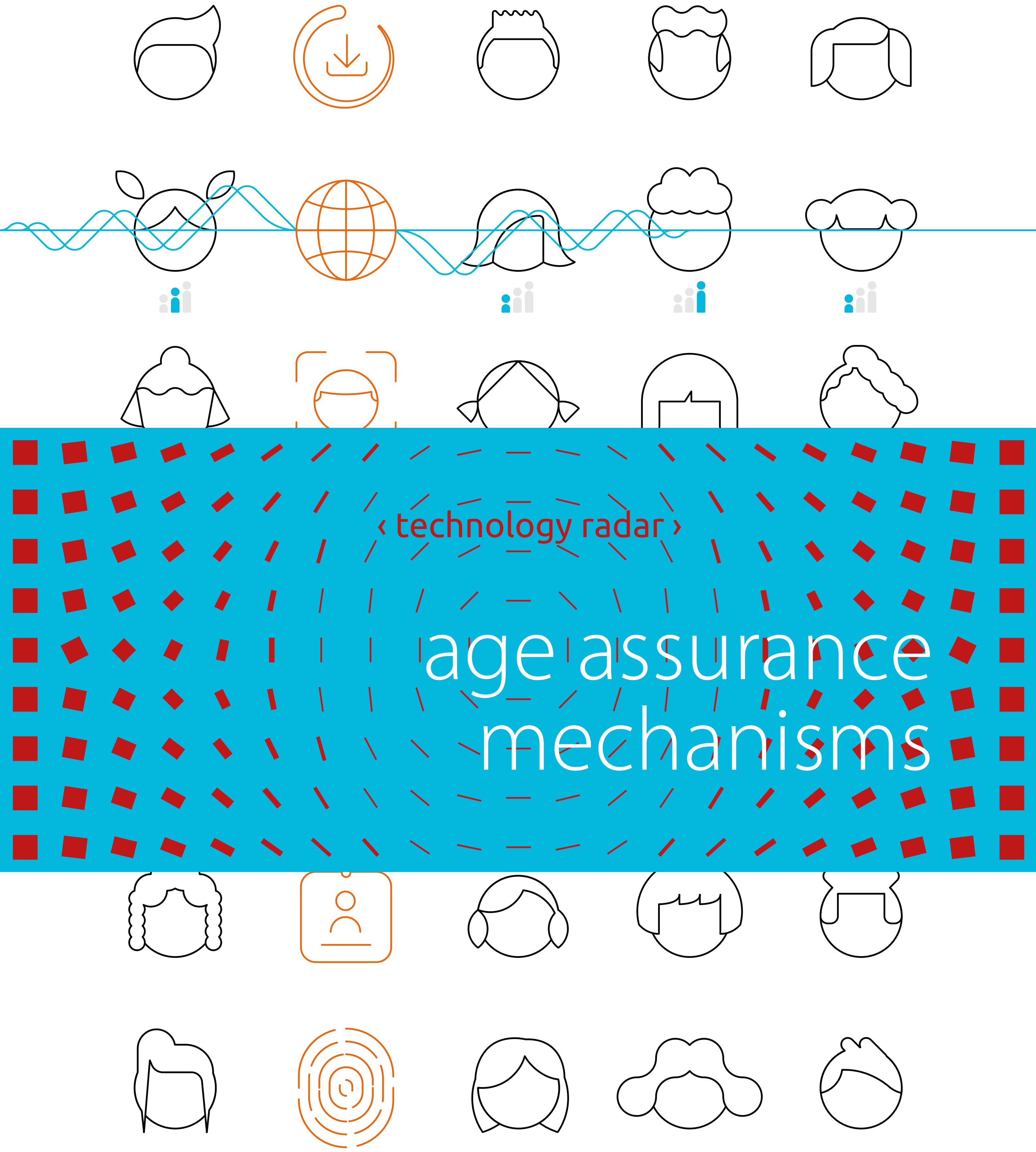


‹ technology radar ›

age assurance mechanisms

ANPD

National Data Protection Agency

‹ technology radar ›

No. 5

age assurance mechanisms

Edgard Costa Oliveira
Roseane Salvio
Jayme Marrone Júnior

ANPD
Brasília, DF
2026

ANPD – National Data Protection Agency

Director-President
Waldemar Gonçalves Ortunho Junior

Directors
Arthur Pereira Sabbat
Iagê Zendron Miola
Lorena Giuberti Coutinho
Miriam Wimmer

Authors and translators
General Coordination of Technology and Research (CGTP)
Edgard Costa Oliveira
Roseane Salvio
Jayme Marrone Júnior

Coordination and review
Lucas Costa dos Anjos
Gustavo Andrade Bruzzeguez
Adi Balbinot Junior
Albert Franca Josua Costa
Angela Halen Claro Franco
Igor Polezi Munhoz

Graphic design / desktop publishing / cover
André Scofano Maia Porto

Infographics
Ewerton Luiz Costadelle

1st edition
Digital publication – PDF
Technology Radar, Number 5, FEB 2026

ANPD
SCN, Qd. 6, Conj. A, Ed. Venâncio 3000, Bl. A, 9th floor
Brasília, DF · Brazil · Zip Code: 70716-900
t. +55 (61) 2025-8101 · www.gov.br/anpd

ISBN: 978-65-82658-01-3

How to cite this publication:

ANPD. **Age assurance mechanisms**. Brasília, DF: ANPD, 2026. (Technology Radar, n.5). Available at: include document link. Accessed on: include date of access to the document.

‹ about the series ›

The "Technology Radar" series is a periodic publication by ANPD that aims to provide concise overviews of emerging technologies that will impact or are already impacting the national and international data protection landscape.

The purpose of the series is to provide relevant information for the debate on data protection in Brazil, with texts structured in an educational manner that is accessible to the wider public, without the intention of exhausting the topics or establishing institutional positions.

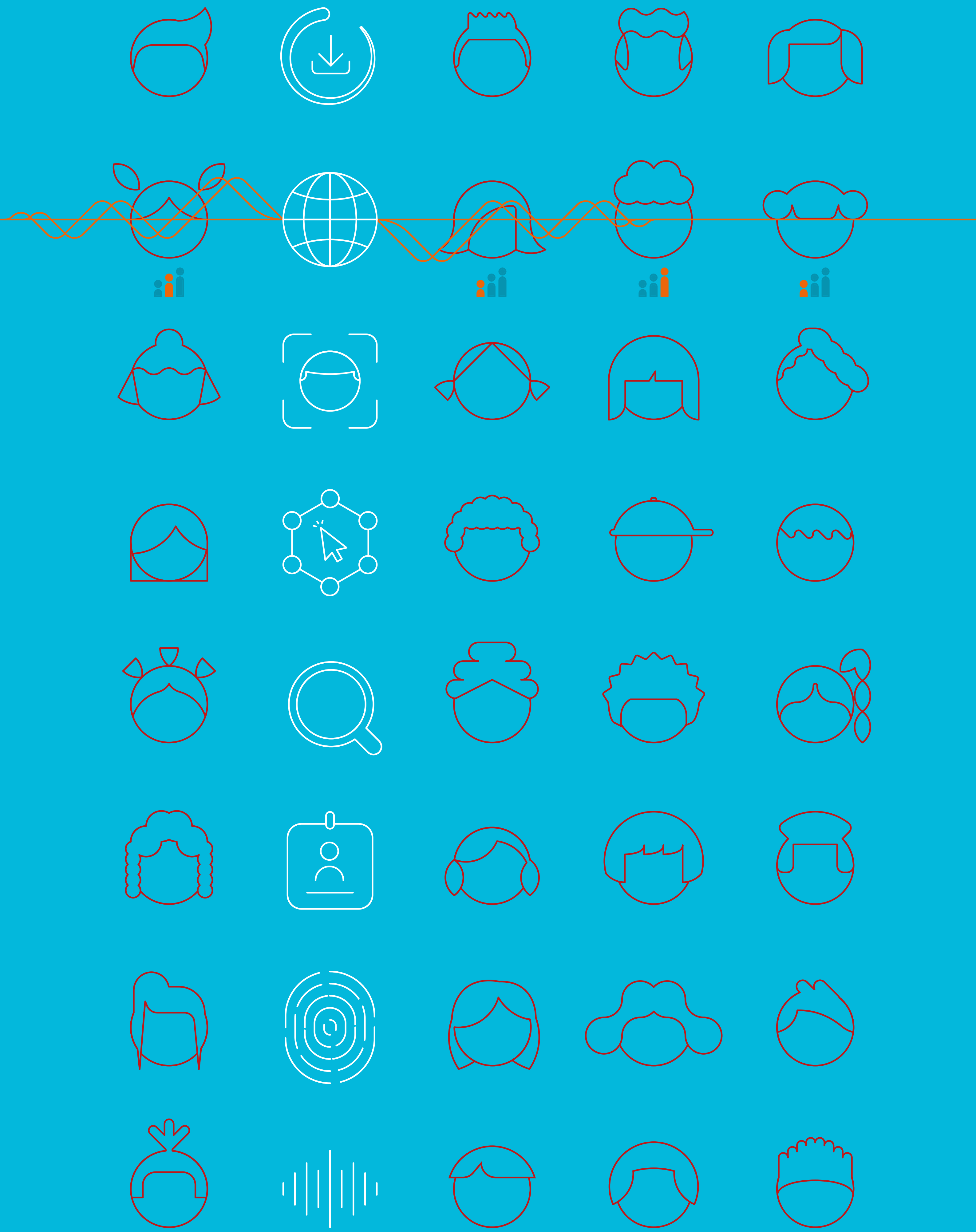
For each topic, the main concepts, potentialities, and prospects are addressed, with a special emphasis on data protection in the Brazilian context. ■

‹ list of abbreviations and acronyms ›

AATT – Age Assurance Technology Trial
ACCS – Age Check Certification Scheme
AEPD – Spanish Data Protection Agency
AI – Artificial Intelligence
API – Application Programming Interface
ARCOM – Audiovisual and Digital Communication Regulatory Authority
AVPA – Age Verification Providers Association
AVS – Age Verification Systems
BBFC – British Board of Film Classification
BSI – British Standards Institution
CHAMPS – Children Amplified Prevention Services
CNIL – National Commission for Information Technology and Civil Liberties
CONANDA – National Council for the Rights of Children and Adolescents
CPF – Individual Taxpayer Registry
DPIAs – Data Protection Impact Assessments
ECA Digital – Digital Statute of the Child and Adolescent
ECA – Statute of the Child and Adolescent
EDPB – European Data Protection Board
EDRi – European Digital Rights
EFA – Electronic Frontiers Australia
EPRS – European Parliamentary Research Service
FOSI – Family Online Safety Institute
GDPR – General Data Protection Regulation
HEAA – Highly Effective Age Assurance
ICO – Information Commissioner's Office
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
ISO – International Organization for Standardization
LGPD – Brazilian Data Protection Law
MDHC – Ministry of Human Rights and Citizenship
MJSP – Ministry of Justice and Public Security
MNO – Mobile Network Operator

NLP – Natural Language Processing
OECD – Organization for Economic Co-operation and Development
OCR – Optical Character Recognition
Ofcom – Office of Communications
PEReN – Center of Expertise for Digital Platform Regulation
PNPDCAAD – National Policy for the Protection of Children and Adolescents' Rights in the Digital Environment
SEDIGI – Secretariat for Digital Rights
UN – United Nations
UNODC – United Nations Office on Drugs and Crime
VaaS – Verification as a Service
ZKP – Zero-Knowledge Proof

‹ summary ›



‹ introduction ›

Internet services and products, social networks, entertainment systems, games, education, health, and transportation—in other words, the digital environment as a whole—has provided society with opportunities to exercise citizenship, fundamental rights, lived experiences, knowledge acquisition, and access to extremely useful and diverse information to individuals.

Children and adolescents wish and need to have access to the digital environment, but this must be done in a way that best serves their interests, so that they are protected from the misuse of information not intended for their age groups. There is a risk of exposing children and adolescents to digital content that is inappropriate and harmful to their physical, emotional, psychological, and cognitive development, such as pornography, incitement to suicide, and self-harm. In addition, people in this audience may be subjected to harmful practices in the digital environment, such as cyberbullying[1], inappropriate contact with strangers, and blackmail via the use of personal data by sexual offenders. They may also be exposed to misleading or abusive advertising about gambling, cigarettes, weapons, alcoholic beverages, and other items inappropriate for children and adolescents.

In 2025, Brazil enacted Law No. 15,211/2025, which provides for the protection of children and adolescents in digital environments, also known as the Digital Statute of the Child and Adolescent (ECA Digital). The law establishes in its Article 10 that

> *Providers of information technology products or services directed at children and adolescents or likely to be accessed by them shall adopt mechanisms to provide age-appropriate experiences, in accordance with this Chapter, respecting the evolving capacities and diversity of Brazilian socioeconomic contexts (Brazil, 2025c).*

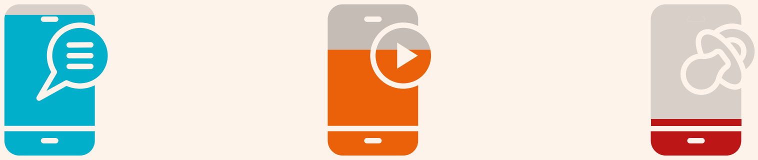
[1] *Cyberbullying is the virtual form of bullying, which is identified by* "repetitive intimidation among children and adolescents, but has its own characteristics, as it has a multiplier effect and large proportions when it occurs on the web" *(SaferNet, [2019]).*

Age assurance is the activity of identifying and confirming a person's age, whether a child, adolescent, or adult, with the aim of verifying or estimating if they are of a certain age to enter digital environments, social networks, electronic games, or to restrict or authorize the sale of restricted products. The result of age assurance is to allow access to the digital environment based on the child's minimum age so that they will only access age appropriate content, as well as to prevent adults from posing as children and illegally interacting with them.

