AGE ASSURANCE MECHANISMS IN DIGITAL ENVIRONMENTS: TECHNICAL OPTIONS, LEGAL LIMITS AND PROPORTIONALITY CRITERIA

Jessica Fernandes Rocha [*]

Abstract: Age assurance in digital environments has become a central issue in contemporary regulation, particularly considering the need to protect children and adolescents from inappropriate or prohibited content, products and services without overlooking the impact of such measures on privacy, personal data protection, inclusion and non-discrimination. Drawing on guidance issued by Brazil's data protection authority, the Agência Nacional de Proteção de Dados ("ANPD"), the regulatory framework surrounding the Brazilian Digital Child and Adolescent Statute, and recent European regulatory and institutional references, this article examines the main mechanisms currently available, organizing them into categories and analyzing their functioning, advantages, and limitations. Based on this framework, the article argues that the legal legitimacy of such mechanisms does not derive solely from their technical capacity to verify age, but also from their regulatory purpose, practical effectiveness and compatibility with principles such as data minimization, purpose limitation, security, inclusion and proportionality. It concludes that there is no universally superior solution in the abstract and that the choice of mechanism should be guided by the specific risk posed by the service and by the pursuit of solutions capable of proving only the necessary age-related attribute, with the lowest possible level of intrusion upon users' rights.

Keywords: Age assurance; Personal data protection; Child protection online; Digital environments; Proportionality.

INTRODUCTION

The regulation of the protection of children and adolescents in digital environments requires a balance between equally relevant objectives: on the one hand, preventing exposure to inappropriate or prohibited content, products and services; on the other, preserving privacy, personal data protection and non-discriminatory access to digital services. In the Brazilian context, Law No. 15,211, of September 17, 2025, also known as "ECA Digital"[1], reinforced the centrality of this issue by requiring reliable and effective age assurance mechanisms within a framework oriented toward risk prevention and the comprehensive protection of

[*] Master of Laws, Federal University of Minas Gerais, Brazil. Email: jrocha@viseu.com.br / ORCID iD: https://orcid.org/0009-0003-4985-9086

[1] Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Lei nº 15.211, de 17 de setembro de 2025*. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Diário Oficial da União, seção 1, edição extra, Sep. 17, 2025. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (last visited Mar. 30 2026).

children and adolescents.[2]

The comprehensive protection of children and adolescents, with the best interests principle at its core, has assumed an increasingly relevant role not only in the debate inaugurated by the ECA Digital[3], but also, more broadly, in the personal data protection regime. In Brazil, this guideline was expressly reinforced by Precedent CD/ANPD No. 1, of 22 May, 2023[4], by establishing that the processing of children's and adolescents' personal data may be based on the legal grounds set out in Articles 7 or 11 of Brazil's General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, "LGPD"),[5] provided that their best interests are observed and prevail, to be assessed in the specific case, pursuant to Article 14 of the Law.

In the same sense, the concept of likely access, around which relevant obligations under the ECA Digital are structured, also reinforces a more realistic regulatory reading of the presence of children and adolescents in digital environments.[6] Instead of proceeding from the implausible premise that this public would be absent from, or only exceptionally present in, these spaces, the regime comes to recognize their concrete participation in digital dynamics, including it as a dimension related to the

---

[2] Agência Nacional de proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. p. 5. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026).

[3] As provided in the caput of Article 5, information technology products or services intended for this public, or likely to be accessed by them, must be "*in accordance with the principle of the best interests of the child and the adolescent"*. Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Lei nº 15.211, de 17 de setembro de 2025*. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Diário Oficial da União, seção 1, edição extra, Sep. 17, 2025. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (last visited Mar. 30 2026).

[4] Brazil. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Conselho Diretor. *Enunciado CD/ANPD nº 1, de 22 de maio de 2023*. Brasília: Diário Oficial da União, seção 1, ed. 98, p. 129, May 24, 2023. Available at https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf (last visited Mar. 30, 2026).

[5] Dispelling restrictive interpretations that would, in absolute terms, limit such processing to the consent of legal guardians. Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Lei nº 15.211, de 17 de setembro de 2025*. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Diário Oficial da União, seção 1, edição extra, Sep. 17, 2025. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (last visited Mar. 30 2026).

[6] Data Privacy Brasil. Roda de Conversa | Implementando o ECA Digital: como operacionalizar o conceito de acesso provável. 1 vídeo (1h51min). *YouTube*, Mar. 11, 2026. Available at https://www.youtube.com/watch?v=LIGKPwrBWds&t=5314s (last visited Mar. 30, 2026).

development of their digital citizenship.[7]

Along the same lines, purely formal solutions lose force, such as generic provisions in terms of use, isolated age restriction notices or self-declarations unaccompanied by measures minimally compatible with the concrete risk of access by children and adolescents. In a digital environment known by recognized widespread use, device sharing and the ease with which merely declaratory barriers can be circumvented, the regulatory sufficiency of these strategies becomes questionable. It is precisely at this point that the discussion of age assurance mechanisms gains central relevance: the legal issue ceases to be whether the platform states, in the abstract, that the service is not intended for minors, and becomes whether it has adopted an effective, proportionate measure compatible with personal data protection to address the concrete risk of likely access by this public.

