Digital ECA: What constitutes probable access?

Authors:

Matheus Botsman Kasputis
| Attorney in the Data Governance team at b/luz

Thiago Xavier Peregrino
| Attorney in the Data Governance team at b/luz

Revisors:

Felipe Gabriades
| Partner in the Data Governance team at b/luz

Fernando Bousso
| Coordinating Partner of the Technology, Data Governance, and Media & Entertainment teams at b/luz

b/luz

b/luz

Table of Contents

Introduction

The Digital Statute of the Child and Adolescent ("Digital ECA") represents a milestone in the consolidation of duties of care and specific responsibilities for platforms, applications, and online services operating in Brazil. Its enactment occurs in a context of intensified regulatory and judicial activity over the digital ecosystem, with growing scrutiny of practices involving data collection and use, recommendation and engagement mechanisms, targeted advertising, content moderation, and the design of features that may expose children and adolescents to risks. In this environment, the protection of children and adolescents ceases to be treated as a sectoral issue and becomes more structurally integrated into the broader digital governance agenda.

Despite its legitimate purpose and the social urgency that drove its approval, the application of the Digital ECA presents a regulatory challenge that is still under development. A significant portion of its concepts will depend on interpretative consolidation, technical parameters, and, above all, supplementary regulation. This becomes particularly sensitive with respect to the criterion of "probable access," which is used to define the scope of application of the law beyond services explicitly directed at children and adolescents. The absence of consolidated objective criteria increases the risk of divergent interpretations, with significant practical implications for product strategies, investments, business models, and regulatory risk management.

This material aims to contribute to this debate from a technical and pragmatic perspective. On the one hand, it seeks to situate the Digital ECA within a broader global regulatory context, highlighting legislative references and international trends that influenced its drafting and public policy choices. On the other hand, it intends to offer a balanced reading of what may be understood as "probable access" in the context of the law, with particular attention to the need for verifiable, risk-oriented criteria capable of ensuring predictability.

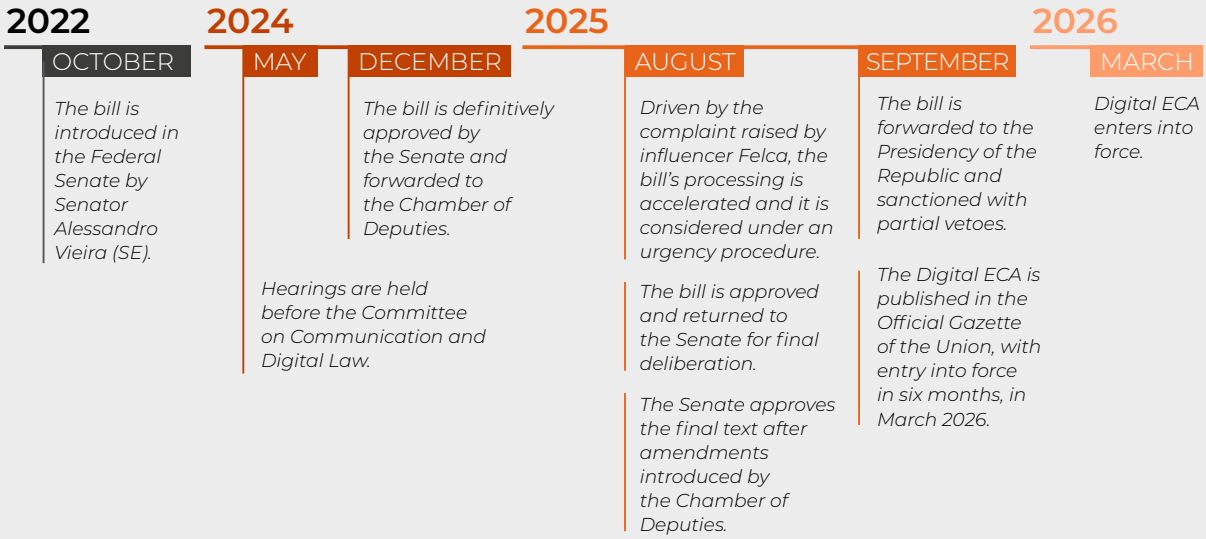
The objective is to support an application that preserves the protective core of the regime while avoiding expansive interpretations that transform the concept of probable access into a general presumption, thereby generating regulatory overload and adverse effects on innovation and the development of digital services.