To assure user's age, there are specific mechanisms used to verify and estimate age through various available applications. They play a special role in protecting children and adolescents in digital environments, due to the growing number of users in this age group who use products and services on the Internet.

The 11th edition of the TIC Kids Online Brazil survey, carried out by Cetic.br/NIC.br, found out that 93% of the population between 9 and 17 years old are Internet users in Brazil (NIC.BR, 2024, p. 21). The survey also revealed new findings on the frequency of use of digital platforms by children and adolescents: more than half of the surveyed population between the ages of 9 and 12 have access to messaging and video and photo sharing platforms "several times a day" or "every day or almost every day." On average, 70% are frequent users of one of the available video platforms (NIC.BR, 2024, pp.22, 67).

The same survey, conducted in 2023, showed that a quarter of those interviewed started accessing the Internet before the age of 6, most of them via cell phone, but also via television, and a minority via computer (NIC.BR, 2023, p. 27). The survey also revealed that, in Brazil, 68% of those between 9 and 10 years old have a profile on at least one of the digital platforms surveyed, and this number rises to 82% among young people aged 11 to 12, and 99% among young people aged 15 to 17 (NIC.BR, 2023, p. 30).



93%

of 9-to-17-year-olds are on the Internet

data from TIC Kids Online Brazil survey (NIC.BR, 2024, p.21) about the frequency and use of digital platforms by children and adolescents

70%

of 9-to-12-year-olds are frequent users

reporting that they access a video platform “several times a day” or “every day or almost every day”

24%

had their first access before the age of 6

mostly via mobile phones, but also via television and, to a lesser extent, via computers (NIC.BR, 2023, p.27)

Figure 1 *Percentages of child users on the Internet.*

Source: own elaboration based on NIC.BR (2023)

The Brazilian Data Protection Law (LGPD) reflects concerns about the protection of personal data and the privacy of children and adolescents in digital environments. Section III of Chapter II of the law is dedicated to this vulnerable group (Brazil, 2018). The regulatory agenda of the National Data Protection Agency (ANPD) for the 2025-2026 biennium, focuses on the processing of children and adolescents’ personal data, including the following topics: (i) the principle of best interests; (ii) consent provided by parents and legal representative; (iii) the collection of information by Internet games and applications; (iv) the transparency of operations carried out with the personal data of children and adolescents; (v) age assurance mechanisms for the use of games and Internet applications; and (vi) the definition of guidelines and good practices that express a set of normative principles, technologies, and privacy by design measures that promote and ensure effective protection of the personal data of children and adolescents in games and Internet applications (ANPD, 2024c).

ANPD's Priority Themes Map for the 2024-2025 biennium also addresses the issue: carrying out enforcement actions to ensure the best interests of children and adolescents, by verifying the compatibility between LGPD and the treatment given by digital platforms, as well as proposing safeguard measures to user's age assurance (ANPD, 2023c).

The Brazilian Ministry of Justice and Public Security (MJSP), through the Secretariat of Digital Rights, established in 2025 an Advisory Committee aimed at formulating a methodology proposal and minimum requirements for age assurance for digital services that can be accessed by children and adolescents. The committee, formed by members of the MJSP, ANPD, and civil society organizations, works on drafting a proposal for this methodology (Brazil, 2025e, p. 86).

Other jurisdictions have implemented initiatives related to this issue. In Spain, the Expert Committee for the Development of a Safe Digital Environment for Youth and Childhood, created in 2024, proposed best practices in digital environments, assessing the risks involved, and recommendations of long-term measures for public administrations to ensure the full development of children and young people. The document established measures such as the regulation of the Age Verification System (AVS) industry, data protection, and measures such as user's non-location, non-identification[2], with the appropriate evolution of parental control and age verification requirements, in accordance with international technical models and standards (Spain, 2024, p. 65).

There is an urgent need to adopt age assurance mechanisms that protect children and adolescents from risks in digital environments, and the challenge of reconciling these mechanisms with the protection of personal data and the protection of privacy. In many cases, access to digital services may be denied if users do not provide personal information to prove their age, including sensitive data such as facial biometrics (e.g., an image of the face captured by facial recognition systems). As guided by ISO/IEC 27566 standard and the UK's *Age Appropriate Design Code*, age assurance systems should balance protecting children and respecting their rights to privacy with the minimization of personal data, especially by avoiding the unnecessary collection of sensitive data such as facial biometrics (ICO, 2022; ISO; 2025).

A study conducted by the French Autorité de Régulation de la Communication Audiovisuelle et Numérique (ARCOM) found that screens are primarily used by minors when unsupervised, and parental monitoring becoming increasingly restricted, because the small screen size of cell phones does not always allow viewing the content consumed (ARCOM, 2024a, p. 8).

[2] *According to Article 2, of Law 15,211 (ECA Digital):* "V – profiling: any form of automated or non-automated processing of personal data to evaluate certain aspects of a natural person, with the objective of classifying them into a group or profile to make inferences regarding their behavior, economic situation, health, personal preferences, interests, consumption desires, geographic location, movements, political positions, or other similar characteristics." *(Brazil, 2025c).*

ARCOM published a study stating that the exposure of children and adolescents to pornographic content on the Internet is increasing sharply. They estimate that the number of children and adolescents visiting pornographic websites each month rose from 19% in 2017 to 28% at the end of 2022 (the publication considered those over 2 and under 18 years old). On average, 12% of the audience of adult websites is made up of children and adolescents (ARCOM, 2024b, p. 5).

Several initiatives were undertaken to provide a basis for policies and regulatory actions on age assurance in Brazil and elsewhere. To better understand the technologies involved in age assurance initiatives, this document first presents some concepts and terms used to characterize the identification of user's age in digital environments.

This Technology Radar aims to analyze the current scenario of age assurance for children and adolescents in digital environments. The study adopts the perspective of data protection authorities, child and adolescent protection entities, experts, and national legislation, with emphasis on Law No. 15,211/2025 (Brazil, 2025c). Section 2 establishes the main related concepts, drawing from international literature to distinguish between age verification and age estimation mechanisms, and defining age assurance as the desired outcome. Section 3 describes and exemplifies the types of mechanisms used. Section 4 outlines the implications of privacy and data protection inherent in the processing of personal information by these mechanisms. Finally, section 5 offers a brief explanation of how the issue is currently addressed in Brazil, followed by section 6 which addresses prospects.

‹ main concepts ›

This section presents some definitions of mechanisms used to identify the age of users in digital environments. The terminology on this subject has been adopted with some variations, such as the use of terms assurance, verification, estimation, and inference of age, often used as synonyms, and with the aim of identifying age to assure, confirm, or guarantee the correct age of users in digital environments, for the purpose of restricting or allowing access to certain products or services.

In Brazil, Law No. 15,211/2025 (Brazil, 2025c) adopts the terms age assurance (*aferição de idade*) and age verification and represents a milestone for the protection of children and adolescents in the digital environment. It establishes in Article 9 that suppliers of information technology products or services that offer content that is inappropriate, unsuitable, or prohibited for minors under 18 years of age must adopt reliable age assurance mechanisms. The Law also prohibits the use of self-declaration of age, a resource widely used by various providers to assign users the responsibility for declaring their own age, without any type of proof or guarantee in the answer given.

Law No. 15,211/2025 dedicates Chapter IV to age assurance mechanisms, allowing the public authorities to act "[...] as a regulator, certifier, or promoter of technical age verification solutions, subject to the limits of legality, privacy protection, and fundamental rights provided for by law " (Art. 11). In Article 12, I, the law also determines that providers of Internet application stores and operating systems take "[...] proportional, auditable, and technically secure measures to ascertain the age or age range of users, subject to the principles provided for in Article 6 of Law No. 13,709, of August 14, 2018 (Brazilian Data Protection Law)."

According to ISO/IEC 27566-1 *Information security, cybersecurity, and privacy protection – Age assurance systems: Part 1: Framework* (ISO; IEC 2025), age assurance is "a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make age-related eligibility decisions with varying degrees of certainty".

Age estimation
Determines a person’s probable age by analyzing biometric or behavioral characteristics, such as face, voice, or digital interaction patterns.

Age verification
Confirms age via official documents or trusted services, such as ID cards, passports, credit cards, or authentication on secure platforms (e.g., GOV.br).

Age inference
Indirectly determines age by analyzing context, consumption data, educational history, or online preferences. It functions as a complementary method in age assurance systems.

Figure 2 *Activities that identify a person's age in digital environments.*

Source: own elaboration based on ISO and IEC (2025).

The Office of Communications (Ofcom), the UK regulatory authority for the broadcasting, internet, telecommunications, and postal industries, uses the term age assurance to refer to both age verification and age estimation. However, self-declaration of age is not considered to be a form of *age assurance*, once it is solely provided by the user (Ofcom, 2023, p. 16).

The Information Commissioner's Office (ICO), the UK's executive body for information transparency and personal data protection, published *Age appropriate design: a code of practice for online services* (ICO, 2022), which defined four main approaches to age assurance: i) age verification; ii) age estimation; iii) self-declaration; and iv) waterfall techniques and age *buffers*.

Various methodologies were also identified to operationalize the concept of age assurance, as first presented by the Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority, which divided the concept of age checking into declaration, certification, and artificial intelligence (CNIL, 2021). In the approach suggested by European Digital Rights (EDRI), the concept of age assurance was split into three subcategories: declaration, document-based verification, and estimation, as a synonym for 'scoring', 'assessment', or 'assurance' (EDRI, 2023, p. 10). For the eSafety Commissioner, Australia's independent online safety regulator, the term age assurance is an umbrella term which includes both age verification and age estimating solutions (Australia, 2023, p. 9).

According to the International Organization for Standardization (ISO), while age verification mechanisms determine a person's age with a high degree of accuracy, usually through official identity documents, age estimation mechanisms provide an approximate age for the purpose of restricting content or services available online, by using behavioral or biometric data based on statistical analysis (ISO; IEC, 2025, section 3). The concept adopted by ISO evolved from the definition of the British Standards Institution (BSI, 2018), where age verification is considered the gold standard of age assurance, due to its accuracy in identifying the user's actual age. Thus, other means of age verification, such as self-declaration, would not be considered ways of guaranteeing the user's age (AVPA, 2025).

As outlined by the Family Online Safety Institute (FOSI), a US civil society organization, age assurance is a broader term that describes various methods such as age verification, estimation, and age gating (FOSI, 2023, p. 3). And, according to the *Research Report: Mapping age assurance typologies and requirements*, age assurance refers to methods used to determine an individual's age, with different levels of confidence and accuracy, grouped into three categories: age estimation, age verification, and age self-declaration (Shaffique; Hof, 2024, p. 12). The report assigns primary responsibility to digital service providers for ensuring appropriate age assurance for users who access their services (Shaffique; Hof, 2024, p. 21).

In a survey conducted in 2024 by the ICO and IFF Research, an independent research agency based in London, out of a total of 235 organizations in the United Kingdom, 63% reported using age assurance methods, with 53% of them being self-declaration methods and credit and debit payment cards 38% each for age verification. Biometric matching via photo identification accounts for 28%, and other methods account for around 10% each, such as third-party databases and mobile network operators, digital footprints, and open banking. Other methods represent between 1% and 6% (ICO; IFF Research, 2024, p. 3).

Ofcom published a guide with criteria for assessing the effectiveness of age assurance methods, or *HEAA Guidance – Highly Effective Age Assurance* (Ofcom, 2025, p. 8), which aims to identify whether the methods are technically accurate, robust, reliable, and fair. Based on this guidance, Ofcom intends to conduct an analysis to measure age assurance technologies among providers of pornographic services and products on the Internet. The goal is to evaluate the use of methods such as open banking, photo identification, biometric facial estimation, *mobile network operators* (MNOs), credit cards, and *digital wallets*, among others, on websites with pornographic content.

In Brazil, in 2024, the Ministry of Justice (MJSP) and the *United Nations Office on Drugs and Crime* (UNODC) signed an agreement to develop a Strategy to End Violence Against Children and Adolescents and to establish the *Children Amplified Prevention Services* (CHAMPS) initiative. To support the agreement, the National Secretariat for Digital Rights (SEDIGI) of the MJSP published a technical note (Brazil, 2025d), which defined age assurance as the set of tools and methods used to prevent children and adolescents from accessing products and services that are inappropriate for their age. The Brazilian strategy, resulting from this agreement, led to the publication of the plan *Grow in Peace: Justice and Public Security Strategy for the Protection of Children and Adolescents*, which proposes forty-five measures for the prevention of violence, the reception and recovery of victims, and the facilitation of access to justice, including the improvement of industry practices, digital services, and adult content websites to improve age assurance standards, in accordance with international best practices (Brazil, 2025b).

The following section lists examples and definitions related to the topic, based on the various approaches and concepts presented above. Therefore, to ensure terminological consistency, this document adopts the umbrella term age assurance to refer to applications used to *verify a person's age, whether via age verification, age estimation, and age inference mechanisms*.

‹ age assurance mechanisms ›

Many applications have been developed by various companies to identify users age within products and services of digital environments. The applications are often presented under different names, such as mechanisms, methods, approaches, or types of age assurance. Age self-declaration is not considered, by some of the institutions analyzed, a method of age assurance, as it depends solely on the individual to provide age and age signal or age range, without having to provide any evidence to support the declaration. For this reason, for the purposes of this study, the mechanism of age declaration or self-declaration will not be considered a method of age assurance if used in isolation, but rather as a characteristic or requirement adopted in conjunction with other methods of age assurance.