The concept of "likely access", in turn, occupies a central position in the logic of the ECA Digital and is defined in Article 1, sole paragraph, of the Law, which considers, in an interdependent manner: (i) the likelihood of use of, and the attractiveness of, the product or service to children and adolescents; (ii) the concrete ease of access and use by this public; and (iii) the significant degree of risk to their privacy, safety or biopsychosocial development.

In this sense, the regulatory focus shifts from the company's stated intention or the formally indicated target audience to the notion of "likely access". In other words, the analysis no longer relies only on formal classifications, generic statements or the abstract destination attributed by the platform to the service, but instead centers on the reality of the digital environment based on the concrete likelihood that children and adolescents will access a given content, product or functionality.

On a practical level, however, the adoption of age assurance mechanisms must consider that different methods offer different levels of reliability and impose different impacts on privacy, data minimization, inclusion and non-discrimination.[8] For that reason, the choice of the legally appropriate mechanism depends not only on its technical capacity for age control, but also on its adherence to the regulatory purpose, its

[7] It should be noted that, under Article 4, item VIII of the ECA Digital, the *"promotion of digital education, with a focus on the development of citizenship and critical thinking for the safe and responsible use of technology"* is established as one of the Law's underlying principles. Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Lei nº 15.211, de 17 de setembro de 2025*. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Diário Oficial da União, seção 1, edição extra, Sep. 17, 2025. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (last visited Mar. 30 2026).

[8] The processing of the personal data of children and adolescents is permitted for the legitimate purposes of protecting, organizing, and ensuring compliance within the digital environment, but this does not authorize excessively intrusive solutions or solutions dissociated from the criteria of necessity, proportionality and best interests.

practical effectiveness and its compatibility with data protection principles.

The ANPD, in turn, emphasizes that both the risks associated with the use of the service or product itself and the risks associated with the age assurance mechanism to be adopted must be considered.[9] It is against this background that the regulatory function of age assurance, the main mechanisms currently available and the legal criteria that may help guide such a choice are examined next.[10]

I. AGE ASSURANCE IN DIGITAL ENVIRONMENTS AS AN INSTRUMENT OF PROTECTION AND REGULATION

Age assurance, in the context of the ECA Digital, should be understood less as an isolated registration requirement and more as an instrument for giving effect to a regulatory model oriented toward risk prevention and the comprehensive protection of children and adolescents in the digital environment. It is precisely within this framework that the ANPD situates the issue when it states that the new regime is based on a logic of proactive and diligent action by providers to prevent and mitigate risks, especially in products and services directed at this public or likely to be accessed by it.[11] In this regard, the requirement for "reliable" and "effective" mechanisms emerges as a development of the broader duty of protection provided for in the ECA Digital and detailed in its regulation[12].

The material "Perguntas e respostas sobre o ECA Digital", for example, makes clear that the law did not prohibit access by children and adolescents to electronic games, nor did it adopt, in the case of social networks, a solution based on a pure and simple ban. The emphasis falls on parental supervision, account linking in certain situations, segregated service versions where appropriate and the requirement of age assurance for access to content that is actually prohibited. This reinforces the idea that age assurance operates as an instrument of proportionate regulation, inserted into a broader architecture of protective measures and

---

[9] Agência Nacional de Proteção de dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 8.

[10] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements. Last visited Mar. 31, 2026. p. 23-27; European Data Protection Board (EDPB). *Statement 1/2025 on Age Assurance*. *Adopted on 11 Feb. 2025*. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211 ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026). p. 1-2.

[11] Agência Nacional de Proteção de Dados (ANPD). *op. cit.,* p. 5.

[12] *Ibid*., p. 4-5.

citizenship-building, not as a mechanism intended indiscriminately to exclude underage persons from these environments. [13]

It is also important to clarify that age assurance is not the same as identity verification, since its purpose is not to identify the user in civil terms, but only to confirm the age-related attribute required by the regulatory context, in proportion to the risk and with the least possible intrusion.[14] The document "Privacy guidance on age assurance technologies", issued by the Office of the Australian Information Commissioner, for example, maintains that age assurance mechanisms should not serve as an indirect route to the user's unnecessary civil identification and should, whenever practicable, be compatible with the preservation of anonymity or pseudonymity after the age check.[15]

Therefore, the solution's design should, as far as possible, be limited to confirming the relevant age or age range, avoiding the collection, retention and circulation of excess data, as well as the association between civil identity and access history. In those terms, age assurance performs a specific regulatory function: to enable decisions to block, condition or modulate access to content, products and services according to the risks they represent for children and adolescents and not to promote broad identification of the user.