1. Legislative History of the Digital ECA

In October 2022, amid growing concern regarding the risks associated with the digital experiences of children and adolescents, including exposure to inappropriate content, excessive or improper collection of personal data, and abusive advertising practices, Bill No. 2,628/2022[1] was introduced in the Federal Senate by Senator Alessandro Vieira (SE). The proposal, which sought to establish the Digital Statute of the Child and Adolescent, would be converted three years later into Law No. 15,211/2025[2].

From its earliest stages, the bill was developed under strong influence from public debate and contributions from organized civil society. It also formed part of a broader regulatory movement shaped by recent international trends, such as the consolidation of accountability frameworks and duties of care in the European Union, through the Digital Services Act (DSA)[3], and in the United Kingdom, through the Online Safety Act (OSA)[4], both of which repositioned the protection of minors as a central axis of digital governance.

However, it was only in August 2025, when digital influencer Felipe "Felca" Bressanim released a video exposing cases of sexual exploitation and the sexualization of children on the internet[5], that the issue gained nationwide prominence. The public reaction to the episode mobilized society and placed pressure on the National Congress to prioritize the matter. In this context, a favorable environment emerged for the expedited processing of the Digital ECA.



1 BRAZIL. Federal Senate. **Bill No. 2,628/2022**. Provides for the protection of children and adolescents in digital environments. Federal Senate, Brasília, DF, 2022. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9205524&ts=1758309711126&disposition=inline. Accessed on February 19, 2026.

2 BRAZIL. **Law No. 15,211, of September 17, 2025**. Provides for the protection of children and adolescents in digital environments (Digital Statute of the Child and Adolescent). Official Gazette of the Union, Brasília, DF, 2025. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Accessed on February 19, 2026.

3 EUROPEAN UNION. **Regulation (UE) 2022/2065** of the European Parliament and of the Council, of October 19, 2022. On a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union, Brussels, 2022. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Accessed on February 19, 2026.

4 UNITED KINGDOM. **Online Safety Act 2023 Chapter 50**. An Act to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes. The Stationery Office, London, 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/50. Accessed on February 19, 2026.

5 FELCA. **Adultification**. Youtube, August 6, 2025. Available at: https://www.youtube.com/watch?v=FpsCzFGL1LE. Accessed on February 19, 2026.

1.1. Proceedings in the Federal Senate

In the Federal Senate, Bill No. 2,628/2022 initially proceeded through the traditional committees but gained renewed momentum with the creation of the Committee on Communication and Digital Law, to which it was reassigned in 2024. Within this new forum, the matter was extensively debated through hearings that brought together representatives from the public sector, private sector, and organized civil society, as well as experts in data protection and children's rights. This process resulted in a substitute text that consolidated the main pillars of the original proposal and was approved on a terminative basis at the end of 2024.

During this stage, key discussions focused on: **(i)** the need for effective age verification mechanisms; **(ii)** the prohibition of behavioral advertising targeted at children and adolescents; **(iii)** the imposition of privacy and security by default settings; **(iv)** the responsibility of digital platforms in preventing systemic risks; and **(v)** the articulation of the new framework with the Brazilian General Data Protection Law.

The approval in the Federal Senate reflected broad consensus regarding the urgency of the matter and the adequacy of its principles-based approach. However, although there was convergence regarding the need for regulatory updates, the legislative process revealed relevant tensions, particularly concerning the degree of state intervention in platform architecture, the design of age verification mechanisms, and the boundaries between obligations imposed on companies and the preservation of rights such as privacy and freedom of expression.