The ISO/IEC 27566-1 standard (ISO; IEC, 2025), for example, proposes that age assurance in the digital environment should occur in three ways: through document verification (difference between dates extracted from official records), biometric estimation (facial, voice, or body) and by indirect inference, based on contextual data or usage patterns.

In the following sections, we present a general description of each type of age assurance mechanism. In section 4, we bring some issues related to privacy and data protection arising from the use of age assurance mechanisms.

Age verification mechanisms

Age verification refers to any method used to ascertain an individual's precise age to ensure they meet the eligibility requirements for accessing certain digital environments. Verification can be done by scanning official or civil documents, or through a third-party service, such as data from government-issued IDs, bank data, or others. Age verification mechanisms are subdivided into three main types: document-based verification, third-party verification, and verification as a service.

Document-based age verification

This type of mechanism requires the user to provide some form of identification document in which age can be verified manually or automatically. This requires original documents from the user, either by sending an image or through online video verification, validated by an information system or by a person. Data is accessed by service providers, from centralized databases, for automatic verification of document integrity, sometimes by using artificial intelligence systems.

Two main mechanisms for document-based age verification have been identified: by official document and by credit card. In *official document verification*, the provider requests copies of documents such as an ID card, driver's license, or passport, by extracting the date of birth and verifying authenticity through manual or automatic analysis, in addition to comparing a photograph of the user with the photo on the document.

Credit card verification consists of a user's card validation, usually by charging a small amount. It is a method designed to ensure that the user is over 18 years of age.

Age verification based on third-party data

Third-party age verification uses information sourced from external parties to validate a user's age. This process encompasses three primary modalities: verification via parental consent, via social recognition, and Verification as a Service (VaaS).

When *verifying age via parental consent*, parents or responsible parties confirm the age by using the means provided by the platform itself. The efficiency of this method depends on prior verification of the parent's age and confirmation of the family relationship, usually through document analysis. A related method involves the family account structure, in which the primary account holder connects the verified credentials to the minor's account, thereby ensuring that services are being provisioned in accordance with the designated age group.

According to the Brazilian Law No. 15,211/2025, Article 24, Chapter IX which addresses social networks,

> *Within the scope of their services, providers of products or services directed at children and adolescents or likely to be accessed by them shall ensure that users or accounts of children and adolescents up to sixteen (16) years of age are linked to the user or account of one of their legal representatives. (Brazil, 2025c).*

Consequently, applications or services that are aimed at children and adolescents (or those expected to attract them) must mandate that the account registered by a user under the age of 16 is connected to an account belonging to a parent or legal representative. This requirement serves as a key measure to afford parental control over children's online behavior, especially within social networking environments.

In *social recognition age verification*, verified users are permitted to confirm the age of new users. This mechanism functions as a system where the platform places its trust in the assurance provided by existing account holders to validate eligibility.

Age *verification as a service (VaaS)*, conversely, involves outsourcing the verification process to trusted public or private institutions, which take the responsibility for identifying and assuring the user's age. This mechanism operates by comparing personal data, such as name and date of birth, with information obtained from official databases of public agencies, banks, or social services. The method is adopted in many countries to verify the age of adults accessing age-restricted websites, to authorize purchases of controlled products such as alcohol and tobacco, to place online bets, and to prevent access to these services by children and adolescents.

In the VaaS process, it is possible to use trusted intermediaries that issue age tokens for users to authenticate themselves, thereby enhancing the security of their personal data (Shaffique; Hof, 2024, p. 33). A token functions as a form of digital proof of age that encrypts the user's age for use in the digital environment by an application provider. It can be stored in the user's browser, similar to a *cookie*, or in a digital wallet on their mobile phone. As the user browses the Internet, the token automatically permits or denies access to specific websites or services, depending on their verified age.

There are also verification methods using the MNO+18 – *Mobile Network Operator 18+ Content Restriction Filter* (ICO; IFF Research, 2024). According to this method, available in the United Kingdom, the operator offers a content filtering service that imposes content restrictions on the mobile phone chip in order to protect customers under the age of 18, based on the rules of the British Board of Film Classification (BBFC).

VaaS can also occur through cross-platform authentication (Shaffique; Hof, 2024, p. 28), one of the most widely used forms of age assurance by large technology companies. It is done by using authentication methods, based on registration in their databases (email, social network, streaming services), which are used for age verification by third parties. These third parties act as central authenticators for the user for all services on the platform.

Age estimation mechanisms

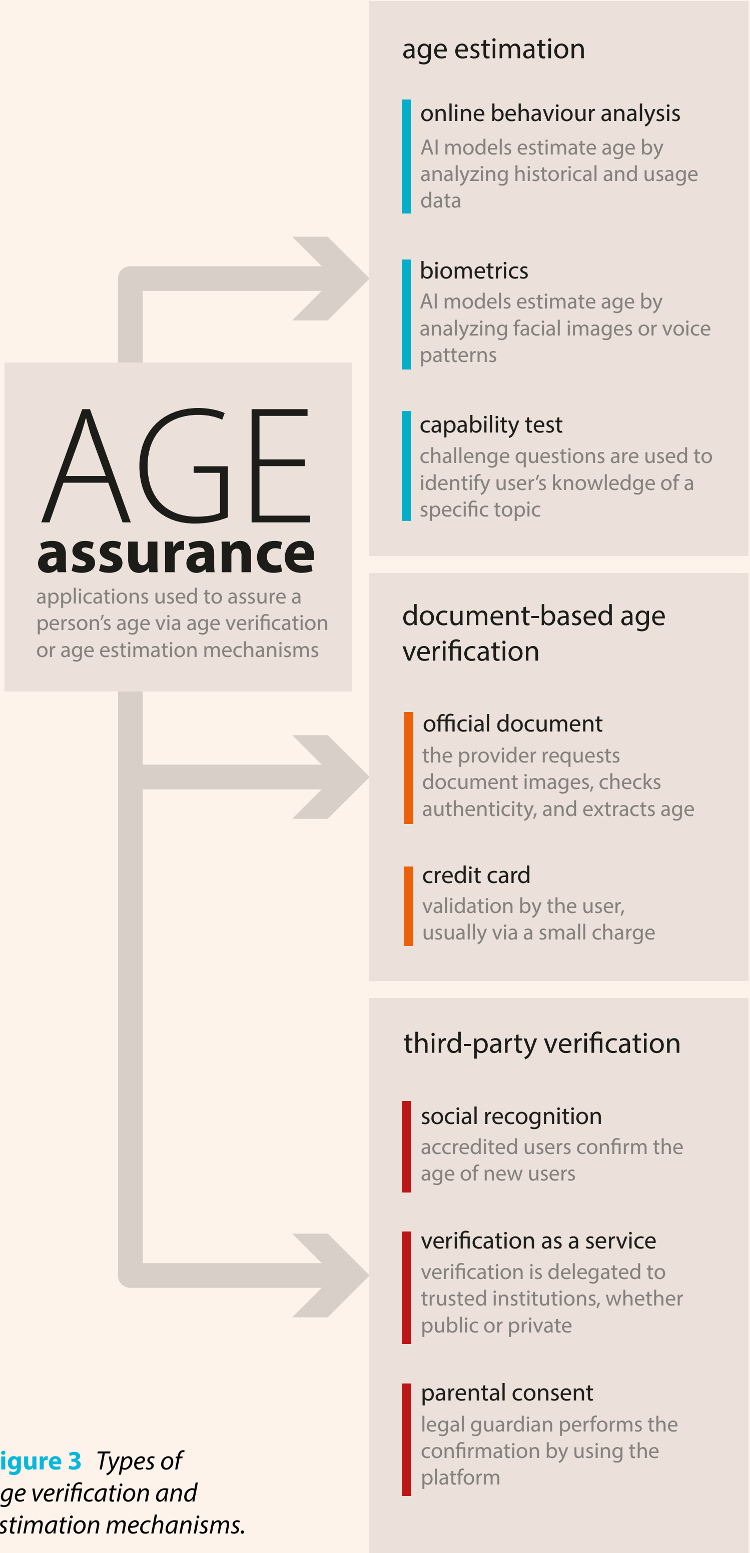
Age estimation refers to methods for estimating a user's age or age range, rather than determining their exact age, without the use of supporting documents or third-party confirmations. These mechanisms use behavioral data (browsing history and purchasing preferences, for example), biometric data, capacity tests, among others, to calculate the probable age by using estimation models. This method can be used to create accounts or to monitor user's service usage.

Age estimation mechanisms can be divided into three main methods: age estimation via online behavior analysis, biometrics, and capacity testing.

Age estimation via online behavior analysis is done by analyzing historical data used by an inference system, mainly supported by artificial intelligence, which estimates the approximate age of the user. User's digital footprints can be tracked via mobile phone number or email address, analysis of interactions or accounts created with this data across many different websites (ICO, 2024b).

Biometric age estimation involves using biometric data (e.g., the user's facial image or voice) to enable the model to estimate age, usually via artificial intelligence technologies. The facial image can be captured in real time by a mobile phone camera or a specific camera, with a higher level of accuracy and efficiency, although these results vary depending on skin tone, gender, and age.

Finally, *age estimation via a capability* test consists of asking the user one or more challenging questions to identify their knowledge of a particular subject, or their ability for solving a problem (in mathematics, general knowledge, etc.) or spelling, for example) and thus gathering them into an age range. It is used to estimate the approximate age of users, based on a prior knowledge of certain content taught in a school grade and, therefore, within an estimated age range.



AGE **assurance**
applications used to assure a person's age via age verification or age estimation mechanisms

age estimation

online behaviour analysis
AI models estimate age by analyzing historical and usage data

biometrics
AI models estimate age by analyzing facial images or voice patterns

capability test
challenge questions are used to identify user's knowledge of a specific topic

document-based age verification

official document
the provider requests document images, checks authenticity, and extracts age

credit card
validation by the user, usually via a small charge

third-party verification

social recognition
accredited users confirm the age of new users

verification as a service
verification is delegated to trusted institutions, whether public or private

parental consent
legal guardian performs the confirmation by using the platform

Figure 3 *Types of age verification and estimation mechanisms.*

Source: own elaboration.

Age inference mechanisms

According to the ISO/IEC 27566-1 standard (ISO; IEC, 2025), age inference is an age assurance method based on verified information that indirectly shows whether an individual is above or below a certain age or within an age range. It is a term often used synonymously with age estimation, particularly when artificial intelligence technologies are used to infer the user's age from behavioral data. By using contextual analysis, behavioral and digital interactions, age inference is used to determine the probable age of a user or an age group based on indirect and verifiable signs collected from behavior, context, and digital data, without requesting official documents or biometric data. In other words, instead of directly asking their age or asking for a document, the system looks for indirect clues in order to draw a reasonable conclusion about a user's age, by analyzing a set of digital facts. Age inference mechanisms derive insights from behavioral indicators gathered during user interaction, such as browsing speed, vocabulary patterns, speaking time, historical content consumption, transaction types, and service usage.

Operational stages of the mechanisms

Based on the approach of ISO/IEC 27566-1 standard (ISO; IEC, 2025), the mechanisms were organized as follows: document verification, identification linked to civil identity, biometric estimation, and behavioral inferences. From a technical standpoint, these approaches generally follow the same operational stages, described as a five-step *pipeline*[3], described below.

1. **Collection**: the system receives as input a photograph, video, audio, official document, or indirect signals, such as browsing patterns or device characteristics.

2. **Pre-processing**: raw data is initially processed to ensure its usability: a document is read by *Optical Character Recognition* (OCR), an image or audio is normalized (adjusted for lighting, noise, or distortions). Only the most relevant features are extracted, such as the outline of the face or skin texture. This filtering step prevents simple errors that could impact the analysis.

[3] *The decision to describe age assurance mechanisms in a pipeline format was inspired by ISO/IEC 27566-1:2025, which characterizes such systems as composed of interdependent components (credentials, processing subsystems, service providers) and uses flowcharts to illustrate the decision-making on age eligibility. This sequential approach is also adopted in academic reports, such as Trustworthy Age Assurance (Sas; Mühlberg, 2024), which organizes the analysis into interconnected phases (self-declaration, document verification, biometric or behavioral estimation, token issuance, and proof transmission). Regarding the stages, although part of the literature simplifies the process into three macro-phases (collection, processing, and issuance), technical standards (ISO/IEC 27566-1:2025) and regulatory guidelines (CNIL, 2022; Ofcom, 2025) point out the importance of detailing five stages: (i) collection, pre-processing, main processing, (iv) integrity controls, and (v) issuance of evidence. This finer fragmentation reflects contemporary requirements for security, privacy, and robustness, justifying the current adoption of a five-phase model presented in this report.*

3. **Main processing**: this is the decisive phase. Depending on the technology employed, it may involve comparing a document against an official database, algorithmic age estimation based on biometrics, or simple age classification into ranges ("under 13," "over 18"). In more advanced applications, the result does not disclose identity but generates a digital credential or token that solely certifies age.

4. **Integrity controls**: to reduce fraud, techniques are applied such as liveness testing, detection of false presentations (such as *deepfakes* or static photos), attempt limitation, and, when necessary, human review. These mechanisms ensure that age verification is not impacted by manipulation.

5. **Disclosure of evidence**: the system generates the ultimate proof that the age criterion has been successfully met. Unlike other methods that expose the name or date of birth, current applications issue only the essential attribute. This proof often takes the form of a digital token, with an expiration date, usage restrictions, and cryptographic protection. In some cases, advanced protocols are applied, such as *zero-knowledge proof* (ZKP)[4], allowing confirmation of age without revealing who the user is, nor which service requested the information.