It is also important to distinguish age assurance from age ratings. Whereas age ratings retain a predominantly informational character, age assurance corresponds to the set of tools capable of restricting access, for example, to pornography, alcoholic beverages, betting or other content and products prohibited or unsuitable for minors. From this perspective, self-declaration ceases to be regarded as sufficient in many contexts precisely because it does not, on its own, ensure the protective effectiveness that the law now requires.[16]

---

[13] Brazil. Secretaria de Comunicação Social da Presidência da República (SECOM/PR). Ministério da Justiça e Segurança Pública (MJSP). Agência Nacional de Proteção de Dados (ANPD). *Perguntas e respostas sobre o ECA Digital*. Brasília, DF: ANPD; MJSP; Secom/PR, 2026b. Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/perguntas_respostas_eca_digital_18032026.pdf (last visited Mar. 30, 2026). p. 5-7.

[14] Brazil. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. *Mecanismos de aferição de idade. Análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025*. Brasília: MJSP, 2026a. Available at https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf (last visited Mar. 30, 2026). p. 3.

[15] Office of the Australian Information Commissioner. *Privacy guidance on age assurance technologies*. Sydney: OAIC, 2026. Available at https://www.oaic.gov.au/__data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf (last visited Mar. 31, 2026). p. 5-6.

[16] Brazil. Secretaria de Comunicação Social da Presidência da República (SECOM/PR). Ministério da Justiça e Segurança Pública (MJSP). Agência Nacional de Proteção de Dados (ANPD). *Perguntas e respostas sobre o ECA Digital*. Brasília, DF: ANPD; MJSP; Secom/PR, 2026b. Available at https://www.gov.br/anpd/pt-br/centrais-

In this same context, researchers and authorities have stressed that age assurance may play distinct roles, especially between: (i) preventing minors from accessing content, products, or services subject to a minimum age requirement, in which case the mechanism operates as a genuine entry barrier and its effectiveness is measured, above all, by its ability to prevent improper entry into the service;[17] and (ii) allowing the application of protections, standards or functionalities adjusted to the user's age or age range, according to the risk involved.[18] This distinction is useful because it shows, more concretely, that the intensity and architecture of age assurance may vary according to the regulatory function performed by the mechanism, without altering its central premise of limiting itself, as far as possible, to the age-related attribute that is necessary.

This understanding is also aligned with recent European literature. The report "Mapping age assurance typologies and requirements" notes that the primary responsibility for ensuring appropriate age assurance mechanisms falls on digital service providers themselves and that the choice of method should be contextual and proportionate to the risk involved.[19] In the same direction, the European Data Protection Board (EDPB) notes that age assurance may be relevant both in situations in which a minimum age is prescribed by law and in contexts in which there is a duty of care to protect children and that its implementation must consider not only data protection but also the full set of fundamental rights involved and the best interests of the child as a primary consideration.[20]

It is therefore clear that age assurance has become established as a regulatory instrument of protection, but its legitimacy depends on remaining linked to a logic of necessity, proportionality and effective protection of rights, rather than to a merely formal claim of age control.

---

de-conteudo/documentos-tecnicos-orientativos/perguntas_respostas_eca_digital_18032026.pdf (last visited Mar. 30, 2026). pp. 2, 4, 8.

[17] Office of Communications; Information Commissioner's Office. *Age assurance: a joint statement by Ofcom and the Information Commissioner's Office*. London: Ofcom; ICO, 2026. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/joint-statement-from-ico-and-ofcom-on-age-assurance/ (last visited Mar. 31, 2026). p. 3.

[18] *Ibid*., p. 13-14.

[19] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 7, 34.

[20] European Data Protection Board (EDPB). *Statement 1/2025 on Age Assurance*. *Adopted on 11 Feb. 2025*. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026). p. 1-2.

II. MAIN AGE ASSURANCE MECHANISMS IN DIGITAL ENVIRONMENTS: CATEGORIES, OPERATION, ADVANTAGES, AND LIMITATIONS

Age assurance mechanisms do not form a homogeneous set. Article 2, IV of Decree No. 12,880 of March 18, 2026, which regulates the Brazilian Digital Child and Adolescent Statute, clarifies that "age assurance" refers to a "general term concerning procedures intended to verify, estimate or infer, directly or indirectly, the age or age range of a user"[21] and that it does so through different "methods, technologies and processes, including documentary, biometric and usage-pattern analysis, and other technically suitable means".[22]

This distinction is relevant because verification, estimation, and inference do not correspond merely to different technologies, but to distinct logics of age assurance, with different levels of certainty, intrusion and dependence on direct or indirect signals concerning the user's age. [23] In a similar sense, European literature treats age assurance as a broad expression for methods with different levels of certainty, encompassing self-declaration, verification, estimation and hybrid or outsourced arrangements.[24] More specifically:

(i) age verification seeks to confirm, with a higher degree of certainty, whether the user has the age required for a given access or, at least, whether the user is above or below a defined age threshold, usually with support from documents, verifiable credentials or validation by trusted third parties;[25] [26]

---

[21] Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Decreto nº 12.880, de 18 de março de 2026*. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília: Diário Oficial da União, 2026c. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Decreto/D12880.htm (last visited Mar. 30, 2026).

[22] *Ibid.*

[23] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos de aferição de idade*. Brasília: ANPD, 2025. (Radar Tecnológico, n. 5). Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf (last visited Mar. 11, 2026). p. 16.

[24] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 25-33.

[25] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 12.