1.2. Proceedings in the Chamber of Deputies

After being received by the Chamber of Deputies at the end of 2024, the bill was assigned to several thematic committees, with particular emphasis on the Committee on Communication. Throughout 2025, the text was the subject of intense debate, with dozens of amendments introduced and specific hearings held. During this period, the legislative debate began to incorporate more explicit concerns related to the mental health of children and adolescents, the design of digital platforms, and the sexualization of online content.

In August 2025, the legislative process accelerated significantly due to the public repercussions of allegations involving the exploitation of minors in digital environments, which led to the approval of an urgency procedure. The bill was considered directly by the Plenary of the Chamber of Deputies, which approved a comprehensive substitute text[6] that preserved the core pillars of the proposal, such as the prohibition of loot boxes, the requirement for parental supervision tools, the ban on profiling for advertising purposes, and the provision of administrative sanctions, while incorporating targeted adjustments negotiated among party leadership.

6 BRAZIL. Chamber of Deputies. **Final wording of the Substitute Bill of the Chamber of Deputies to Senate Bill No. 2,628-A of 2022. Substitute Bill of the Chamber of Deputies to Senate Bill No. 2,628 of 2022**, which "Provides for the protection of children and adolescents in digital environments." Chamber of Deputies, Brasília, DF, 2025. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2986940&filename=-Tramitacao-PL%202628/2022. Accessed on February 19, 2026.

1.3. Approval and Presidential Assent

As the text approved by the Chamber of Deputies contained certain differences from the original version passed by the Federal Senate, the bill returned to the initiating chamber in August 2025, where it was approved swiftly and without substantial modifications.

The bill was then forwarded for presidential assent and was enacted as Law No. 15,211 of September 17, 2025, with partial vetoes concentrated on three main points: **(i)** the direct attribution of powers to ANATEL to implement blocking measures, due to an alleged defect of legislative initiative; **(ii)** the permanent allocation of fines to the National Fund for Children and Adolescents, due to budgetary concerns; and **(iii)** the assessment that the one year vacatio legis was excessive in light of the urgency of the protection sought. This last point proved particularly relevant, as it resulted in the reduction of the period for the law's entry into force to six months, through a provisional measure issued by the Executive Branch and later converted into Law No. 15,352/2026.

With its official publication on September 17, 2025, the period for regulated entities to adapt to the new legal obligations began, marking the transition of the Digital ECA from the legislative sphere to the phase of implementation and practical application, under the supervision of the ANPD as the autonomous administrative authority responsible for the protection of children and adolescents in digital environments[7]. At this stage, the definition of the scope of application of the statute becomes particularly relevant, as it does not apply only to products and services "directed" at children and adolescents, but also to those of "probable access", a central concept for understanding the practical reach of the obligations imposed and which will be examined in the following chapter.

7 BRAZIL. **Decree No. 12,622/2025**. Regulates Law No. 15,211 of September 17, 2025, designating the Agência Nacional de Proteção de Dados as the autonomous administrative authority responsible for the protection of children and adolescents in digital environments, and establishing competences for the enforcement of judicial blocking orders. Official Gazette of the Union, Brasília, DF, 2025. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Decreto/D12622.htm. Accessed on February 19, 2026.

2. The Concept of Probable Access

The Digital ECA adopts, as a structural element of its scope of application, the notion that protection obligations are not limited to products and services "directed" at children and adolescents. Instead, the legislator opted for a broader criterion, also applicable to information technology services that are of "probable access" by children and adolescents. This legislative choice has immediate practical relevance, since a significant portion of the platforms and applications used by children and adolescents are not formally presented as products for children or youth, but rather as services designed for general audiences. In this context, the legislator's understanding was that conditioning the application of the law solely on explicit targeting would, to a large extent, allow products and services with strong appeal and high risk to escape the protective framework.