To move beyond theory, some countries have evaluated age assurance methods within controlled testbeds by making comparable analysis, considering criteria such as accuracy, bias, fraud resilience, and impact on data protection rights. The most notable example is the *Age Assurance Technology Trial* (Australia, 2025a) conducted in Australia in 2025, which compared documentary, biometric, inferential, and token-based models. The study also measured the performance of these technologies in different layers of the digital ecosystem, such as devices, operating systems, browsers, and platforms, highlighting the importance of interoperability (ACCS, 2025, p. 8)[5].

[4] *Zero-knowledge proof (ZKP) are cryptographic protocols that allow a user to demonstrate the veracity of information, such as being of legal age, without revealing the underlying data, ensuring privacy and minimizing personal attributes. This technique has been highlighted in international regulatory debates on age assurance mechanisms, such as in reports by the CNIL (2022) and the European Commission (European Commission, 2025d), which point to its potential to balance robustness and data protection.*

[5] *The Age Assurance Technology Trial (Australia, 2025a) was conducted by Australia's eSafety Commissioner in 2025, in a controlled test environment (testbed), comparing documentary, biometric, inferential, and token-based methods, focusing on criteria such as accuracy, bias, anti-fraud resilience, and impact on data protection. The Global Age Assurance Standards Summit (ACCS, 2025) did not directly carry out the testbed, but systematized and discussed the results obtained, highlighting the importance of interoperability and international standardization.*

A generational approach of age assurance mechanisms

Age assurance mechanisms can be analyzed in a timeline, where each type can be identified by technical advances, regulatory demands, and social requirements. Here follows a proposal of the evolution of applications in five generations[6]. While this chronology contains overlaps and should not be considered strictly sequential, it clearly delineates the developmental trajectory. This path spans from simple, initial acts of self-declaration to the establishment of sophisticated, scalable systems for auditable and validated credentials.

1st Generation | Self-declaration (2000–2010)

The initial stage of age assurance in digital environments is characterized by self-declaration. In this model, users themselves provide their age, either by entering a date of birth or by checking boxes such as "I am over 18 years old." Some platforms sought to reinforce this procedure with proxies such as credit card numbers, SMS, validated email, or authentication via third-party accounts.

Despite these variations, the method still relies on the user's good faith and does not establish a verifiable link to their civil identity. CNIL (2022) and Ofcom (2024) classify self-declaration as a low-intrusion but low-reliability practice, and it may be only “suitable for low-risk processing, when used in conjunction with other techniques” (ICO, 2022). As mentioned before, age declaration or self-declaration mechanisms will not be considered a method of age assurance if used in isolation. In the same vein, ANPD has also taken a position in its Technical Note No. 50/2024, when assessing digital platform practices, by highlighting that self-declaration, when used solely, is not a suitable mechanism for age verification (ANPD, 2024b).

From a technical standpoint, the first generation of age assurance mechanisms are based on simple forms, usually in HTML or embedded in applications. Some systems adopt basic format validations, such as preventing negative ages or ages above 120, by checking date consistency, or by limiting successive attempts to reduce fraud and brute-force attacks. The

[6] *In order to explain the classification of age assurance technologies into "generations," we highlight some research points: 1 - Technical and regulatory literature considers solutions as distinct stages or categories, reflecting historical evolution. 2 - There are regulatory frameworks (CNIL, ICO, Ofcom, EDPB, European Commission) that have propelled evolutionary change. 3 - ISO/IEC 27566-1:2025 proposes types/categories (verification, estimation, inference), with different levels of confidence and temporal maturity. 4 - Comparative studies (Sas; Mühlberg, 2024) also groups methods into technological "families". 5 - Regulatory authorities (CNIL, 2022; Ofcom, 2025) and EDPB (2025) emphasize that simpler methods (self-declaration) are ineffective, and that newer technologies cryptographic tokens, zero-knowledge proof) represent an advance in reliability and data protection, which occurs on an evolutionary scale. These arguments led us to propose a classification that involves time, complexity, and technological resources.*

self-declared data is then recorded in the account or device registry and used to enable or restrict features, such as access to certain content or interaction resources.

In practice, this flow is quite predictable and technically deficient, because it is easy to manipulate birth dates which make this type of information unreliable for age verification purposes. As a result, it is easier to create multiple accounts by using false data because information is not unique enough to prevent fraud. In other words, because it is easily deducible and simple to falsify, the date of birth is a facilitating factor for the creation of multiple registrations with false information. In addition, the absence of mechanisms for linking to civil identity and additional layers of verification, such as biometrics or document verification, limits the method's reliability.

Studies conducted by regulatory authorities such as Ofcom (2024) and the Australian Age Assurance Technology Trial (Australia, 2025a, p. 142), show high rates of age misrepresentation by children, which confirms that even with minor compensatory controls, self-declaration remains a low-reliability solution.

2nd Generation | Document verification and biometrics (2010–2018)

The second generation of age assurance mechanisms emerged with the popularization of smartphones with cameras and the digitization of financial and public services. The technical flow, described in international standards (ISO; IEC, 2025), in a technical note from SEDIGI (Brazil, 2025d) and in Ofcom reports (2024), begins with the capture of an official document such as an identity card, driver's license, or passport, which is submitted to OCR (Optical Character Recognition).

This step converts the image into structured text, allowing for the automatic extraction of information such as name, document number, and date of birth. More advanced systems not only perform text recognition but also analyze graphic patterns (holograms, fonts, margins, and micro textures) to detect signs of forgery.

The next step involves face matching: the user submits a selfie or a brief video, which is then compared with the document's photograph. This step is based on recognition algorithms. Facial recognition creates a link between the declared identity and the person who is accessing, thereby mitigating the risk of document misuse by third parties.

Liveness detection is incorporated to enhance system efficiency. In the passive model, algorithms evaluate subtle characteristics of the capture, such as light reflections on the skin or image depth, without requiring user interaction. In the active model, there is a requirement for real-time movement, such as blinking, smiling, or turning the face at different angles. Both methods are recommended by recent studies (Australia, 2025a) and Ofcom reports (2025) to prevent printed photos, videos, or deepfakes from fooling the system.

3rd Generation | Biometric and behavioral estimates or inferences (2018–2022)

The third generation of age assurance mechanisms come from advances in artificial intelligence and the growing use of deep learning models in computer vision and pattern analysis. Unlike document verification, this model does not rely on the submission of official credentials, because age is estimated directly from biometric or behavioral characteristics.

The technical flow involves, first, the capture of data such as facial images, voice samples, short videos, or even patterns of interaction with devices (e.g., typing, browsing speed, and use of applications). This data is processed in neural networks trained with large databases of labeled examples, allowing for the identification of discriminative features (expression lines, skin texture, voice variations, reaction time, among others).

Regression algorithms estimate an approximate numerical age, while classification models estimate, for each age group defined in the training, the probability of assigning the user to the class with the highest probability, such as "under 13," "13 to 17," or "18+." This model is described in international standards (IEEE, 2024; ISO; IEC, 2025), by regulatory authorities such as the Age Assurance Technology Trial (Australia, 2025a), the Global Age Assurance Standards Summit (ACCS, 2025), and other reports (Ofcom, 2024). This approach is considered more practical in regulation contexts, as it reduces the need to collect and store personal documents. However, this generation has significant technical and ethical limitations. Accuracy varies according to the quality of the input data and the diversity of the training base.

Voice analysis is a biometric method also used in this generation, which is based on the premise that acoustic characteristics change throughout human development. The operation begins with the collection of a voice sample in which the user repeats a phrase or reads aloud a short text. Next, parameters such as fundamental frequency (pitch), formant distribution (vocal resonances), articulation velocity, and prosodic variation are extracted. Finally, algorithmic classification occurs, in which machine learning models, Random Forest, or neural networks associate the acoustic vector with a probable age group.

Voice recognition can be useful in contexts where a camera is not available, such as virtual assistants and audio-based games. It can be less accurate than facial analysis. Another form of age verification involves the analysis of writing and linguistic patterns. The system collects typed texts or transcribed speech from the user and applies natural language processing (NLP) techniques to identify, for example, the frequency of slang, emojis, and abbreviations; the syntactic structure typical of adolescents (short sentences, frequent spelling errors); and even lexical richness in conjunction with stylistic choices associated with older age groups.

Supervised text classification models can estimate or infer age with increasing accuracy but still face problems such as cultural adaptation and manipulation (children can imitate adult vocabulary).

In addition to voice and language, patterns of interaction with devices provide useful signals such as typing speed *keystroke dynamics*, response time in games and riddles (children tend to have different schedules than adults) and device usage (duration, types of applications, etc.).

Data collection generates behavioral vectors analyzed by probabilistic classification algorithms. This modality, known as passive biometrics, is described in international standards (IEEE, 2024; ISO; IEC, 2025), in surveys such as the Age Assurance Technology Trial (Australia, 2025a). Applied research shows that typing patterns can be used as age indicators. Pentel (2018), for example, showed that the analysis of keystroke dynamics on different devices allows age groups to be distinguished with a high degree of accuracy, even in short and uncontrolled input scenarios. This type of data processing works in the background, without explicit user interaction.

4th Generation | Tokens and cryptographic proofs (2022–2025)

The global regulatory landscape for data protection intensified after 2022. At this point, the idea that it is not necessary to expose one's complete identity to guarantee a single attribute, such as legal age, gained prominence. Solutions based on zero-knowledge proof and double-blind protocols emerge in tandem with the advancement of self-sovereign identity credentials and privacy by *design* requirements.

The fourth generation of age assurance technologies is based on advanced cryptographic approaches that allow age attributes (such as being of legal age) to be verified protecting personally identifiable information. In this model, minimal credentials, known as "cryptographic tokens," are issued and used selectively and securely.

The *EU Age Verification Solution*, launched by the European Commission in July 2025, represents a milestone in this generation. It will allow users to prove that they are over 18 without sharing personal data. The proof of age is presented and issued by separate entities, with confidentiality and untraceability, a model associated with the principle of privacy by design (European Commission, 2025a). In addition, the use of zero-knowledge proof continues to be developed to ensure that such authentications are non-binding and untraceable.

This trend is supported by academic and governmental analysis that highlight the role of ZKPs in promoting data minimization, especially in systems such as digital wallets, which are compatible with the General Data Protection Regulation (GDPR) (European Union, 2016) and eIDAS (European Commission, 2025c). This technology allows valid evidence to be presented without exposing additional metadata that could compromise user privacy. Some of these solutions are presented in more detail below.

Cryptographic tokens (age tokens)

Age tokens are a type of digital credential, issued and signed by a trusted entity, which serves to prove a specific attribute of a person without exposing complete data. This model is described in international standards (ISO/IEC, 2025; W3C, 2025) and in recent studies in Australia (Australia, 2025b) and the European Union (European Commission, 2025a). In the context of age assurance, the token does not carry any personal data. Instead, it contains only the necessary information, for example, "over 13 years old" or "between 16 and 18 years old" or even "over 18 years old." This credential is protected by encryption, which guarantees authenticity.

In general, the use of tokens involves four main steps.

1. Initial validation. The user proves age to a trusted provider (through official documentation, biometrics, or other robust methods).

2. Token generation. The provider issues a cryptographically signed digital token (standards such as JWT or blockchain-verifiable credentials). This token contains only the necessary attributes: "18+" or "between 16 and 18 years old."

3. Secure storage. The token is stored by the user, either in digital wallets or in local drive on the device (with a defined expiration date).

4. Presentation in third-party services. When requested, the user presents the token, which is validated by the issuer's public key.

This flow creates a layer of unlinkability, in which the accessed service does not know which assurance method was originally used, and the verification provider does not know in which services the token will be used.

Double-blind model

In recent age assurance architecture proposals, it is important to distinguish between what is meant by a cryptographic token and what is called a double-blind model. As mentioned, the token is a digital credential issued by a trusted entity. It functions as a kind of mathematical stamp that certifies only a specific attribute, for example, that the user is over 18 years of age, without revealing date of birth or any other personal data. This credential may be temporary, subject to reuse policies, and protected by a digital signature that prevents forgery.

The double-blind model, in turn, is the protocol that manages the use of these tokens. The term "double-blind" expresses the arrangement in which the parties involved have access only to minimal information about the user. Thus, the issuer of the credential and the receiving service do not know the service behind the presentation. In other words, the issuer does not track the user's behavior, and the receiver does not have access to the identity and is restricted to the binary information matched by the age requirement. The double-blind structure is based on W3C standards (2025), in ISO/IEC 27566 (2025), in the *European Age Assurance Solution: Operational, Security, Product and Architecture Specifications* (European Commission, 2025d), and in the *Age Assurance Technology Trial* experiments in Australia (2025a).

Thus, the cryptographic token represents the data minimization tool, and "digital key" contains only the age attribute. The double-blind model defines the rules for circulating the token to preserve privacy throughout the cycle. They both build a strategy to reduce traceability and reinforce protection against personal data processing abuse.

Zero-knowledge proof

A promising application to improve compliance with data protection standards in age assurance systems is the use of *zero-knowledge proof* (ZKP). In this model, there is no need to share personal data such as date of birth, but only in order to mathematically prove compliance with age requirements.

In practical terms, the user's device or a digital wallet performs a cryptographic calculation on securely stored information (date of birth, for example). The result is a mathematical proof sent to the service which the platform, in turn, does not have access to the personal data, but receives sufficient evidence to confirm whether the condition was met. The outcome is simple: the answer comes in the form of "yes" or "no", allowing or denying access.

This model avoids the creation of centralized databases with birth dates, reduces tracking between different services, and significantly reduces the risks in the event of data leaks.