[26] Also in accordance with Article 2, V of Decree No. 12,880 of 18 March 2026, which regulates the Brazilian Digital Child and Adolescent Statute. Brazil. Presidência

(ii) age estimation, in turn, does not intend to prove the exact age, but rather to approximate the user's age or probable age range based on elements such as biometrics, behavioural data or capacity tests;[27]

(iii) age inference operates through indirect and contextual signals that allow one to conclude, in a non-deterministic manner, that the user is probably above, below or within a certain age range, which is why it usually approximates estimation, although it emphasizes even more the dependence on usage patterns, digital context and other indirect evidence.[28]

In practical terms, therefore, the central difference lies in the fact that verification tends to rely on more direct and robust elements of age confirmation, whereas estimation and inference work with probabilities, approximations and indirect signals, generally with a lower degree of certainty and with their own risk profile as regards accuracy, intrusion and possible discriminatory effects.

The European report "Mapping age assurance typologies and requirements" identifies ten main methods of age assurance, namely: (i) self-declaration; (ii) hard identifiers; (iii) credit cards; (iv) self-sovereign identity; (v) account holder confirmation; (vi) cross-platform authentication; (vii) facial age estimation; (viii) behavioural profiling; (ix) capacity-testing; and (x) third-party age assurance services.[29] Although useful for showing the diversity of possible solutions, the document itself warns that this list is not exhaustive and that, in practice, platforms may resort to combinations of different mechanisms.

Although specialized literature details multiple specific methods, for didactic purposes it may be useful to organize these solutions into five categories, as explained in the following subtopics. This systematization facilitates legal assessment because it allows a clearer comparison of the level of reliability, degree of intrusion, potential for exclusion and adherence to the regulatory purpose, since the ANPD emphasizes that there is no universally appropriate mechanism, but rather one that is

---

da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. *Decreto nº 12.880, de 18 de março de 2026*. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília: Diário Oficial da União, 2026c. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Decreto/D12880.htm (last visited Mar. 30, 2026).

[27] Shaffique; Van Der Hof; Center for Law and Digital Technologies (eLaw). *op cit*., p. 12.

[28] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos de aferição de idade*. Brasília: ANPD, 2025. (Radar Tecnológico, n. 5). Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf (last visited Mar. 11, 2026). p. 24.

[29] Shaffique; Van Der Hof; Center for Law and Digital Technologies (eLaw). *op. cit*., p. 25-33.

appropriate to the particularities of the context. [30]

III. DECLARATORY MECHANISMS

In this category, age is ascertained based on information declared by the user, without the presentation of independent evidence capable of proving the accuracy of the information provided, the most common example being self-declaration of age or date of birth by the user. Its main advantage is low friction, associated with limited data collection and operational simplicity. Its central limitation, however, is structural: it is an easily manipulated method and, for that reason, one with a low degree of reliability, since it does not establish even a minimally secure link between the information declared and the user's real age.[31]

Both European literature and the ANPD converge in pointing out that solutions based exclusively on self-declaration do not offer sufficient robustness when the context requires effective protection, although they may have residual usefulness in low-risk scenarios or as an initial screening step for the application of additional controls.[32] In other words, it is a mechanism that may, in certain cases, form part of graduated age assurance architectures, but which, in isolation, tends to be incompatible with contexts in which the protection of children and adolescents depends on minimally reliable containment of access.

IV. EVIDENCE-BASED VERIFICATION MECHANISMS

In these methods, age is not extracted solely from the user's own

---

[30] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos de aferição de idade*. Brasília: ANPD, 2025. (Radar Tecnológico, n. 5). Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf (last visited Mar. 11, 2026). p. 7-9; Information Commissioner's Office (ICO). *Age assurance report technical annex*. Wilmslow: Information Commissioner's Office, 2024. Available at https://ico.org.uk/media2/migrated/4030925/20240704-ico-age-assurance-report-technical-annex.pdf (last visited 13 Mar. 2026). p. 2-5.

[31] Agência Nacional de Proteção de Dados (ANPD), *op. cit*., p. 27-28; Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 12-13.

[32] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 25; Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 12.

declaration, but is confronted with or confirmed by minimally verifiable external evidence, such as an official document, consultation of third-party databases, use of a credit or debit card, and, in some contexts, solutions linked to open banking.[33] These mechanisms tend to offer a degree of certainty greater than that of self-declaration and, for that reason, are often intuitively perceived as safer.