The term "probable access" appears in the very provision that defines the scope of application of the Digital ECA, establishing that the law applies to any information technology product or service "directed at children and adolescents in the country or of probable access by them." The statute further details the concept by indicating that probable access is considered to exist when the following situations are present:

- a sufficient probability that children and adolescents will use or be attracted to the product or service;
- considerable ease of access and use by this audience; and
- a significant degree of risk to privacy, security, or biopsychosocial development, particularly in services involving social interaction and large-scale sharing.

From a comparative perspective, it is worth noting that the Brazilian concept is related to recent international discussions, particularly in the United Kingdom, where the notion has consolidated that certain platforms should be treated as accessible to minors when there is a relevant likelihood of use by this audience. However, the Digital ECA introduces an important distinction, as the legislator expressly linked the criterion of probable access to the level of risk that the service poses to the privacy, security, and biopsychosocial development of children and adolescents. In other words, the analysis does not concern only whether children may or tend to access a given service, but also whether such access, within the context of that product or platform, involves relevant risks that justify the reinforced application of the protective regime.

Although the legal text provides these criteria, their concrete application now begins to rely on initial regulatory parameters, particularly with respect to the distinction between self-declaration, age verification, and age estimation, as well as principles applicable to technical age assurance solutions. Even so, there remains considerable room for complementary regulation by the ANPD and for the development of stable interpretative approaches regarding evidentiary methodologies and thresholds for applicability.

2.1. Objective Elements for Characterizing Probable Access

The delimitation of "probable access" should be constructed based on objective and verifiable elements capable of providing predictability for companies while preserving the protective purpose of the Digital ECA. Although the legal text indicates relevant parameters, the practical application of the concept requires a methodology that avoids two symmetrical risks. On the one hand, the adoption of overly generic criteria may lead to the classification of virtually any publicly available service as one of "probable access," generating significant regulatory and cost implications without proportional gains in protection. On the other hand, an excessively demanding evidentiary threshold may empty the concept of its practical effect, encouraging merely formal strategies for the declaratory exclusion of minors without any material change in functionalities, access frictions, or the risk profile of the product.

In this context, the most appropriate interpretation tends to be one that treats probable access as the result of a cumulative and contextual assessment. The objective is not to identify a single decisive indicator, but rather a set of converging signals that allow a reasonable conclusion that children and adolescents are sufficiently likely to use the service, that access and use occur with considerable ease, and that, given the characteristics of the product, the level of risk to privacy, security, or biopsychosocial development is significant. This structure is particularly important because the Digital ECA expressly links probable access to risk, which excludes interpretations based solely on popularity or mere technical accessibility.

The first group of evidence concerns the declared target audience and the positioning of the service. Descriptions in app stores, institutional webpages, terms and policies, age ratings, as well as the way in which the company presents the product to the market, constitute a relevant starting point. Although such declarations are not conclusive on their own, they contribute to the assessment when compared with the actual functioning of the service. In other words, it is the consistency between what is declared and what is effectively delivered that gives substance to the criterion, rather than labeling alone.

The second group relates to language, design, and engagement mechanisms embedded in the product. Interfaces strongly oriented towards gamification, frequent rewards, progression systems, collectibles, recurring challenges, aesthetics and language typically associated with younger audiences, as well as flows centered on continuous consumption, rapid recommendation, and retention stimuli, are relevant indicators of attractiveness. The same reasoning applies to the predominant type of content and the curation tools used, particularly where there are high cadence algorithmic feeds, autoplay features, or recommendation systems that expand exposure to content and interactions without the user exercising informed and gradual choices.[8]

8 This interpretation is consistent with the ANPD's position regarding the risks to children and adolescents arising from access to feeds without prior registration that would allow the identification of the minor and the application of the appropriate protective measures to ensure the safety of this group.