Although the concepts of ZKP and the double-blind model may have some similarities, they are two distinct approaches that can be applied in age assurance systems, but both operate at various levels. ZKP is a cryptographic method, while the double-blind model is a trust arrangement between different actors. In order to better understand this difference, the following table provides a comparison.

Table 1 *Comparison between ZKP and double-blind model*

Aspect	ZKP (Zero-Knowledge Proof)	Double-blind model
Definition	Cryptographic protocol that allows a fact to be proven without revealing the data itself.	Trust architecture in which sender and receiver do not have full access to the data.
How it works	Users authorize a device or digital wallet to perform mathematical proof of age data (e.g., age ≥ 18) and only send the verifiable result.	A trusted authority issues a blind token/credential; the platform only reads the token, and the authority does not know where it was used.

Aspect	ZKP (Zero-Knowledge Proof)	Double-blind model
Privacy	Very high: the platform only receives 'yes' or 'no', never the birth date.	Very high: separation of duties avoids cross-tracking between an issuer and the platform.

Source: Sas and Mühlberg (2024), ISO and IEC (2025), CNIL (2022), EDPB (2025).

These two approaches can be complementary, despite their differences; for instance, tokens issued in a double-blind model can be based on ZKP proofs, thereby increasing cryptographic robustness and protection against tracking.

5th Generation | Establishing testbeds and integrating into the *technological ecosystem* (2025 onwards)

The 5th generation shifts the focus from "which method to use" to "how to co-prove, integrate, and audit" within real-world ecosystems. This requires demonstrable evidence of performance and data protection, guiding regulatory and public policy decisions. The core concept is that while previous generations focused on individual services (where each website and application ran its own verification), this generation focuses on the entire digital infrastructure. This shift mandates auditable protocols and native integration across the ecosystem. Countries such as Australia and the United Kingdom have launched testbeds[7] designed to compare different age assurance technologies. In these environments, applications are evaluated against standardized criteria of accuracy, bias, anti-fraud resilience, and privacy protection. This stage represents a more robust integration phase, in which age assurance mechanisms are tested across the entire ecosystem, including devices, operating systems, browsers, and platforms. The strategy is to guarantee that they have interoperable functions, with standardized credentials and subject to independent audits.

Significantly, the Australian study *Age Assurance Technology Trial* (Australia, 2025a), was executed by an independent certifying body, with support from academic institutions and industry stakeholders. This trial represents a practical stage of regulatory experimentation, whose final report compares accuracy, bias, fraud detection, and privacy safeguards, and documents how solutions behave in layers of the technological ecosystem

[7] ***Testbeds*** *are controlled experimentation environments created to comparatively evaluate different age assurance technologies before their large-scale adoption. Such environments allow for the analysis of technical effectiveness, proportionality, impacts on privacy and digital inclusion. The European Commission, for example, has been conducting pilot projects with the so-called "mini wallet" as a way of proving age while preserving privacy (European Commission, 2025b). The CNIL, in turn, recommends that verification models be tested under controlled conditions to ensure robustness without compromising data minimization (CNIL, 2022). In the United Kingdom, Ofcom now requires high-risk services to employ methods considered "highly effective," previously evaluated in test environments (Ofcom, 2025). Similarly, ISO/IEC 27566-1 establishes trust and security parameters that can be validated in testbeds prior to implementation in digital ecosystems (ISO; IEC, 2025).*

(device, operating system, browser, and platform) – a necessary condition for truly interoperable and auditable implementation.

Concurrently, the United Kingdom has aligned the requirement for "*Highly Effective Age Assurance*" (HEAA) with its regulatory enforcement (Ofcom, 2024). Similarly, the European Commission has published an age assurance plan that prioritizes minimized credentials and future integration with the *European Digital Identity Wallet*. This reinforces the global trend towards controlled testing, standardized metrics, and privacy-preserving design from the outset (European Commission, 2025a).

The core technological elements of this generation include interoperability architectures, ecosystem-derived credentials, advanced cryptographic tokens, and integration with sovereign digital wallets, accompanied by reinforced security layers. Furthermore, regulatory experiments such as the European Commission's *Overall Architecture – European Age Assurance Solution* (2025) and Australia's *Age Assurance Technology Trial* (2025a) highlight the crucial importance of *testbeds* for evaluating performance, bias, and privacy impact. The following list outlines a summary description of these elements that characterize the 5th generation of age assurance mechanisms.

- **Interoperability architectures**: standardized protocols that allow different verification methods (document, biometrics, cryptographic tokens) to work together.

- ***Ecosystem derived credentials***: operating systems and browsers now offer native age verification APIs, so that the application does not manipulate directly raw data; it only receives the evidence (e.g., "18+ valid until 2026").

- **Advanced cryptographic tokens**: issuance of minimized, audience-bound, short-lived age attributes, reducing the risk of tracking. These tokens can use cryptographic signatures or zero-knowledge proof to ensure privacy.

- **Integration with sovereign digital identities (eID, *wallets*)**: use of wallets such as the *EU Digital Identity Wallet* or Gov.br in Brazil to certify age attributes without exposing personal data.

- **Enhanced security layers**: liveness mechanisms (Ofcom, 2025), protection against collusion attacks, and continuous credential validation, built into the device.

- **Test environments (testbeds)**: platforms that bring together regulators, industry, and academia to compare solutions in identical scenarios, evaluating performance, bias, and impact on privacy (example: Age Assurance Technology Trial in Australia, 2025a).

Table 2 presents a comprehensive summary, distinguishing the 5th generation from its predecessors. This comparative overview highlights the key aspects, operational mechanisms, and inherent limitations of each generation, underscoring the shift towards ecosystem-wide interoperability and enhanced data protection.

Table 2 *Summary of the 5th generation of age assurance mechanisms*

Aspect	What it is	How it works	Limitations / Challenges
Core concept	Integration of age assurance and the digital ecosystem: device, operating system, browser, and platform.	Native APIs in browsers and operating systems provide platforms with only the evidence of age group ("≥ 18"), without exposing raw data.	Complexity of global standardization and reliance on cooperation among major technology players.
Interoperable architectures	Protocols commonly evaluated in testbeds.	Different methods (document, biometrics, tokens) are compared side by side in terms of accuracy, bias, fraud, and privacy.	High-cost testing and the need for transparent and auditable evaluation criteria.
Advanced cryptographic tokens	Digital credentials that only attest the age attribute.	Issuance by reliable authority for short validity, domain binding (audience-bound), and the use of ZKP and blind signatures to prevent tracking.	Requires digital wallets infrastructure and reliable and widely distributed digital signatures.

Integration with sovereign digital identities	Use of wallets such as EU Digital Identity Wallet or Gov.br.	Sharing selective exclusion of derived attributes (e.g., “≥ 18”), without revealing name, CPF or date of birth.	Risk of exclusion of people without access to a robust sovereign digital identity.
Regulatory testbeds	Age-assurance testbeds with academia, regulators, and the private sector.	E.g.: Age Assurance Technology Trial in Australia – methods compared: document, biometric, inferential and tokens, under identical conditions.	Still experimental, such results are not always transferable to other contexts, cultural, and legal.

Source: CNIL (2022), EDPB (2025), Ofcom (2024), and Australia (2025a).

‹ age assurance and personal data protection[8] ›

Risks to children's right to personal data protection arise from data collection by public or private institutions, as well as from the sharing of photos by family members (sharenting[9]). These practices may reveal sensitive information about the child, including location, activities, emotions, health aspects, and personal relationships.

In this context, General Comment 25 of 2021 (UN, 2021), of the United Nations Committee on the Rights of the Child, addresses the protection of children in digital environments. Specifically, section E of the Comment recognizes children's right to privacy as vital for their autonomy, dignity, safety and the exercise of their rights. The comment recommends that countries define measures to ensure children's privacy, specifically, mandating the use of privacy and security by design, in products and services that affect children.

Fernandes (2021, pp. 243–252) proposed a series of recommendations for regulating the protection of children's rights, including the requirement

[8] *This section highlights some aspects found in the literature on personal data protection in relation to the age assurance mechanisms studied. However, it is not exhaustive and does not aim to present specific suggestions on the topic.*

[9] ***Sharenting** is a term that combines the words "sharing" and "parenting." It refers to the practice of parents excessively sharing photos, videos, and details of their children's lives on social media (Alana, 2025).*

for age verification. On this subject, the author asserts that "it is essential that products or services that process personal data know who usually uses them, in order to establish the most rigorous protection standards when children and adolescents can access them." (Fernandes, 2021, p. 247).

Livingstone, Stoilova, and Rahal (2023a) and Livingstone and Pothong (2023b) discussed how digital skills and literacy support children's rights and indicated 11 principles of children's rights applicable to the digital environment. In principle 4 (age appropriate), the authors indicate that age-appropriate policies and products should be developed by design, and that age-assurance mechanisms should be considered. According to the author (2023b, p. 8), the age-assurance mechanisms currently adopted in digital environments do not meet the requirements of the European Union's General Data Protection Regulation (GDPR), since they are insufficient and do not protect children from accessing inappropriate content and harmful products and services.

In Brazil, from a data protection perspective, LGPD establishes that the processing of personal data of children and adolescents must be carried out in their best interests (Brazil, 2018, Art. 14). In 2022, ANPD approved the regulation of the application of LGPD for small-scale processing agents, by considering of high risk the processing of data of children and adolescents, when carried out on a large scale and/or when it could significantly affect the fundamental interests and rights of the data subjects (ANPD, 2022, Art. 4). In 2023, ANPD issued a statement regarding the possible interpretations of LGPD Article 14, concluding that in the processing of personal data of children and adolescents, the hypotheses provided in Articles 7 or 11 may also be applied, provided that the best interests of this group are observed (ANPD, 2023a).

The Guide on the Legal Hypotheses for the Processing of Personal Data and Legitimate Interest provides considerations for children and adolescents about data processing. It cites General Comment No. 14, 2013 of the UN Committee on the Rights of the Child (2013), which emphasizes that children have the right to have their best interests assessed and prioritized. Furthermore, it requires consideration of the positive and negative impacts of decisions affecting an individual child, an identified group of children, or children in general. Thus, any action or decision involving this audience must ensure compliance with the best interests of the child, taking into account their physical, emotional, and educational development, as well as the principles for the processing of personal data provided for in Article 6 of LGPD, such as purpose, necessity, transparency, and security and risk mitigation measures (ANPD, 2024a, p. 9).

The age assurance mechanisms presented in this study, in particular document-based age verification and age estimation mechanisms, require the collection, processing, and, in some cases, storage of personal data from adults and children, some of which is sensitive, such as biometric data. This raises concerns about the protection of personal data.

Sas and Mühlberg (2024, p. 7) concluded that there is no age assurance method capable of verifying the user's age with infallibility and adequately protecting individuals, adults, and children's fundamental rights. Authors warned that the existence of measurement applications lacking adequate protection for fundamental rights could normalize excessive privacy intrusion and increase the risks of data leakage and misuse.

EDPB agrees that the available age assurance mechanisms may impact users' fundamental rights (EDPB, 2022, p. 26). The principles of proportionality and necessity (Brazil, 2018, Art. 6) must be observed in the analysis of the nature of the service, the data collected, processed, and treated, and the risks of the service or content that will be associated with age verification technologies (CNIL, 2021). In addition, the reliability level of the methods must be proportional to the severity of the identified risks related to the service. However, accuracy and reliability are directly related to methods considered more invasive and riskier (Sas; Mühlberg, 2024, p. 19).

Notably, the definition of inappropriate content and associated risks may vary, with users and regulators holding different views on what may be harmful (Caglar; Nair; 2021, p. 4), and that the adequacy of available methods changes with technological advances and their associated risks, requiring periodic reviews (EDPB, 2023).

The implementation of age assurance technologies that reveal the identity of users of online services may allow personal information to be linked to the content accessed. This can pose a threat to users who depend on anonymity to ensure their physical safety and the proper exercise of their professional duties. Similarly, it negatively affects members of marginalized communities and victims of violence, who need protection from undue exposure. Furthermore, it can compromise the exercise of fundamental freedoms of both children and adults, thus creating an inhibiting effect on users' legitimate activities (EDPB, 2022, p. 26; EDRI, 2023, p. 27). Finally, there are also cyber risks and those associated with the reuse of this data for behavioral advertising and commercial, police, or political profiling (Sas; Mühlberg, 2024, p. 34–35).

In fact, self-declaration is not considered an age assurance mechanism on its own, even though it reduces the exposure of personal data, but offers little or no effective age assurance and can be easily circumvented by the user.

Age verification via the use of official documents is one of the most efficient verification methods in terms of accuracy, but it requires a security infrastructure to process and store large volumes of data. Furthermore, this application may exclude children without official documentation (Shaffique; Hof, 2024, p. 26).

The use of credit card verification, on the other hand, carries risks of profiling and security, as it involves the collection of personal and financial data (Sas; Mühlberg, 2024, p. 66). It has low reliability, as children can use adult's credit cards to access services restricted to those over 18 (Shaffique; Hof, 2024, p. 27). It has limited accessibility, because not everyone has a credit card, and the minimum age for obtaining one varies between countries, which limits the use of children and adolescents. Therefore, these methods may reveal more information than the necessary for age assurance purposes, which may violate the principle of necessity, depending on the context in which it is required.

In some countries, document verification can be strengthened via direct link to national digital identification systems, such as Gov.br in Brazil or electronic identification (eID) in the European Union. Under this arrangement, instead of submitting documents to each service, the user shares a derived attribute, such as the condition "over 18 years of age." This strategy reduces the exposure of personal data (name, social security number, address), in accordance with the need for minimization and disassociation.