Even so, their adoption is not free from regulatory trade-offs: documentary verification, for example, may mean excessive data collection when the regulatory purpose requires only proof of an age range; and mechanisms based on financial instruments or banking relationships may exclude users who do not have access to those tools. In practical terms, this is a category suited to higher-risk contexts, but its legitimacy depends on a concrete analysis of the proportionality between the level of certainty obtained and the cost imposed in terms of privacy, inclusion, and data exposure.[34]

V. PRE-EXISTING RELATIONSHIP OR ACCOUNT-BASED CONFIRMATION MECHANISMS

In this category, age assurance does not begin with a new autonomous check performed by the platform itself, but rather with the use of a pre-existing relationship, account or registration considered more reliable, such as confirmation by the primary account holder, parental supervision with account linking, cross-platform authentication, or, in some contexts, checks based on a pre-existing relationship with mobile operators.[35]

In some architectures, age assurance may also rely on age signals provided by layers of digital infrastructure, such as operating systems and app stores, including by means of APIs or other native interfaces of operating systems, browsers and digital ecosystems, through which the application receives only the age-related evidence required, without directly handling the user's raw data.[36] This same logic also encompasses

---

[33] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 26-27; Information Commissioner's Office (ICO). *Age assurance report technical annex*. Wilmslow: Information Commissioner's Office, 2024. Available at https://ico.org.uk/media2/migrated/4030925/20240704-ico-age-assurance-report-technical-annex.pdf (last visited 13 Mar. 2026). p. 2-3.

[34] *Ibid*., p. 26-27.; *Ibid*., p. 2-3.

[35] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 27-28.

[36] Brazil. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. *Mecanismos de aferição de idade. Análise das contribuições à consulta pública*

hybrid architectures in which the digital infrastructure provides a preliminary age signal, without exhausting the need for contextual assessment by the application itself in higher-risk situations.

Its main advantage, especially where there is re-use of a relationship or age signal already previously established elsewhere in the digital ecosystem, is to reduce repetitive friction and allow integrated or interoperable solutions,[37] especially in family ecosystems or services with segmented age profiles.[38] On the other hand, confirmation by a responsible adult is not always appropriate in contexts in which parental involvement may compromise the adolescent's privacy; and cross-platform authentication may intensify dependence on large digital intermediaries and informational concentration.[39]

Moreover, when age assurance depends on infrastructure layers of the device itself or of the digital ecosystem, its usefulness may be reduced in situations in which the device is shared among different people or when access occurs through browsers, applications or environments that do not receive or do not recognize that age signal.[40] In other words, the usefulness of these mechanisms presupposes that the age signal supplied by the digital infrastructure sufficiently tracks the person who is actually accessing the service.[41]

They are, therefore, useful mechanisms in specific contexts, but poorly suited to function as a general or undifferentiated solution.[42] Their appropriateness tends to be greater when there is reasonable reliability in the pre-existing relationship or in the infrastructure issuing the age signal, as well as when the context of use allows a presumption of relative

---

e subsídios para regulamentação da Lei nº 15.211/2025. Brasília: MJSP, 2026a. Available at https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf (last visited Mar. 30, 2026). p. 12-13.

[37] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026).

[38] Shaffique; Van Der Hof; Center for Law and Digital Technologies (eLaw), *op. cit*., p. 27-28.

[39] *Ibid*., p. 28-29.

[40] Brazil. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. *Mecanismos de aferição de idade. Análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025*. Brasília: MJSP, 2026a. Available at https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf (last visited Mar. 30, 2026). p. 12-13, 46.

[41] This assumption may fail in contexts involving shared devices or when access takes place through technical environments that do not receive or do not recognize the same signal, thereby reducing the solution's reliability and practical coverage.

[42] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 26.

stability between the registered profile and the user who is actually accessing the service.

VI. ESTIMATION OR INFERENCE MECHANISMS

These techniques include facial age estimation, voice estimation, behavioral inference, digital-footprint analysis and capacity tests.[43] Unlike evidence-based verification, here age is not directly proven, but estimated based on physical, behavioral or contextual signals. In essence, the system does not merely ask "how old are you?" nor does it necessarily require a document, but instead seeks to approximate the answer based on indicia, such as facial traits captured by a camera, browsing patterns, interaction history, the way the account is used or the user's performance in challenge questions.

Its main advantage lies in the possibility of reducing the need for formal documentation and, in some cases, offering a more fluid experience. That apparent fluidity, however, is offset by the fact that the age-related conclusion comes to depend on probabilistic models, training data, and statistical correlations, rather than on direct proof of age. In this regard, this is also the category that concentrates some of the strongest regulatory reservations.

The ANPD records caution regarding solutions based on facial biometrics due to risks of surveillance, algorithmic bias and the collection of sensitive data,[44] while European literature calls attention to opacity, accuracy problems, profiling risks and discriminatory impacts, especially in mechanisms based on behavioral inference.[45] Regulatory concerns fall both on the precision of the result and on the volume of signals processed, the risk of secondary uses and the unequal effects that these mechanisms may produce in practice.

As a consequence, although these methods may appear technologically sophisticated, their legal support depends on a particularly rigorous analysis of the necessity, proportionality and safeguards adopted. In practical terms, this means that their use tends to

---

[43] *Ibid*., p. 29-33; Information Commissioner's Office (ICO). *Age assurance report technical annex*. Wilmslow: Information Commissioner's Office, 2024. Available at https://ico.org.uk/media2/migrated/4030925/20240704-ico-age-assurance-report-technical-annex.pdf (last visited 13 Mar. 2026).

[44] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 9.

[45] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 29-31.

be more difficult to sustain when less intrusive alternatives exist that are capable of producing an equivalent result with lower risk to privacy, data protection, inclusion and non-discrimination.

