty of prevention in the strict sense.

Figure 5: Flowchart of the duty to manage risks.



EXAMPLE 4

Caio, 15, posts a photo of his artistic performance at school on an online platform. In the comments section, a group of classmates begins posting repeated messages containing insults, derogatory nicknames, and incitement for other users to ridicule the post. In accordance with its terms of use and its internal policy for preventing violations of the rights of children and adolescents, the platform's automated system identified a pattern of offensive language and coordinated interactions, classifying the series of actions as a risk to the adolescent user. This pattern analysis and classification mechanism was developed internally by the platform and implemented into the service's architecture following tests and evaluations with documented results deemed satisfactory. Consequently, the case was referred for contextual analysis by human moderators, who confirmed the pattern of harassment

and systematic online intimidation. Accordingly, the unlawful content is removed, and the accounts of the responsible users are suspended. Caio is notified that the platform identified and addressed the situation ex officio, preserving its integrity and the original post, and is informed of the reason and rationale for the measure, with the option to file an appeal.

Analysis · This example illustrates the platform's preventive action, in compliance with the duty of prevention in the strict sense and, more specifically, with the provisions of Article 6, II and § 2, of the Digital ECA. Thus, it adopts reasonable measures to prevent and mitigate risks of facilitating access to and exposure to unlawful content, based on a clear, effective policy that complies with Brazilian legislation on the prevention of systematic online bullying and other forms of harassment on the internet.

Duty of protection

The duty of protection requires providers of information technology products or services to **ensure the comprehensive and special protection of children's and adolescents' rights in the digital environment, affording them absolute priority,** guided by the principle of their best interests. It complements the duty of prevention in the strict sense and is directly related to some of the fundamental principles governing the use of information technology products and services by children and adolescents. Among these principles, set forth in Article 4 of the Digital ECA, the following are particularly noteworthy: the guarantee of their comprehensive protection, the absolute prevalence of their interests, and protection against commercial exploitation.

This last aspect is of great importance in the context of the duty of protection and is reflected in specific rules set forth in the Digital ECA,

such as the prohibition on *the use of profiling techniques to target commercial advertising at children and adolescents, as well as the use of emotional analysis, augmented reality, extended reality, and virtual reality for this purpose* (Art. 22). Similarly, one must consider the prohibition on abusive advertising and the restrictions on the marketing of certain products to children and adolescents in the digital environment, such as games of chance, fixed-odds betting, lotteries, tobacco products, alcoholic beverages, and narcotics, pursuant to Articles 31 and 32 of Decree No. 12,880/2026, respectively.

Given these provisions, the duty of protection requires diligent action, proportionate intervention, and an effective response to content, conduct, or dynamics that affect children and adolescents. Thus, it demands appropriate containment and response to identified risks in order to ensure the comprehensive, special, and priority protection of the rights of children and adolescents in the digital environment.

Duty to inform

The duty to provide information, in the context of the Digital ECA, imposes on providers of information technology products or services the obligation to **provide clear, accessible, and adequate information about products and services, including operating and usage conditions, as well as the risks involved and the security measures adopted.** This is an autonomous and cross-cutting obligation that should not be confused with merely formal transparency, nor is it satisfied by simply making available lengthy, technical, or difficult-to-understand texts.

For the purposes of the Law, "informing" means making effective communication efforts to ensure genuine understanding by the target audience. Therefore, the duty pertains to structural aspects of the product or service and varies depending on how the provider organizes, presents,

and contextualizes essential information related to its activities.

Consequently, it is noted that this obligation can be fulfilled, among other ways, through the following measures:

(i) use of simple, clear, and objective language appropriate for the age group, using visual aids whenever possible;
(ii) prominent display and simplified access to the most relevant information, especially that related to risks, features, restrictions, settings, and the consequences of certain choices; and
(iii) communication at appropriate points in the user flow without disrupting the regular user experience.

Information targeted at children and adolescents must meet even stricter standards, given their status as developing individuals. Simply providing formal access to the text is not enough. Conditions must be created so that users and guardians can understand — in a manner consistent with their respective roles — how the service works and the main impacts of its use. For the same reason, designs and communication strategies that conceal risks, obscure essential information, make it difficult to reverse choices, or induce decisions contrary to the best interests of children and adolescents are incompatible with this duty. In this vein, the Digital ECA prohibits providers "to design, modify, or manipulate interfaces with the purpose or effect of compromising the user's autonomy, decision-making, or choice" (Art. 18, §2).