Despite the technical advantage over self-declaration, this method has significant limitations. If the service requires more information to identify the user, it can enable highly reliable tracking of activities, increasing the risks of surveillance or misuse by private actors, and cyber risks. Furthermore, the concentration of identity data on government or private servers increases the security risk and requires high standards to prevent cyberattacks or potentially damaging incidents (EDRI, 2023, p. 30; Sas; Mühlberg, 2024, p. 61). The repetition of this process on different platforms multiplies the points of data collection, incompatible with principles of personal data protection, such as the principle of necessity. In this context, challenges related to digital inclusion and accessibility are perceived, especially by children and young people, who are the main target of online age assurance mechanisms. EDRi estimated that eID Wallet could exclude 20% of general users (EDRi, 2023, p. 30).

Age assurance methods based on third-party actions, such as social recognition verification, may require the user to have connections with friends and relatives who are active on the service or platform they intend to use, in addition to the possibility of a long waiting time to obtain consent (EDRi, 2023, p. 16). This mechanism is not very effective because it is impossible to guarantee the accuracy of the information provided by the accreditors. Furthermore, in the case of child and adolescent users, consent is only valid when provided by a parent or a legal representative, according to LGPD (Brazil, 2018, Art. 14).

With regards to age verification via parental consent, the capacity of parents or responsible parties to assess the risks associated with accessing and sharing certain information on platforms or services and in the processing of collected personal data must be duly considered. Nascimento and Bernardes (2025) conducted research on the creation of children's profiles on social networks by their own parents, even though the legal recommendations and policies of these networks do not allow access to this audience. Olszewski (2025, p. 17) conducted research on digital overexposure (oversharing)[10], which is very common nowadays.

[10] ***Oversharing*** *is the act of sharing personal information excessively, often without thinking about the consequences. It is a combination of the words "over" (excessive) and "sharing." This can happen with any type of information and with anyone, whether on social media, in private messages, or even in online conversations (Olszewski, 2025).*

It is not only adults who participate in this overexposure, as more children have videos, photos, routines, and sensitive information published by their own parents on social networks, infringing on children's personality, privacy, and image rights.

Both methods of third-party verification face challenges related to the reliability of the information provided and the need for additional validation by the accreditors and legal representatives, which demands the implementation of complementary controls to ensure the accuracy of the age assurance process.

On the other hand, EDRi (2023) warns about the risk of outsourcing age verification to companies, such as in VaaS. This outsourcing can undermine the involvement of parents and responsible parties and create extremely restrictive environments for children and adolescents due to the possible exclusion of broad categories of content that is not harmful, as a simple precaution, while there is no legal regulation, impacting their right to information. There are inherent risks of providers having excessive control over what children can see and do online (EDRi, 2023, pp. 26–27). The level of assurance of this method depends on how age was initially verified, in addition to delegating to these companies the authority to control the application, increasing their control over the age verification data in their custody.

Although it offers greater reliability through cross-validation with official databases, VaaS requires strong technological integration between the service and the databases, as well as the collection and processing of large volumes of personal data. This characteristic gives the application a high technological risk, requiring security protocols and compliance with data protection regulations to mitigate potential vulnerabilities and ensure the privacy of verified users.

Sas and Mühlberg (2024, p. 67) mention three risks associated with this method from the perspective of personal data protection: i) knowledge of the user's identity by the website or application (service provider) accessed; ii) knowledge by the service provider of the relationship established between the user and the third-party verifier; and iii) the third-party verifier's knowledge of who the provider is and what service is being accessed. If these three pieces of information are combined, surveillance and profiling will become possible.

Although cryptographic age tokens can prevent user identification, direct transmission via API from the verifier to the service provider introduces privacy and security risks. This method reveals the provider's identity, exposing the purpose of verification, and allowing the user's online activities to be tracked (Sas; Mühlberg, 2024, p. 70).

To address this issue, double-blind methods employ cryptographic mechanisms to ensure that neither the service provider nor the third-party verifier knows each other. These verifiers are usually certified by an authority that establishes the implementation specifications for the age assurance system (Gorin; Biéri; Brocas, 2022; PEREN, 2022, p. 10). The solution, however, requires the choice of an independent and reliable intermediary party to transmit the proof of age.

The collection of biometric data on a mass scale for the purpose of age estimation raises concerns regarding the proportionality of interference with the privacy rights and personal data protection. This is true especially when there is no guarantee that the data will not be reused for other purposes, such as surveillance, profiling, information filtering, and mass monitoring. In addition, storing this sensitive data poses risks of leaks. Furthermore, according to Law No. 15,211/2025, "data collected for age verification of children and adolescents may be used solely for this purpose, with its processing for any other purpose being prohibited" (Brazil, 2025c, Art. 13).

In addition to the issues mentioned, there are limitations to the method, as the user could display a photograph of another person, such as an adult, to circumvent the age check, which would render the collection ineffective. Another relevant point concerns the accuracy of the result verification, especially for users close to a certain threshold (e.g., 18 years old), which casts doubt on the accuracy of the mechanism, particularly when its adoption is required in high-risk scenarios (ICO, 2024b).

Estimation methods that assess user behavior require a lot of data that goes beyond age, which may also reveal other information about the data subject, leading to risks of massive data processing for profiling (Shaffique; Hof, 2024, p. 31). If this data is aggregated, it may also reveal the user's identity. Detailed profiles can be used for surveillance purposes or use by malicious actors (Sas; Mühlberg, 2024, p. 51). It is therefore necessary to balance the accuracy of these methods with security, protection of privacy, and personal data (EDRi, 2023, p. 24).

Estimating age through capacity tests eliminates the collection of personal data, but it is not very accurate and can lead to biases due to the difficulty in identifying an age based on the results of the responses given to the challenges. Each child's cognitive ability varies, and it is difficult to establish minimum knowledge requirements by age, based on an age group or school grade (Shaffique; Hof, 2024, p. 32), in addition to the risks of exclusion (Sas; Mühlberg, 2024, p. 58).

Although promising privacy-preserving techniques such as digital identities are under development, they still face security and inclusion challenges. To ensure a fair balance between protection and autonomy, Sas and Mühlberg (2024, p. 42) suggest conducting mandatory risk assessments and creating a clear regulatory framework to ensure that these technologies are implemented safely and responsibly. Also, there should be studies on alternative technical solutions such as reporting systems, filtering and warning of harmful content, incorporation of accessible panic buttons, and adoption of age-appropriate designs that prioritize privacy and security. From a social perspective, they highlight the importance of education and awareness for adults and children, and in-depth debate between policymakers and society.

The *Age Assurance Technology Trial* (Australia, 2025a), commissioned by the Australian government to assess the effectiveness, reliability, and privacy impacts of various age assurance technologies, aims primarily to protect children from online risks, such as exposure to pornography and age-restricted services or social networks. The report thoroughly analyzes age assurance technologies, by evaluating 48 providers and their solutions (such as age verification, estimation, and inference, parental control, and parental consent). The evaluation is based on international criteria, including accuracy, interoperability, reliability, ease of use, minimization of bias, data protection and privacy, and readiness for implementation.

The document also investigates how these technologies integrate into the digital ecosystem.

The conclusion of the trial was that age assurance is feasible and effective in Australia, without major technological barriers, with ready-to-use solutions that have been independently validated. It revealed that the sector is dynamic and innovative enough, driven by private investment, with a wide variety of options that can be adapted to different contexts, demonstrating that there is no one-size-fits-all solution. However, these conclusions were contested by Electronic Frontiers Australia (EFA), a digital rights organization that participated in the study's advisory board. EFA argued that claims that age assurance can be "private, efficient and effective" are "contradicted by the evidence" and criticized the methodology used to reach these conclusions (EFA, 2025). The organization highlighted specific concerns about technology providers that proactively established capabilities to retain personal and biometric data, anticipating possible requests from law enforcement or regulators, even when there are no legal requirements for such retention. EFA also criticized that the privacy compliance assessment was based simply on reading external privacy policies, characterizing this approach as "privacy washing."

The analysis points to challenges, such as the need to avoid excessive data retention by providers, which can pose significant risks to the right to privacy. However, the age assurance systems showed consistent performance across different demographic groups. The success of the trial assessment model, based on international standards, suggests that it could serve as the basis for the creation of an accreditation and certification system in Australia, ensuring that age assurance providers meet security standards and the required privacy in the country, which may serve as inspiration to other countries around the world.

EFA (2025) also expressed concern that the study could be used as justification for the wider implementation of digital identification technologies, characterizing the regulation of minimum age for social networks as a "trojan horse" due to the widespread adoption of digital ID.

Convergence of age assurance approaches

The growing presence of children and adolescents in the digital environment has challenged data protection authorities to rethink their regulatory approaches. In this scenario, several recent regulatory frameworks have gained relevance by proposing technical and legal paths for building more structured and effective protection for children online: the ISO/IEC 27566-1 standard (ISO; IEC, 2025) and *Age Appropriate Design*, published by the UK ICO (ICO, 2022), the Brazilian Data Protection Law (LGPD – Brazil, 2018), the Guide on the Use of Digital Devices (Brazil, 2025a), and Law 15,211, the ECA Digital (Brazil, 2025c).

The ISO/IEC FDIS 27566-1 standard (ISO; IEC, 2025) is an attempt to organize the different methods that can be used to identify a user's age in digital services. It proposes levels of assurance, which vary according to the degree of certainty and technical robustness. This classification is not restricted to systems engineering but is also directly linked to the risk level that the service may pose to a child. Thus, services that offer sensitive content, such as games with violent elements or open social networks, should operate with more rigorous age assurance mechanisms, while others, which pose less risk, may adopt lighter approaches. In establishing this logic of proportionality, the ISO 27566-1 standard (ISO; IEC, 2025) focus on privacy as a core value, as it proposes that age assurance mechanisms shall be designed to protect sensitive attributes, avoid unnecessary tracking, and minimize data collection.

The Age Appropriate Design Code, in force in the UK since 2021, is a code of conduct that sets standards for providers of information society services regarding default protection practices in services that are accessible to children, even if they are not explicitly intended for them. One of its most innovative points is in Standard 3 (ICO, 2022), which stipulates that services must know the age of the user with a degree of certainty appropriate to the risk involved, or else apply uniformly all child protection rules to all users.

Furthermore, the British code brings the concept of "best interests of the child" to the center of digital product design. This means that, by default, the service must operate with the maximum privacy possible, with disabled features such as geolocation, profiling, and sensitive data collection. LGPD, especially in Article 14, requires specific consent from at least one parent or legal representative, when this is the legal scenario, but also refers to the adoption of proportionate, transparent, and best practice-based measures. These elements are present in both ISO/IEC 27566-1 (2025) and the Age Appropriate Design Code (ICO, 2022). In addition, the Guide on the Use of Digital Devices, published in Brazil in 2025, reinforces these understandings by recommending that public policies seek technical methods of age assurance and protect, by default, children's browsing, and consumption of digital content (Brazil, 2025a).

Law 15,211/2025 (ECA Digital) establishes strict obligations to ensure the safety and privacy of children and adolescents in the digital environment. The law requires age assurance to be carried out by effective, proportionate, and auditable mechanisms, thus prohibiting simple self-declaration and allowing the government to act as a regulator. One of the central pillars is the principle of *privacy by design*: all products and services must operate with the maximum level of protection enabled from the outset. This protection extends to privacy, with the requirement for data minimization and geolocation restriction by default. In addition, the law prohibits the use of designs that manipulate users, compromising their autonomy, or inducing them to disable safeguards.

Regarding commercial exploitation and parental control, the ECA Digital expressly prohibits the profiling of children and adolescents' data for targeted advertising purposes, requiring social networks to clearly inform users of age restrictions. For parents and legal representatives, the law requires the provision of accessible parental tools, which must also operate with maximum protection by default and provide clear metrics of usage.

Table 3 illustrates similarities in understanding, comparing the main age assurance mechanisms in digital environments, based on the following references: standard ISO/IEC 27566-1 (ISO; IEC, 2025), *Age Appropriate Design Code* (ICO, 2022), Brazilian Data Protection Law (LGPD – Brazil, 2018), Guide on the Use of Digital Devices (Brazil, 2025a), and Law No. 15,211/2025, the ECA Digital (Brazil, 2025c).

Table 3 *Regulatory convergence among LGPD and SEDIGI/MJSP Screen Guide, ISO/IEC 27566-1, ICO Age Appropriate Design Code, and Law No. 15,211/2025.*

Aspect addressed	ISO/IEC 27566-1:2025 (ISO; IEC, 2025)	Age Appropriate Design (ICO, 2022)	LGPD Law No. 13,709/2018 (Brazil, 2018)	Screen Guide (Brazil, 2025a)	ECA Digital Law No. 15,211/2025 (Brazil, 2025c)
Age assurance	Defines three methods: age verification, age estimation, and age inference.	Standard 3: age appropriate application, with risk proportional verification	Art. 14: treatment of children's data requires consent of parents or by the legal representative and must use reasonable means to verify age.	Chapter 10 p. 135: recommend appropriate age verification mechanisms to prevent access to inappropriate content.	Arts. 9 and 10: effective age assurance mechanism, self-declaration is prohibited; Art. 11: public authorities may act as regulator/ certifier.
Risk-based and proportionality categorization	Establishes levels of guarantee (from basic to rigorous) according to the risk level.	Standards 2 and 3: DPIA and verification should consider risks to child.	Art. 50, §1: requires appropriate measures in accordance with the type of data and risks involved.	Chapter 10: indicates proportional use of methods and policies according to age groups.	Art. 12: proportional, auditable, and safe for age assurance.
Data minimization	Provides objectives such as 'minimization of attributes'.	Standard 8: collect only the minimum necessary for the service.	Art. 6, III: principle of necessity – to limit treatment to a minimum necessary.	Chapter 8: highlights the need to minimize data collection and prioritize anonymity.	Art. 12, §1: principle of minimization; prohibited unrestricted sharing.
Privacy by design and by default	Provides privacy as a pillar of the system.	Standard 7: default configuration must be high privacy.	Art. 6, VII: principles of security and protection of privacy; art. 46: security measures.	Chapters 6 and 10: recommend privacy by default as a digital design principle.	Art. 7: products should operate by default with maximum level of protection.
Transparency and informed control	Includes user awareness and transparency practices.	Standards 4, 10, and 15: clarity of the terms and warnings adapted to age.	Art. 9, 14, §6 and 18: right to clear and appropriate information about the treatment.	Chapters 4 and 10: guides that children should receive clear explanations and appropriate to age.	Art. 7, §1: clear information; Art. 24: social networks should inform age group restrictions.