VII. ATTRIBUTE-PROOF ARCHITECTURES AND THIRD-PARTY SERVICES

Finally, this category covers age assurance providers, self-sovereign identity[46], verifiable credentials[47], reusable digital wallets[48], age tokens[49] and cryptographic techniques aimed at proving only the necessary attribute, without displaying excess information.[50] Within this group, it is useful to distinguish: (i) cryptographic tokens, which operate as digital signals that a certain age requirement has been met; (ii) double-blind models, structured so that the different participants in the ecosystem do not have complete visibility over the information and cannot easily trace it among themselves; and (iii) zero-knowledge proofs (ZKPs), which make it possible to prove that the user meets the age requirement without revealing the underlying data used for that proof. [51]

This category is especially relevant because it allows, at least in theory, proof only that the user is above or below a certain age threshold, without sharing the full date of birth, a document, or other unnecessary identifiers. For that reason, both the ANPD and European authorities treat

---

[46] Self-sovereign identity (SSI) can be understood as a model in which the user retains, in their own digital wallet, credentials issued by trusted entities and uses them to prove only a specific attribute, such as being over a certain age, without disclosing the full set of identifying data to the service.

[47] Verifiable credentials may be understood as digital credentials that make it possible to prove a specific attribute in a manner whose authenticity can be verified by third parties.

[48] Reusable digital wallets are digital tools that store credentials and allow them to be presented again in different contexts.

[49] Age tokens are signals or digital credentials issued for the sole purpose of proving a relevant age-related attribute, such as being above or below a certain age.

[50] Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 33; Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 16, 24-26; Information Commissioner's Office (ICO). *Age assurance report technical annex*. Wilmslow: Information Commissioner's Office, 2024. Available at https://ico.org.uk/media2/migrated/4030925/20240704-ico-age-assurance-report-technical-annex.pdf (last visited 13 Mar. 2026). p. 3.

[51] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos de aferição de idade*. Brasília: ANPD, 2025. (Radar Tecnológico, n. 5). Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf (last visited Mar. 11, 2026). p. 33-35.

it as a particularly promising direction from the standpoint of data minimization and privacy. Even so, such solutions are not automatically appropriate, since their concrete design must avoid tracking[52], excessive sharing, informational concentration and secondary use of data by the third party involved.[53]

VIII. LEGAL LIMITS AND PROPORTIONALITY CRITERIA FOR CHOOSING AGE ASSURANCE MECHANISMS IN LIGHT OF DATA PROTECTION

The choice of an age assurance mechanism in digital environments requires an analysis that considers not only its capacity for age control, but also the regulatory costs and impacts associated with the solution adopted. This is the central point of the ANPD's guidance, which places age assurance within a risk-management logic in which the solution adopted must be proportionate both to the risk associated with the service and to the effects of the mechanism itself on privacy, data protection, inclusion and non-discrimination.[54]

In a convergent sense, the EDPB states that age assurance must be implemented in a proportionate, risk-based manner; and always by means of the least intrusive alternative among those capable of achieving the intended regulatory purpose.[55] This means that the legally relevant question is not which mechanism appears strongest in the abstract, but which solution is necessary and sufficient for the specific context.

One of the most significant legal benchmarks is purpose limitation (Article 6(I)), which the LGPD includes among its principles and defines as "processing for legitimate, specific and explicit purposes of which the

---

[52] Tracking, in this context, consists in the possibility of reconnecting, monitoring, or correlating the use of the age assurance mechanism across different instances of access, services, or actors involved, thereby making it possible to extract more information about the user than is strictly necessary to confirm the age-related attribute.

[53] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 25-26; Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). *Research report: Mapping age assurance typologies and requirements*. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026). p. 33.

[54] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 7-10.

[55] European Data Protection Board (EDPB). *Statement 1/2025 on Age Assurance. Adopted on 11 Feb. 2025*. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026). p. 2-3.

data subject is informed, with no possibility of subsequent processing that is incompatible with such purposes"[56]. Age assurance may justify data processing because it aims to restrict, condition or modulate access according to the user's age range, not because it authorizes, by itself, a new cycle of collection for commercial, registration or analytical purposes.

The ANPD expressly states that data collected for age assurance may be used only for that purpose, prohibiting secondary use, traceability and the continuous, automated or unrestricted sharing of personal data.[57] Along the same lines, the EDPB observes that age assurance mechanisms must not open space for additional identification, profiling, tracking or other processing disconnected from age verification itself.[58]

The second limit is data minimization, which requires restricting the processing to the age-related attribute necessary for the relevant context of use, a safeguard reflected in the LGPD through the principle of necessity (Article 6(III)), which limits processing to "limitation of the processing to the minimum required for the accomplishment of its purposes, encompassing relevant, proportional and non-excessive data in relation to data processing purposes."[59] For that reason, the ANPD's guidance values solutions capable of proving only whether the user meets the applicable age requirement, without exposing the full date of birth, document number or other unnecessary identifiers, mentioning verifiable credentials and zero-knowledge proofs as relevant examples in this direction.[60]

A third important legal filter concerns the security of the data processed, likewise enshrined in the LGPD (Article 6(VII)) as a principle requiring the "use of technical and administrative measures able to protect

---

[56] Brazil. Agência Nacional de Proteção de Dados. *Law No. 13,709 of August 14, 2018*. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019). Brasília: ANPD, 2018. Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf (last visited Apr. 1, 2026).