The duty to inform extends throughout the entire lifecycle of digital products or services, covering both prospective and retrospective information — that is, the types of information typically found in transparency reports. Prospective information guides users' choices and protects them before or during the use of the product or service. It consists of information about the actual functioning of the product or service and its features. This includes the methods of data collec-

tion and processing[19], the use of parental control tools, age ratings, the risks arising from the content made available by the product or service, and the security measures adopted.

Retrospective information, in turn, is intended to **ensure transparency and accountability to society and public authorities regarding the measures adopted by the regulated entity.** Its primary instrument is the semiannual transparency reports provided for in Article 31 of the Digital ECA, in which internet application providers must report on their activities during the period. These reports must include information on the channels available for receiving complaints and the systems and processes for investigating them; the number of complaints received; the amount of content or account moderation, by type; the measures adopted to identify unlawful acts and children's accounts on social media; technical improvements for the protection of personal data and privacy and for verifying parental consent; details of the methods used and the presentation of the results of impact assessments, as well as the identification and management of risks to the safety and health of children and adolescents, among other information. In other words, compliance with the duty of prevention also depends on fulfilling the duty to inform.

Under the terms of Article 31, the obligation to publish semiannual transparency reports applies only to providers with more than 1,000,000 (one million) registered users in the age group of children and adolescents who have an internet connection within the national territory. Providers are exempt from this obligation if their services are under editorial control or the content provided is protected by copyrights previously licensed from a responsible economic agent (distinct from the end user). This exempt is conditional upon meeting the requirements set forth in Article 39, § 1, items I through IV.

Transparency, in this context, is not merely about making documents available. It is a duty aimed at fostering an effective understanding of the measures adopted. Fulfilling this duty requires enabling affected individuals to make informed choices, as well as allowing society to monitor whether providers of information technology products or services are complying with their legal obligations.

The duty to inform addresses a structural issue in the digital environment: the information asymmetry between service providers and users. The providers design the features, define their service's data flows, and operate their systems; therefore, they have a duty to understand the potential impacts of what they offer. In the absence of adequate communication, this disparity further exacerbates the vulnerability of children and adolescents.

EXAMPLE 5

Bruno, a 13-year-old teenager interested in a new interactive dance game, creates an account on the DançaTech platform. To start playing, he must accept the standard terms of use. When he begins a dance session at home, the game starts recording his body movements and images of his surroundings, streaming everything in real time to other users. While Bruno dances in the living room, the camera captures details of the space, such as furniture and personal belongings. A few days later, Bruno's guardians are surprised to discover that clips of his dances are circulating in the game's promotional materials.

Analysis · In this case, the complete failure to provide information to the user and his legal guardians indicates that the platform's conduct constitutes a violation of the duty to inform, as protected by various legal statutes, such as the Digital ECA and the LGPD. In addition to the need to provide clear, accessible, and

adequate information about how the platform operates, it must be noted that the use of images of children and adolescents for commercial promotional purposes requires authorization from their legal guardians, which was also not obtained in this case.

Duty of safety

Under the Digital ECA, the duty of safety can be defined as the responsibility to **prevent the occurrence of accidental or unlawful situations that result in the improper processing of children's and adolescents' personal data, or that impact their life, health, and physical and psychological well-being.** In practice, this requires the adoption of reasonable measures that are proportionate to the characteristics of the service, its functionalities, its scale, and the degree of influence it exerts over content and interactions.

The Digital ECA is not limited to the risks of unauthorized access, personal data leaks, or other security incidents. It also covers typical vectors of harm in the digital environment, such as sexual exploitation and abuse, violence, intimidation, harassment, incitement to harmful behavior, and other situations in which the service's architecture may facilitate significant exposure.

The intensity of the duty of safety varies according to the provider's position and the service's structure: the greater the capacity to amplify, direct, or facilitate interactions and content accessible to children and adolescents, and the greater the platform's reach, the greater the burden of demonstrating that security is built into the design and continuously maintained during operation.

Safety, under this framework, is a permanent condition for the responsible operation of the product or service. The provider must demonstrate that it identifies relevant risks, adopts appropriate controls, and maintains a continuous process for reviewing the measures implemented.