Aspect addressed	ISO/IEC 27566-1:2025 (ISO; IEC, 2025)	Age Appropriate Design (ICO, 2022)	LGPD Law No. 13,709/2018 (Brazil, 2018)	Screen Guide (Brazil, 2025a)	ECA Digital Law No. 15,211/2025 (Brazil, 2025c)
Geolocation and traceability	Does not provide traceability as objective.	Standard 9: geolocation deactivated by default, with active warning.	Articles 12 and 13: measures for privacy protection must be adopted, including sensitive geolocation.	Chapter 5: geolocation should be avoided or controlled with transparency.	Art. 17, §4, VI: geolocation restriction implementation by default, clear warning.
Profiling and inference	Addresses reference as a method and requires trust indicators.	Standard 12: no profiling by default; Avoid harmful effects.	Art. 20: right to review automatic decisions; non-discrimination principles.	Chapter 7: alerts on profiling risks and improper use of behavioral data.	Art. 22 and 26: prohibited profiling for advertising or creation of profiles.
Persuasion techniques (nudges)	Not suitable for the collection or misuse of attributes without basis.	Standard 13: prohibits nudges that encourage the supply of excessive data.	Art. 6, IV and V: prevention and adequacy; prohibits unnecessary delivery of data.	Chapter 8: advises against the use of strategies that manipulate children's behavior.	Art. 17, §2: prohibits design that compromise autonomy or induces deactivation of safeguards.
Inclusion and accessibility	Recommend inclusion of different public, including vulnerable ones.	All over: recognizes different capabilities and access.	Art. 6, VIII: Principle of non-discrimination; Article 50: good practices and governance.	Chapter 3: policy inclusive practices should contemplate diversity and equitable access.	Art. 3: respect for progressive autonomy; Art. 17: accessible tools.
Right to information and access control tools	Provides clear practice statements and control by individuals.	Standard 15: accessible tools to exercise rights and report concerns.	Art. 18: right to access, correction, and portability guaranteed to the data subject and legal responsibility.	Chapter 9: reinforces the right to information, complaints, and access to personal data.	Art. 16 and 18: parental tools with maximum protection control by default, use metrics.

Source: own elaboration based on ISO/IEC (2025), ICO (2022), Brazil (2018, 2025a, 2025c).

As shown in Table 3, there is convergence among the regulatory frameworks compared, as well as complementarity, whose application assists with the development of policies, regulations, solutions, and the definition of requirements for age assurance mechanisms.

Age assurance principles

In this section, we present a collection of age assurance principles proposed by data protection authorities around the world[11] that are in the process of regulating or guiding age assurance in digital environments. We noticed that the definition of principles is one of the first steps in approaching the age assurance theme in some jurisdictions.

CNIL advocates the creation of online age assurance systems that do not compromise freedom of navigation. The French authority has established a set of key principles to guide the development of these systems, by ensuring that they are effective and respect the privacy of data subjects (CNIL, 2021). Age assurance in digital environments should be guided by an approach that balances security and privacy. Principles such as minimization, proportionality, robustness, simplicity, and proportionality are fundamental. Minimization ensures that data collection is limited to what is essential to prevent misuse, such as publicity. Proportionality ensures that the verification method is appropriate to the level of risk of the content, without unduly compromising user's privacy. Robustness requires that, in high-risk situations, verification be rigorous, going beyond self-declaration, while simplicity promotes easy-to-use solutions that integrate age verification and parental consent. Together, these principles aim to create a safer online environment for everyone, without sacrificing individual freedoms or the rights to privacy and personal data protection.

The European Commission (EC) has released a report establishing a comprehensive set of requirements for age assurance in digital environments, with the aim of protecting users, especially children and adolescents (Shaffique; Hof, 2024). The document is based on principles such as proportionality, privacy, security, and accuracy, by emphasizing that age assurance systems must be effective without compromising user freedom or privacy. The EC also highlights the importance of inclusion, transparency, and, notably, by listening to children's opinions in the development of these applications. The Commission is proposing the use of digital wallets as an age verification architecture, based on data protection principles such as data minimization, user-centricity, and security. This approach seeks to create a robust and secure system, ensuring that data subjects retain control over their personal data.

[11] *This proposal of principles or requirements for age verification mechanisms were collected from the following institutions: the Commission Nationale de l'Informatique et des Libertés (CNIL) in France, the European Commission (Shaffique; Hof, 2024), the European Data Protection Board (EDPB), ARCOM, the Spanish Data Protection Agency (AEPD) and the Comité de Personas Expertas de España, the e-Safety Commissioner, the Global Age Assurance Standards Summit, Ofcom, and finally The 5RightstFoundation, a pioneering British non-governmental organization in defining age assurance principles, whose principles underpinned the notion of digital innovation appropriate for contained in the IEEE 2089.1-2024 / IEEE Standard for Online Age Verification (IEEE, 2024).*

The principles established by institutions such as CNIL and the European Commission demonstrate a unified and careful approach to age assurance in digital environments. Both entities recognize the need to balance the protection of children and adolescents with freedom to browse the Internet. These entities argue that age assurance systems should go beyond simple self-declaration, similar to what is provided for in the ECA Digital. They need to be proportionate to the risk, robust enough to be effective, and at the same time simple to use. The focus on data minimization and personal data protection is central, aiming at personal data collection under the principles of minimization and necessity.

In 2024, the Organization for Economic Co-operation and Development (OECD) published the report "*Towards digital safety by design for children*," in order to guide governments and digital service providers in creating a safer online environment for children. The document highlights that child safety should be a priority, from the design of platforms and services. Thus, the OECD (2024) proposed the adoption of essential measures, such as the implementation of age assurance mechanisms, child-centered design, proactive harm detection, rigorous protection of personal data and privacy, the provision of adequate information, and the creation of effective customer support channels. In addition, the report emphasizes the importance of encouraging children's participation in decisions that affect them, by promoting a culture of digital safety and well-being.

In 2025, the European Data Protection Board (EDPB) issued the Statement 1/2025 on age assurance, with the aim of guiding the processing of personal data in this context, following the principles of GDPR. The statement establishes ten fundamental principles, focusing on ensuring that age assurance applications are proportionate and do not violate rights and freedoms. Among the main points are limiting the collection and use of data to the minimum necessary; risk assessment, data protection by design; and the security of such mechanisms. The document emphasizes the importance of ensuring lawfulness and transparency in all processes, in addition to the responsibility of service providers (EDPB, 2025).

The French media regulatory authority, ARCOM, published a guide in 2024 requiring online pornographic content services to implement reliable age assurance mechanisms. The guide does not impose a specific technology but establishes minimum requirements that systems must meet to be considered acceptable (ARCOM, 2024b). Among the requirements are: the independence of verification providers from content platforms; the guarantee of confidentiality for users; and the protection of personal data and privacy. The document also requires that the mechanisms be widely accessible to the population and that they clearly and explicitly demonstrate their level of privacy protection. The goal is to ensure that these services cannot operate in France without a robust system that protects user privacy and prevents children and adolescents from accessing inappropriate content.

In December 2023, the Spanish Data Protection Agency (AEPD) released a Decalogue of Principles for Age Verification, aimed at protecting children and adolescents from inappropriate online content. The agency defined a protection system that includes not only a verification mechanism, but also content classification policies, access filtering, and the display of which sites are age restricted. AEPD emphasized that these systems should avoid identifying and tracking children and adolescents, focusing on verifying the status of "authorized access" anonymously and only the content that is considered inappropriate. The document also reinforced the idea that digital education and content selection are a shared responsibility between families, governments, and industry, featuring the urgency of effective regulations and public policies (AEPD, 2023).

eSafety, Australia's online safety regulator, in collaboration with OAIC data protection agency, are working to strengthen the protection of children and young people in the digital environment. Based on the *Online Safety Act* of 2021, they published the *Roadmap for Age Assurance*, in 2023, a guide that proposes a regulatory framework, requiring digital platforms to adopt age assurance mechanisms to restrict access to pornography. The document also suggests the creation of an accreditation system for providers of these services, with the aim of ensuring principles such as privacy, security, transparency, and respect for human rights. The initiative, which includes consultations with society and educational actions, seeks a broad and holistic approach to mitigate the risks of exposing children to inappropriate content (Australia, 2023).

In 2023, Ofcom published a guide for providers of pornographic content to comply with Part 5 of the *Online Safety Act*, with the aim of preventing children from accessing these services. The document provides guidance on the implementation of age assurance methods, by listing examples of verification and estimation mechanisms. The main obligations include choosing and implementing methods listed in the guide, ensuring that the process is effective in identifying whether the user is a child, and that pornographic content will not be found by children and adolescents. In addition, the guide recommends that providers document and publish detailed information about the type of method used, how it works, and how privacy and data protection are ensured, which promotes transparency and accountability in the sector (Ofcom, 2023).

The UK organization 5Rights Foundation pioneered the establishment of principles for age assurance on the Internet, with a focus on protecting children and adolescents. Their established principles advocate the importance of recognizing children and their needs as Internet users, ensuring a child-centered approach to data use, and publishing terms of use in age-appropriate language. Based on these concepts, the Institute of Electrical Engineers and Electronics (IEEE) developed the technical standard IEEE 2089.1-2024 (IEEE, 2024), which details a set of 11 principles. The document emphasizes that age assurance must preserve privacy, be proportionate to risk, and be easy for children to use, accessible, and inclusive. It also highlights the need for verification providers to offer security, transparency, and channels for dispute resolution, while holding themselves accountable for their methods (5Rights, 2023).

The *Global Age Assurance Standards Summit*, organized by *the Age Check Certification Scheme* (ACCS), resulted in a *Communiqué* that established principles for age assurance: IEEE 2089.1-2024, with a focus on safety for children in the digital environment. The document is based on six principles: i) human rights and the best interests of the individual, requiring a balance between protection and empowerment; ii) proportional and risk-based implementation, which requires impact assessments prior to the adoption of systems; iii) privacy by design, with a preference for technologies such as zero-knowledge proof (ZKP) and data minimization; iv) standards-based interoperability, encouraging the use of international standardization norms such as ISO/IEC and IEEE; v) digital inclusion and accessibility, ensuring that applications are accessible to all; and vi) transparency, accountability, and innovation, which requires independent certification of systems and collaboration between regulators and industry to encourage compliance and the ethical development of new technologies (ACCS, 2025).

In summary, based on a comparative analysis of the international guidelines presented above, there is significant convergence in the principles that should guide age assurance systems on the Internet, especially regarding the protection of children and adolescents. In particular, the following stand out:

- **Privacy and data protection by default and by design**, as a structural axis of all age assurance systems;
- **Proportionality**, which requires that the level of assurance be appropriate to the risk of the service accessed, avoiding excessive data collection;
- **Minimization and limitation of purpose**, limiting data collection to what is strictly necessary for the purpose of age assurance and prohibiting secondary uses;
- **Transparency and accountability**, requiring users, especially legal representative, to be clear about the methods used and their impacts;
- **Risk management and information security**, ensuring the integrity, confidentiality, and availability of the data used in the verification processes;
- **Inclusion and accessibility**, ensuring the participation of children and adolescents in decisions and avoiding the digital exclusion of children without official documents or with socioeconomic limitations;

- **Human rights, non-discrimination, and equity**, as a guarantee that the methods used do not generate unjustified unequal treatment; and

- **Interoperability and technical robustness**, which facilitate standardization, regulatory compliance, and solutions of scalability.

In addition, there is a need for actively listening to children and adolescents in regulatory processes and for developing child-centered solutions that fully respect their digital rights, in accordance with the UN Convention on the Rights of the Child and the standard ISO/IEC 27566-1 (ISO; IEC, 2025). This global convergence indicates that regulatory efforts are moving not only to prevent children's access to inappropriate content, but also to foster a safe, ethical, and inclusive digital ecosystem, in which respect for children's rights is the starting point for technological innovation.

‹ age assurance in the brazilian context ›

In Brazil, with the enactment of Law No. 15,211 of September 17, 2025, known as ECA Digital or the Digital Statute of the Child and Adolescent, Brazil consolidated a specific regulatory framework for the protection of children and adolescents in digital environments. Chapter IV of the Law provides detailed provisions on age assurance mechanisms, by establishing obligations and parameters that directly address the concept of age assurance. Among the innovations of the law, the following stand out:

- The requirement that digital application and service providers adopt robust and auditable age assurance mechanisms to prevent children and adolescents from accessing content, products, and services that are inappropriate for their age group, prohibiting self-declaration;

- The provision that assurance mechanisms must be guided by privacy protection, data minimization, and proportionality, prohibiting excessive collection or the use of data for purposes other than age assurance;

- The possibility for public authority to act as regulator, certifier, or promoter of technical age assurance solutions, ensuring that such mechanisms are reliable, transparent, and secure;

- The establishment of rules for the inspection, accountability, and sanctioning of suppliers who fail to comply with age assurance standards, strengthening coordinated action between the ANPD and other competent bodies.