[57] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 14-18.

[58] European Data Protection Board (EDPB). *Statement 1/2025 on Age Assurance*. *Adopted on 11 Feb. 2025*. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026). p. 3-4.

[59] Brazil. Agência Nacional de Proteção de Dados. *Law No. 13,709 of August 14, 2018*. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019). Brasília: ANPD, 2018. Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf (last visited Apr. 1, 2026).

[60] Agência Nacional de Proteção de Dados (ANPD). *op. cit*., p. 16.

personal data from unauthorized accesses and accidental or unlawful events of destruction, loss, alteration, communication or dissemination"[61] - especially when the mechanism involves biometrics or other more sensitive information. In those cases, the ANPD indicates that the use of the solution requires a more robust justification as to necessity and appropriateness, mainly if there are less intrusive alternatives capable of producing an equivalent result.[62]

The EDPB adds that the intensity of the interference with rights and freedoms may, in many scenarios, justify the prior carrying out of a data protection impact assessment.[63] It is also relevant to verify the mechanism's technically demonstrable effectiveness: proportionality is not the same as choosing the solution that appears least invasive, but rather the least invasive solution that is still sufficient for the risk faced. For that reason, the ANPD separates proportionality from accuracy, robustness and reliability, warning that solutions based exclusively on self-declaration have a low degree of confidence and that the mechanisms adopted must have their performance documented and tested against fraud or material error.[64]

The criteria of inclusion, non-discrimination, transparency and contestability also form part of the proportionality assessment. The ANPD emphasizes that age assurance mechanisms must not result, directly or indirectly, in the disproportionate exclusion of users from digital life, drawing attention to barriers related to the absence of documents, socioeconomic vulnerability, motor or cognitive limitations and inequalities in access to devices and connectivity[65]. In the same direction, the EDPB expressly includes non-discrimination among the rights potentially affected by age assurance systems.[66]

For that reason, when the main solution imposes relevant obstacles to access or use, or may disproportionately affect certain groups, it is important to provide alternative or complementary means of age assurance, especially for people who belong to vulnerable groups.[67] In a convergent sense, such alternatives work as safeguards to reduce undue

---

[61] Brazil, *op. cit.*

[62] Agência Nacional de Proteção de Dados (ANPD). *op. cit*., p. 17-18.

[63] European Data Protection Board (EDPB). *Statement 1/2025 on Age Assurance*. *Adopted on 11 Feb. 2025*. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026). p. 2-3.

[64] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 19-20.

[65] *Ibid*., p. 11-13.

[66] European Data Protection Board (EDPB), *op. cit*., p. 2.

[67] Agência Nacional de Proteção de Dados (ANPD), *op. cit*., p. 20.

exclusions and to reconcile the protection of children and adolescents with the requirements of proportionality, effectiveness and respect for fundamental rights, especially when the method originally adopted depends on an appropriate document, a compatible telephone or other requirements that not all users are able to meet.[68]

Lastly, it should be observed that the ANPD's guidance recommends providing clear information on the purpose of the age assurance mechanism, the data used and the consequences of the assessment, as well as ensuring the availability of channels to challenge decisions and correct errors, which is particularly relevant in the case of mechanisms susceptible to false positives or false negatives.[69] In summary, the legally defensible choice will depend on demonstrating, in documented form, that the mechanism is necessary in view of the risk, sufficient for the purpose, limited to the minimum data required, surrounded by appropriate safeguards and structured in a way that avoids tracking, discrimination and undue exclusion.

CONCLUSION

Age assurance in digital environments is not solved by the search for an abstractly or universally "more appropriate" mechanism, but by the choice of the solution that, in each context, offers a degree of reliability compatible with the regulatory risk involved, without imposing excessive processing of personal data or disproportionate restrictions on access. It is precisely for this reason that the sources examined reject uniform responses and indicate that the legitimacy of the mechanism depends on its adherence to the regulatory purpose, its practical effectiveness and its compatibility with principles of data protection laws such as minimization, purpose limitation, security and non-discrimination.

The comparison among the main age assurance mechanisms shows that self-declaration tends to be insufficient in high-risk contexts, displaying low robustness due to its vulnerability to attempts by users to circumvent it. It was also concluded that mechanisms based on the analysis of evidence, such as documents, third-party databases or financial instruments may offer a greater degree of certainty, but may also increase friction, data exposure and access difficulties for certain users. In turn, estimative or inferential methods, although at times presented as innovative solutions, concentrate relevant concerns related to opacity, bias, surveillance and the sensitivity of the data involved.

In this scenario, architectures that make it possible to prove only the

---

[68] European Data Protection Board (EDPB), *op. cit*., p. 6-7.