Thus, the duty of safety completes the protective core of the Digital ECA. Without technical and organizational conditions proportionate to the specific risks of the product or service, the other duties of prevention, protection, and information are compromised.

Notes

Providers of information technology products or services ▸ p. 08–28

[1] "Art. 3 [...] § 1 A product is any good, whether movable or immovable, tangible or intangible. § 2 A service is any activity provided in the consumer market in exchange for compensation, including those of a banking, financial, credit, and insurance nature, except those arising from labor relations." BRAZIL. Law No. 8,078, of September 11, 1990. Provides for consumer protection and other measures. Consumer Defense Code, Art. 3, §§ 1 and 2. Federal Official Gazette: Brasília, DF, Sept. 12, 1990. Available at: Legislation Portal — Planalto. Accessed on: Apr. 29, 2026. ▸ p. 13

[2] BRAZIL. National Data Protection Agency. Board of Directors. Matter for consideration by the Board of Directors—Digital ECA. Document No. 0259383/2026/DIR-IM/CD/ANPD. Case No. 00261.001299/2026-96. pp. 4–5. Brasília, DF: ANPD, March 19, 2026. Available at: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/fundamentacao.pdf. Accessed on: April 29, 2026. ▸ p. 22

[3] Although § 4 of Art. 29 of the Digital ECA refers only to services with editorial control, Art. 39 of the Law expressly exempts providers of copyright-protected content from complying with that obligation. ▸ p. 28

Likely access by children and adolescentes ▸ p. 29–41

[4] See, among others, the following provisions of the Digital ECA that refer to these providers or impose specific obligations on them: Articles 2, III, IV, VI, VII, IX; 9, § 2; 12; 17, § 4, VIII; 20; 21; 24 through 26; 39, § 1. With regard to Decree No. 12,880/2026, the following provisions may be cited: Articles 11; 15 through 19; 21 through 23; 25. ▸ p. 31

[5] The cell phone is the primary device for accessing the Internet: 96% of users aged 9 to 17 connected to the Internet via a cell phone in 2025. Daily cell phone use reaches 90% of users, rising to 98% among adolescents aged 15 to 17. BRAZILIAN NETWORK INFORMATION CENTER (NIC.br). Survey on Internet Use by Children and Adolescents in Brazil: TIC Kids Online Brazil 2025. 1st ed. São Paulo:

Brazilian Internet Steering Committee, 2026. Available at: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/. Accessed on: Apr. 29, 2026. ▸ p. 37

Duty of prevention ▸ p. 42–57

[6] EUROPEAN UNION. European Commission. Communication from the Commission: Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (C/2025/5519). Official Journal of the European Union, Series C, Luxembourg, Oct. 10, 2025. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52025XC05519. Accessed on: Apr. 29, 2026. ▸ p. 49

[7] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). Children in the digital environment: revised typology of risks. Paris: OECD Publishing, 2021. (OECD Digital Economy Papers, No. 302). Available at: https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html. Accessed: Oct. 8, 2026. ▸ p. 49

[8] UNITED NATIONS. Office of the United Nations High Commissioner for Human Rights. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework. New York; Geneva: United Nations, 2011. (HR/PUB/11/04). Available at: https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. Accessed on: Oct. 8, 2026. ▸ p. 49

[9] Article 14, § 6, of the LGPD provides that "information regarding data processing referred to in this article must be provided in a simple, clear, and accessible manner, taking into account the user's physical, motor, perceptual, sensory, intellectual, and mental characteristics, using audiovisual resources when appropriate, so as to provide the necessary information to parents or legal guardians and information appropriate for the child's understanding." BRAZIL. Law No. 13,709, of August 14, 2018. General Personal Data Protection Law (LGPD). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: Apr. 29, 2026. ▸ p. 54

Appendix I

Summary table – Key concepts

Concept	Note
Provider of an information technology product or service	▸ An entity subject to compliance with the obligations set forth in the Digital ECA, regardless of the location, development, manufacture, offering, marketing, and operation of the service or product; ▸ In general, any provider that renders services or markets products in the digital environment, subject to requirements regarding targeting or likely access by children and adolescents; ▸ The identification criterion is functional in nature and is guided by the purpose and impact of the service or product, regardless of the technology used; ▸ Asymmetric treatment based on (i) the degree of interference with the product, (ii) the number of users, and (iii) the size of the provider.
Information technology product or service	▸ Product or service: (i) provided remotely, (ii) by electronic means (even if the device also contains a physical component), and (iii) provided upon individual request (without prejudice to shared use); ▸ A service may be provided in exchange for direct compensation paid by the user or through indirect forms of compensation, such as in the case of advertising-based services; ▸ This does not include broadcasting services, telemarketing, or services provided in a physical setting or with the simultaneous presence of the parties.