The third group of evidence concerns ease of access and use. Here, the relevant factor is less the abstract possibility of access and more the presence or absence of effective frictions that discourage minors from entering sensitive functionalities. Among other aspects, the analysis should consider whether the service allows meaningful browsing and uses without registration, which data are required at sign up, the existence of social login mechanisms that reduce friction, the point in the user journey at which age is requested, and, above all, the robustness of verification mechanisms. Barriers based solely on self-declaration, without controls proportionate to the associated risk, tend to carry little weight when the product is attractive and allows broad interaction. By contrast, age verification mechanisms and the segmentation of functionalities, when consistently designed and supported by technical documentation, may be relevant in reducing the likelihood of use by minors in higher risk areas.

The fourth group involves marketing and communication strategies. Campaigns with influencers whose audience is predominantly composed of adolescents, advertising language oriented toward school references or youth culture, activations in digital environments with a high concentration of minors, and incentives for virality and peer referral may reinforce the conclusion that the service, although general purpose, is in practice captured by this audience. It is important, however, that this assessment be grounded in evidence rather than assumptions. The analysis should focus on demonstrable commercial intent and on the acquisition channels effectively used.

The fifth group, central to the rationality of the regime, concerns the level of risk associated with functionalities and with the model for processing personal data. Services featuring open social interaction, direct messaging, groups, live streaming, profile search and discovery, automated recommendations of people and content, large scale sharing, public exposure of attributes and metadata, or extensive integration with third parties generally increase the level of criticality. Similarly, models based on behavioral advertising, profiling, extensive collection of usage signals, and intensive personalization tend to amplify risks and reduce the room to argue that access by minors is merely incidental or peripheral. This link to risk is precisely what prevents the conclusion that the entire internet would, by definition, constitute an environment of probable access.

For operational purposes, it is possible to consider adopting a two-step assessment approach. In the first step, the probability and ease of use by minors are examined based on signals of attractiveness and access frictions, relying on observable and documentable evidence. In the second step, the materiality of risk is assessed, considering the functionalities effectively available prior to any age verification and the data processing architecture associated with those functionalities. This structure favors proportionate decision making, enables the internal prioritization of measures, and reduces uncertainty in interactions with regulators and the market. The operationalization of this analysis also tends to consider the architecture for the circulation of age signals among different actors in the digital ecosystem, including providers, app stores, operating systems, and browsers, insofar as such mechanisms increasingly become objective elements in the evaluation of access frictions and the age appropriateness of the service.

In the same vein, evidence management is an important component of compliance. Aggregated data regarding the age composition of audiences, when obtained lawfully and governed appropriately, usage reports, journey analyses, records of product decisions concerning controls and barriers, and impact assessments focused on children and adolescents are useful instruments for demonstrating diligence. It is also particularly important to clearly distinguish what is functionally accessible without barriers from what depends on verification, as this distinction is often decisive in characterizing risk and, consequently, in determining whether probable access exists.

HYPOTHETICAL CASES

Some hypothetical situations illustrate how the combination of factors may alter the conclusion.

CASE 1: a short video sharing application, with an algorithmic feed, comments, direct messages, and content creation tools, allows full use without age verification mechanisms and invests in influencers whose audience is largely composed of adolescents. Even if it describes itself as "for everyone," the combination of high attractiveness, low access friction, and high associated risk indicates a tendency toward characterization as a service of probable access.

CASE 2: a corporate productivity platform designed for teams requires a corporate email address for registration, offers functionalities centered on project management, does not include public social components, and does not engage in behavioral advertising. Although adolescents could theoretically create accounts using personal email addresses in certain contexts, the typical low attractiveness for this audience, combined with access friction and reduced risk, tends to exclude the characterization of probable access.

CASE 3: a free mobile game with strong gamification elements, group chat, and in app purchases, classified as "12+" in the app store, with significant user acquisition through social media and no effective age controls for access to chat or public profile exposure. In this scenario, attractiveness is high, friction is low, and risk is significant, particularly due to social interaction and monetization. The tendency is toward classification as probable access, requiring proportionate measures, including with respect to verification design and interaction controls.