[69] Agência Nacional de Proteção de Dados (ANPD). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026). p. 23.

necessary age-related attribute, without excessive disclosure of identity or other personal data, gain prominence, especially when structured in a way that different actors in the ecosystem access only the information strictly necessary for their role, with secure communication of the age-related result and safeguards against tracking and secondary uses. It is precisely this relationship among reliability, intrusiveness and purpose that turns the classification of mechanisms into a useful tool for legal analysis and practical decision-making.

In legal terms, the decisive point is that proportionality, in this field, does not operate as an ancillary consideration, but as a true architectural criterion. The greater the risk associated with the content, product or service, the greater the degree of robustness that may be required of the mechanism, and even so, the solution adopted must remain strictly linked to the purpose of age assurance and limited to the minimum necessary to achieve it. The protection of children and adolescents in digital environments requires effective measures, but their legitimacy depends on those measures not turning protection into a pretext for excessive data collection, expanded tracking or undue exclusion of users.

REFERENCES

Agência Nacional de Proteção de Dados (ANPD). Mecanismos de aferição de idade. Brasília: ANPD, 2025. (Radar Tecnológico, n. 5). Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf (last visited Mar. 11, 2026).

Agência Nacional De Proteção de Dados (ANPD). Mecanismos confiáveis de aferição de idade: orientações preliminares. Brasília: ANPD, 2026. Available at https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@download/file (last visited Mar. 25, 2026).

Brazil. Agência Nacional de Proteção de Dados. Law No. 13,709 of August 14, 2018. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019). Brasília: ANPD, 2018. Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf (last visited Apr. 1, 2026).

Brazil. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Conselho Diretor. Enunciado CD/ANPD nº 1, de 22 de maio de 2023. Brasília: Diário Oficial da União, seção 1, ed. 98, p. 129, May 24, 2023. Available at https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf (last visited Mar. 30, 2026).

Brazil. Presidência da República. Casa Civil. Secretaria Especial para

Assuntos Jurídicos. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Diário Oficial da União: seção 1, edição extra, Sep. 17, 2025. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (last visited Mar. 30 2026).

Brazil. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. Mecanismos de aferição de idade. Análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025. Brasília: MJSP, 2026a. Available at https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf (last visited Mar. 30, 2026).

Brazil. Secretaria de Comunicação Social da Presidência da República (SECOM/PR). Ministério da Justiça e Segurança Pública (MJSP). Agência Nacional de Proteção de Dados (ANPD). Perguntas e respostas sobre o ECA Digital. Brasília, DF: ANPD; MJSP; Secom/PR, 2026b. Available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/perguntas_respostas_eca_digital_18032026.pdf (last visited Mar. 30, 2026).

Brazil. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. Decreto nº 12.880, de 18 de março de 2026. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília: Diário Oficial da União, 2026c. Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Decreto/D12880.htm (last visited Mar. 30, 2026).

Data Privacy Brasil. Roda de Conversa | Implementando o ECA Digital: como operacionalizar o conceito de acesso provável. 1 vídeo (1h51min). YouTube, Mar. 11, 2026. Available at https://www.youtube.com/watch?v=LIGKPwrBWds&t=5314s (last visited Mar. 30, 2026).

European Data Protection Board (EDPB). Statement 1/2025 on Age Assurance. Adopted on 11 Feb. 2025. Brussels: EDPB, 2025. Available at https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf (last visited Mar. 13, 2026).

Information Commissioner's Office (ICO). Age assurance report technical annex. Wilmslow: Information Commissioner's Office, 2024. Available at https://ico.org.uk/media2/migrated/4030925/20240704-ico-age-assurance-report-technical-annex.pdf (last visited 13 Mar. 2026).

Office of Communications; Information Commissioner's Office. Age assurance: a joint statement by Ofcom and the Information

Commissioner's Office. London: Ofcom; ICO, 2026. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/joint-statement-from-ico-and-ofcom-on-age-assurance/ (last visited Mar. 31, 2026).

Office of the Australian Information Commissioner. Privacy guidance on age assurance technologies. Sydney: OAIC, 2026. Available at https://www.oaic.gov.au/__data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf (last visited Mar. 31, 2026).

Shaffique, Mohammed Raiz; Van Der Hof, Simone; Center for Law and Digital Technologies (eLaw). Research report: Mapping age assurance typologies and requirements. Luxembourg: European Commission, 2024. Available at https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements (last visited Mar. 31, 2026).

* * *

Jessica Fernandes Rocha
Senior Lawyer in Privacy, Data Protection, and AI Governance at Viseu Advogados, holding the international certifications "Artificial Intelligence Governance Professional" (AIGP), "Certified Information Privacy Manager" (CIPM) and "Data Protection Officer Certified in Brazil" (CDPO/BR) from the International Association of Privacy Professionals (IAPP). Holds both a Bachelor of Laws and a Master of Laws from the Federal University of Minas Gerais (UFMG). Specialist in Digital Labor Law, Labor Compliance and the LGPD. Author of chapters in legal books, researcher at the UFMG Study Group on Law and Technology (DTec-UFMG) and member of the Data Protection Committee of the OAB/MG.
Email: jrocha@viseu.com.br
ORCID iD: https://orcid.org/0009-0003-4985-9086

10.59224/bjlti.v4i1.54-74
ISSN: 2965-1549