Concept	Note
Social network	▸ An internet application whose primary purpose is the sharing and dissemination by users of opinions and information conveyed through text or image, audio, or audiovisual files on a single platform, via accounts that are connected or accessible in an integrated manner, allowing users to connect with one another; ▸ It should not be confused with other interpersonal communication platforms, such as private messaging services (when used for private communications) or closed meetings.
App stores	▸ Internet applications that distribute and facilitate the download, for device users, of internet applications made available or accessible through their platform; ▸ They are characterized by acting as intermediaries in the distribution of internet applications through download/installation, connecting users with manufacturers and developers; ▸ They should not be confused with marketplaces or games or applications that allow in-app purchases; ▸ Together with operating systems, they play a structural role in the implementation of the Digital ECA, especially in the implementation of age assurance mechanisms. Both serve as a central connection point between developers and end users, proving essential in the digital application chain.

Concept	Note
Operating Systems	▸ System software that controls the basic functions of hardware or software and enables internet applications, computer programs, apps, or other software to run on them; ▸ Operating systems shape the user experience from the very first setup and continuously influence interaction with applications, making them essential in the digital application chain; ▸ The Digital ECA provides differentiated treatment based on the size and nature of the operating system provider, particularly for open-source and free software-based operating systems or operating systems used in closed environments with limited provider intervention, adopting a risk-based regulatory approach guided by the principle of proportionality.
Services with editorial control and copyright-protected content	▸ Internet applications whose primary purpose is to make previously selected content available, without the use of automated selection methods, by a responsible economic agent; ▸ These presuppose prior human evaluation and curation of the content to be made available, as is generally the case on streaming platforms.

Concept	Note
Duty of prevention	▸ The legal obligation of providers of information technology products or services to act proactively and diligently by adopting appropriate, proportionate, and effective measures that, throughout the life cycle of the products and services, prevent or mitigate risks of violations of the rights of children and adolescents and protect their best interests; ▸ A regulatory model focused on risk prevention and the comprehensive protection of children and adolescents in the digital environment; and ▸ The duty of prevention (in the broad sense) has four dimensions: › *Prevention in the strict sense:* the duty to prevent risks to the privacy, safety, and health of children and adolescents in the digital environment; › *iProtection:* the duty to ensure the comprehensive, special, and priority protection of children's and adolescents' rights in the digital environment, guided by their best interests; › *Information:* the duty to provide simple, clear, accessible, and appropriate information about products and services—prospectively, regarding operating and usage conditions, as well as the risks involved, the security measures adopted, and other factors that influence users' choices and protection; and retrospectively, through the publication of the semiannual transparency reports provided for in Article 31; and

Concept	Note
	› *Safety:* the duty to prevent the occurrence of accidental or unlawful situations that result in the improper processing of children's and adolescents' personal data, or that impact their life, health, and physical and psychological well-being.

Appendix II

Summary table – Likely access

The requirements for likely access set forth in Article 1, sole paragraph, of the Digital ECA are **cumulative**, subject to the following: (i) respect for **the principle of the best interests** of the child and adolescent; (ii) **legal presumption** of likely access for the categories of providers set forth in the Digital ECA and Decree No. 12,880/2026; and (iii) **relevant evidence** indicating a greater likelihood of meeting the requirements that constitute the concept of likely access.