CASE 4: a general news portal, with predominantly textual content, no comment features, and no intensive personalization, relying on contextual advertising and simple audience measurement mechanisms. Adolescents may consume the content, but the risk level is lower, and the nature of the service reduces specific attractiveness. The characterization of probable access would depend on additional signals, such as deliberately youth-oriented language, the presence of sections strongly aimed at adolescents, or acquisition strategies clearly directed at this audience.

In summary, the characterization of probable access should rely on a set of converging factors and on a risk-oriented analysis, avoiding generic presumptions. This interpretation preserves the effectiveness of the Digital ECA while also contributing to a more predictable and proportionate regulatory environment, in which enhanced measures are prioritized where there is in fact a higher likelihood of use by minors and greater exposure to relevant risks, without indiscriminately imposing burdens incompatible with low-risk business models or with services that implement effective frictions and controls.

2.2. Protective Purpose versus Risks of Expansive Interpretation

The development of objective criteria for characterizing probable access cannot be separated from the purpose that guides the Digital ECA. The protection of children and adolescents in the digital environment constitutes a central interpretative vector and imposes on economic actors an enhanced duty of caution whenever there is relevant risk to privacy, security, or biopsychosocial development. This premise, however, does not eliminate the need for interpretative restraint.

An interpretation that excessively expands the concept of probable access, bringing it closer to the mere abstract possibility of access, tends to undermine the distinction outlined in the previous section between qualified probability and simple technical accessibility. If every service available on the internet is considered, by definition, to be of probable access to minors, the criterion ceases to function as an instrument of regulatory differentiation and instead becomes a general rule applied indiscriminately.

The first effect of such expansion is legal uncertainty. Companies that structure products for adult audiences, adopt proportionate entry barriers, and do not present converging signals of attractiveness to minors may nonetheless be classified as subject to a more burdensome regime, without clear parameters defining the threshold at which possibility becomes probability. Regulatory predictability, an essential element for investment decisions and product design, becomes compromised.

There are also direct impacts on compliance costs. Treating low risk services as equivalent to services with open social interaction, strong algorithmic components, or behavioral advertising may impose complex and costly technical obligations indiscriminately. In practice, this raises barriers to entry and may contribute to market consolidation in favor of large platforms with sufficient resources to absorb such requirements. Rather than expanding protection, the result may be reduced diversity and competition.

Another relevant aspect concerns innovation. Digital environments depend on rapid cycles of experimentation, functional adjustments, and testing of engagement models. If mere technical accessibility by minors is sufficient to trigger a regulatory regime entirely oriented toward childhood and adolescence, companies may respond by restricting functionalities, limiting interactions, or even discontinuing services in the Brazilian market as a way of mitigating regulatory risk. Protection would no longer be calibrated according to concrete risk but rather determined by the fear of broad liability.

This scenario may also generate an additional interpretative distortion. In order to avoid classification as a service of probable access, economic actors may adopt merely formal strategies of declaratory exclusion without any material change to the product's architecture. The incentive becomes documentary rather than structural. Paradoxically, this weakens the protective objective itself, as the focus shifts from the effective reduction of risk to the construction of defensive narratives.

The protective purpose of the Digital ECA is better served when the concept of probable access functions as a mechanism of regulatory prioritization. Services that present converging

signals of attractiveness to minors, relevant ease of use, and high levels of risk should indeed be subject to reinforced obligations. Conversely, when the probability of use is residual and the risk is low or mitigated through consistent access frictions, the automatic application of a stricter regime tends to be disproportionate.

Adopting an interpretation oriented toward risk, cumulative factors, and contextual analysis allows the protective core of the statute to be preserved without transforming it into a clause of universal application. This approach promotes systemic coherence, reduces uncertainty, and encourages investment in governance and effective controls rather than merely formal solutions. Ultimately, the protection of children and adolescents is strengthened when the law differentiates situations carefully and proportionately, avoiding both the trivialization of the concept and its practical neutralization

2.3. Adoption of Reasonable Measures and the Logic of Due Diligence

Once the objective elements for characterizing probable access have been defined and the risks of expansive interpretations recognized, it becomes necessary to address a central point: how the company's concrete conduct should influence the legal assessment. The analysis cannot be limited to the structure of the product alone. It must also consider the standard of diligence adopted in preventing and mitigating risks.

In the digital environment, the absolute elimination of the possibility of access by minors is, in most cases, technically unfeasible or disproportionate. Age verification systems present well known limitations, whether because they depend on self-declaration or because they require the collection of additional data, with relevant impacts on privacy and user experience. Requiring infallibility may, in practice, amount to establishing a standard that cannot realistically be met.

In this context, the legal assessment should follow a model of reasonable diligence. The central question is no longer whether any improper access occurred, but whether the company structured its service and its controls in a manner consistent with the risks identified. The analysis therefore focuses on the coherence between risk diagnosis, product design, mitigation measures, and internal governance.

This standard aligns with the logic already consolidated in the field of personal data protection and in the regulatory practice of the ANPD, where a risk-based approach and the demonstration of accountability are emphasized. The elimination of all residual risk is not required. Rather, the expectation is that technical and administrative measures that are proportionate to the risk are adopted, documented, and periodically reviewed. The same rationale can and should guide the application of the Digital ECA.

In this framework, diligence involves at least four dimensions. The first is prior risk assessment, with clear identification of functionalities potentially sensitive to children and adolescents and of the stages of the user journey where access is most likely to occur. The second is the implementation of proportionate frictions and functional segmentation that

restrict or adapt critical features before any robust age verification takes place. The third is ongoing governance, including monitoring of aggregated metrics, review of controls, and updating of policies considering evidence regarding patterns of use. The fourth is documentation capable of demonstrating, in a consistent manner, the decisions taken and the technical grounds that supported them.

It is also important to distinguish isolated failures from structurally inadequate design. The existence of residual access, particularly when resulting from deliberate user behavior, should not automatically lead to the conclusion that the service is of probable access or that regulatory obligations have been breached. A different situation arises when the product architecture disregards evident risks, maintains sensitive functionalities openly accessible, and relies on merely symbolic barriers. In such cases, the absence of diligence reinforces the legal characterization.

By incorporating the logic of diligence, the concept of probable access ceases to be purely descriptive and begins to interact with the conduct of the economic actor. This does not mean weakening the protection of children and adolescents but rather making it operational. Companies that invest in governance structures, impact assessments, usability testing focused on risk, and effective mechanisms of functional segmentation should have these efforts considered in the legal analysis.

This approach creates appropriate incentives. Instead of encouraging purely formal strategies of declaratory exclusion, it promotes structural interventions in product design, continuous improvement of controls, and transparency in risk management. Protection thus becomes anchored in concrete and verifiable practices rather than broad presumptions.

In summary, the adoption of reasonable and proportionate measures should play a central role in the application of the Digital ECA. The criterion of probable access cannot be dissociated from the standard of diligence demonstrated by the company. This interpretation preserves the protective purpose of the statute while avoiding the imposition of a liability regime based on technical impossibility, thereby contributing to a more stable and functional regulatory environment.

3. Conclusion and Paths Toward Legal Certainty

The concept of probable access occupies a central position in the Digital ECA and will be decisive for the practical scope of its obligations. The development of legal certainty will depend, mostly, on the consolidation of objective criteria, the stabilization and complementarity of regulatory guidance, and institutional dialogue among regulators, the Judiciary, the private sector, and civil society. An approach grounded in risk, proportionality, and prior diligence tends to offer a more stable and functional path.

Protecting children and adolescents in the digital environment does not necessarily require a generalized interpretation of the statute. While excessively broad interpretations may appear to strengthen protection, they may also produce unintended effects, such as the disproportionate restriction of children's and adolescents' access to legitimate digital products and services, with negative consequences for their educational, social, and cultural development.

In this context, the interpretation of the scope of application of the Digital ECA must be careful and technically grounded, in order to reconcile protection, innovation, and the sustainable development of the digital ecosystem.

b/luz

www.baptistaluz.com.br/