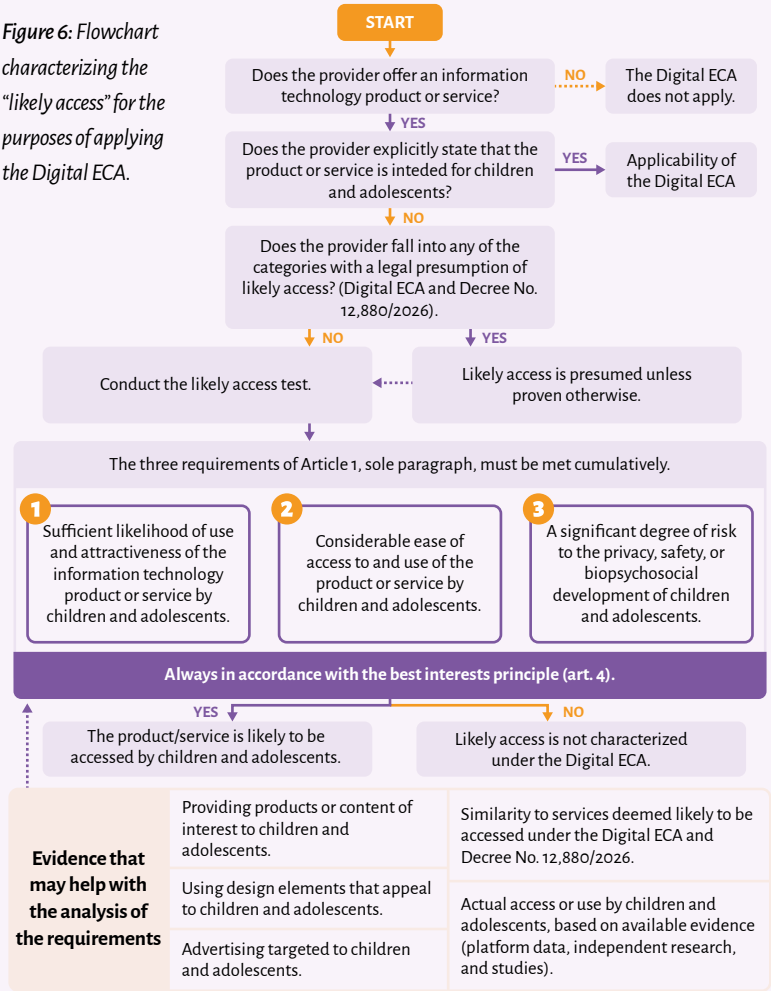
Requirements	Note
Likelihood of Use and Attractiveness	▸ This relates to the characteristics of a given product or service that make its use desirable to children and adolescents, even if it is not specifically targeted at or is formally prohibited for this audience; ▸ It involves the ability of the design, content, and presentation strategies of a given information technology product or service to arouse the interest of children and adolescents.
Ease of Access and Use	▸ Technical, operational, and contextual conditions that reduce barriers to accessing and using the product or service;

Requirements	Note
	▸ This involves the technological architecture, delivery mechanisms, interaction interface, operational flows, and user experience elements that structure the functioning of the product or service, its usability, and other elements that may prevent or reduce practical barriers to access or use by children or adolescents; ▸ Features or adaptations for accessibility purposes do not, on their own, determine likely access; rather, the architecture, usability, interaction flows, and other elements of the product or service must be considered.
Significant risk to privacy, safety, and biopsychosocial development	▸ Significant negative effects resulting from the use of a product or service, taking into account the probability of occurrence and the potential severity of the consequences; ▸ Legal presumption of significant risk in the case of products and services that enable social interaction and large-scale information sharing; ▸ Emphasis on the 4Cs methodology (contact, contract, content, and conduct); ▸ Risk mitigation measures may modulate obligations and the duty of prevention, but they do not exempt a service from being classified as likely to be accessed by children.

Appendix III

Likely access test

Figure 6: Flowchart characterizing the "likely access" for the purposes of applying the Digital ECA.



Categories with a legal presumption of likely access or targeting
Social media
App stores
Operating systems
Services with editorial control
Electronic games
Adult content providers
Generative artificial intelligence systems
E-commerce platforms that facilitate the purchase and sale of products and services prohibited for children and adolescents

IMPORTANT

The provider's self-assessment is not binding. The ANPD may—based on legal criteria, the principle of the best interests of children and adolescents, and the specific characteristics of the product or service— reach a different conclusion and require compliance with the provisions of the Digital ECA, including the differentiated treatment provided for in Articles 34 and 39. The applicability of the law does not depend solely on the provider's declaration nor on formal classifications of the target audience.

Differentiated Treatment: The obligations set forth in Articles 6, 17, 18, 19, 20, 27, 28, 29, 31, 32, and 40 of the Digital ECA shall apply in accordance with the characteristics and functionalities of the information technology product or service, modulated according to the degree of interference of the provider of the product or service over the content made available, the number of users, and the size of the provider.



www.gov.br/anpd