In Brazil, many initiatives have paved the way to drafting legislation to protect children and adolescents in digital environments. Of particular note are the resolutions of the National Council for the Rights of Children and Adolescents (CONANDA): Resolution No. 245 (Brazil, 2024a), which stands for children and adolescents rights in the digital environment; and Resolution No. 257 (Brazil, 2024b), which establishes the general guidelines of the National Policy for the Protection of the Rights of Children and Adolescents (PNPDCAAD), with the objective of "[…] ensure the absolute priority of the children and adolescents rights in the digital environment" (Brazil, 2024b). In particular, from the perspective of privacy and data protection, the policy establishes the principles of ensuring the protection of personal data, informational self-determination and the right to privacy and the prevention of excessive use as elements to be considered from the design phase of digital products and services (*privacy by design*) and by default (*privacy by default*), with the adoption of the most protective settings available (Brazil, 2024b).

Similarly, Article 17, §3 of CONANDA Resolution No. 245 (Brazil, 2024a) establishes that "service providers must create and improve mechanisms that prevent the use of digital services and environments by children and adolescents whenever their services are not appropriate and safe for this audience." In turn, Article 19 states that

> *effective age verification mechanisms in digital services and environments accessible to children and adolescents must be available to prevent children and adolescents from accessing platforms, products, services, and content that are illegal or incompatible with their age (Brazil, 2024a).*

In Article 19, Resolution No. 245 establishes that "data on children and adolescents obtained by age verification mechanisms and systems may not be used for any other purpose other than age verification" (Brazil, 2024a).

PNPDCAAD is structured around ten thematic axes (Brazil, 2024b, Article 4). In particular, we highlight the axe of defining and publishing guidelines and references for parental mediation mechanisms for the use of technology products or services, by application providers, in collaboration with the Ministry of Justice's Indicative Classification Policy Coordination and the Internet Steering Committee.

ANPD case study: age verification inspection process

In March 2021, ANPD's General Coordination of Inspection began an action regarding the collection and processing of personal data by the TikTok platform. The process was triggered from questions raised about the feature called "anonymous TikTok viewer," which allowed feed without registration, and about the sharing of data provided in the company's Privacy Policy.

Based on information provided by the questions raised and the platform itself, ANPD inspected LGPD compliance practices. It concluded that the age verification mechanism adopted was fragile, allowing navigation without account registration and resulting in improper processing of personal data of children and adolescents. Furthermore, they evaluated the age verification measures applied in the platform's age gate version and they understood that, used in isolation, they were not sufficient measures, since self-declaration alone does not constitute a mechanism capable of preventing access by children and adolescents (ANPD, 2023b).

As a follow-up to the TikTok case, in 2024, ANPD conducted a new analysis, which concluded that the identified irregularities up to that point provided sufficient evidence of violations of LGPD requirements, thus starting a sanctioning process for the proper investigation of these violations. Among the irregularities identified there were failures in age verification during and after registration on the platform and the data processing carried out in the "anonymous TikTok viewer" feature. It thus determined the whole suspension of the "anonymous TikTok viewer" feature until adequate age verification mechanisms were in place, and the production of a compliance plan in accordance with Article 36 of LGPD, which must be clear and comprehensive, containing details of objectives, the execution deadlines, the corrective actions necessary to reverse the identified irregularities, the criteria for monitoring and following up on the adopted measures, as well as the expected path to achieving the desired results. The details of this analysis are available for further information. (ANPD, 2024b).

‹ prospects ›

The use of age verification assurance mechanisms for children and adolescents in digital environments is an essential requirement for attesting age, security control, privacy, and data protection of this age group in digital environments. Age assurance is a theme present in the agenda of most regulatory agencies and governments worldwide, so that digital service providers comply with their principles and compliance requirements. This movement has been driving the digital identification industry to develop applications that meet the demands of users, the market, and especially governments. Therefore, the market of Internet products and services must seek solutions that adopt age assurance and comply with existing standards and regulatory frameworks, while enabling a safe user experience in these environments. Current applications are quite varied, and there is no universal technology or mechanism that serves all contexts.

Law No. 15,211/2025 (Brazil, 2025c), the Digital Statute of the Child and Adolescent (ECA Digital), Brazil's new law published in 2025, highlights the need to standardize technical requirements aimed at the development of certified age assurance applications that combine security, personal data protection, and accessibility. The law also reinforces the role of the Government as a regulator, a certifier, and a promoter of technologies, by strengthening the governance mechanisms of digital platforms. Furthermore, its integration into the LGPD enforcement system corroborates the complementarity of these legal frameworks and the regulatory functions of ANPD.

At the international level, two recently released documents are also noteworthy. First, *The legal and policy landscape of age assurance online for child safety and well-being* (OECD, 2025) analyzes the legal and political context in OECD member countries. Age assurance laws were grouped into three main categories: i) age-appropriate service delivery, which applies protections for different age groups in mixed-audience services (often in online safety laws); ii) hard age limits, which prohibit access below a certain age (such as online pornography or the purchase of age-restricted goods); and iii) privacy and data protection legal frameworks, which require parental consent or create special protections for children's data.

According to the study (OECD, 2025), despite increasing regulation, the legal context is complex and often confusing, with age assurance requirements that can be explicit (mandatory use of mechanisms) or implicit (inferred from the need to protect children, but without requiring a specific mechanism). Although the 27 OECD countries require special data protection for children, and 33 require parental consent, the minimum age required for these limits varies widely (between 13 and 18 years). For the category of strict limits, protections are uneven: although almost all countries ban access to pornography, only twenty-three have specific laws for online content, and only five of them include detailed age assurance requirements. There is a widespread lack of specificity in how to comply with these requirements, but implementation guidelines are emerging from online safety and privacy regulators.

The second released document we wish to comment about is the *Social Media Minimum Age: Regulatory Guidance* (Australia, 2025b), prepared by *the Office of the eSafety Commissioner*, the independent Australian authority responsible for enforcing the *Online Safety Act* of 2021. The document gives concrete form to the amendment promoted by *the Social Media Minimum Age Amendment* of 2024, which sets 16 as the minimum age for having accounts on social media platforms. As of December 2025, these services are required to take *"reasonable steps"* to prevent people under the age of 16 from using these environments.

In addition to defining technical methods, the document (Australia, 2025b) establishes guidelines based on principles such as reliability, proportionality, privacy by design, accessibility, and transparency, reinforcing the idea that age assurance should not be conceived isolated, but as part of a digital governance system linked to systemic risk assessments, transparency reports, and safeguards of fundamental rights. Among the relevant innovations presented in the guide, three types stand out:

1. the adoption of the principle of successive validation, which encourages the combined and sequential use of multiple age assurance methods (document verification, biometric estimation, behavioral inference) to reduce errors and biases;

2. the prohibition of exclusively requiring government documents or credentials from the national digital identity system, always requiring the provision of proportionate alternatives; and

3. the introduction of severe sanctions, including fines, public disclosure of violations, and direct accountability of executives.

By prioritizing independent audits, objective performance metrics, and safeguards against evasion attempts, the Australian document (Australia, 2025b) marks a significant turning point: it shifts the debate from an approach focused solely on technical solutions to an integrated regulatory model in which technological innovation, personal data protection, and corporate accountability are systematically linked. This arrangement highlights a paradigm shift, by bringing age assurance closer to a continuous regulatory governance regime, capable of inspiring future regulatory strategies in Brazil.

In summary, age assurance tends to evolve from a merely programmatic guideline into a fully enforceable legal duty subject to inspections. This movement will transform age assurance into a structural requirement of the digital ecosystem, directly impacting the design, the development, and the provision of products and services aimed at children and adolescents, in line with the principles of comprehensive protection and their best interests.

Privacy by design is one of the solutions for age assurance that will guide the development of new products and services. New tools and solutions will be incorporated into digital environments with technologies that ensure the security and confidentiality of age assurance data.

Regarding technical standards or international standards, the works of the IEEE (2024) and ISO (2025) on age assurance also stand out and will inspire and guide the entire market in developing solutions for this purpose. With the launch of these standards, other complementary standards are likely to emerge and address increasingly specific issues.

The European Union proposed an age verification model, called the "mini wallet," which is now under development (European Commission, 2025a). This solution allows users to prove that they are over 18 without sharing further personal information. In addition, it is compatible and interoperable with the *EU Digital Identity Wallet*, a continental identity solution to be used by all European citizens, scheduled to be launched by the end of 2026 (European Commission, 2025b). However, EDRi has estimated that the eID *wallet* could exclude around 20% of users (EDRi, 2023, p. 30).

‹ final considerations ›

The complexity of the digital environment requires a continuous and multifaceted effort to ensure the safety and well-being of children and adolescents. As demonstrated, the protection of this audience is not limited to a single measure, but rather to a set of actions involving legislation, technology, and public policies.

However, the implementation of these protection mechanisms is full of challenges, such as the need to balance security with the protection of personal data and privacy. The search for age assurance solutions must respect principles such as data minimization, avoiding the unnecessary collection of sensitive information, such as biometrics. Therefore, the main challenge is to develop technologies that effectively protect children and adolescents, preserve their fundamental rights, and align with the best interests of the child.

In this context, advisory committee initiatives and international collaboration are crucial to improving requirements for age assurance mechanisms. Joint work between public authorities, civil society, and industry is essential to creating a digital environment that promotes the full development of children and adolescents, allowing them to safely enjoy the benefits of the Internet. Age assurance thus emerges as a key piece in this ecosystem, functioning as the main tool to promote awareness for the protected and responsible exercise of digital rights.

‹ references ›

5RIGHTS FOUNDATION. **Child online safety toolkit**. London: 5Rights Foundation, 2023. Available at: https://childonlinesafetytoolkit.5rightsfoundation.com/wp-content/uploads/2022/05/5Rights-Child-Online-Safety-Toolkit-English.pdf. Accessed on: May 5, 2025.

ACCS. **Summit Comuniqué Final**: Global Age Assurance Standards Summit – Summit Communiqué. Amsterdam: ACCS, 2025. Available at: https://accscheme.com/wp-content/uploads/Summit-Communique-Final-Document-May-2025.pdf. Accessed on: July 1, 2025.

AEPD. **Decálogo de principios: verificación de edad y protección de personas menores de edad ante contenidos inadecuados**. Madrid: AEPD, 2023. Available at:: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf. Accessed on: Jan. 25, 2025.

ALANA. **Glossário**: Sharenting. c2025. Available at: https://alana.org.br/glossario/sharenting/ Accessed on: Oct. 6, 2025.

ANPD. **Enunciado CD/ANPD nº 1, de 22 de maio de 2023**. Brasília, DF: ANPD, 2023a. 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. Accessed on: Apr. 30, 2025.

ANPD. **Guia orientativo hipóteses legais de tratamento de dados pessoais – legítimo interesse**. Brasília, DF: ANPD, 2024a. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 22 Jan. 2025.

ANPD. **Nota Técnica nº. 50/2024/FIS/CGF/ANPD**. Brasília, DF: ANPD, 2024b. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nt-50-pub.pdf. Accessed on: 30 Abr. 2025.

ANPD. **Nota Técnica nº. 6/2023/CGF/ANPD**. Brasília, DF: ANPD, 2023b. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/tiktok-nota_tecnica_6_versao_publica.pdf. Accessed on: 30 Abr. 2025.

ANPD. **Portaria ANPD nº 35, de 4 de novembro de 2022**. Torna pública a Agenda Regulatória para o biênio 2023-2024. Brasília, DF: ANPD, 2024c. Available at: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Accessed on: 8 jan. 2025.

ANPD. **Resolução CD/ANPD nº 10, de 05 de dezembro de 2023**. Aprova o Mapa de Temas Prioritários para o biênio 2024-2025 e dispõe sobre a periodicidade do Ciclo de Monitoramento. Brasília, DF: ANPD, 2023c. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528. Accessed on: Apr. 30, 2025.

ANPD. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 27 jan. 2022. Available at: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Accessed on: Apr. 30, 2025.

ARCOM. **Pratiques médias des mineurs et exposition aux contenus inappropriés**. Paris: ARCOM, 2024a. Available at: https://www.arcom.fr/sites/default/files/2024-11/Arcom-Pratiques-medias-des-mineurs-et-exposition-aux-contenus-inappropries-etude-qualitative-resultats-detailles.pdf. Accessed on: Jan. 15, 2025.

ARCOM. **Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques**. Paris: ARCOM, 2024b. Available at: https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf. Accessed on: Jan. 15, 2025.

AUSTRALIA. Department of Infrastructure, Transport, Regional Development, Communications and the Arts. **Age Assurance Technology Trial**: Part A: Main Report. Stockport: Age Check Certification Scheme, 2025a. Available at: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf. Accessed on: Sept. 1, 2025.

AUSTRALIA. E-Safety Commissioner. **Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography**. Austrália: Australian Government, 2023. Available at: https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf. Accessed on: May 8, 2025.

AUSTRALIA. E-Safety Commissioner. **Social Media Minimum Age**: Regulatory Guidance. Australia: Australian Government, 2025b. Available at: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1757990720895. Accessed on: Sept. 29, 2025.

AVPA. **Definitions**. c2025. Available at: https://avpassociation.com/definitions/. Accessed on: May 7, 2025.

BRAZIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed on: June 9, 2025.

BRAZIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Accessed on: Dec. 20, 2024.

BRAZIL. **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, DF: Presidência da República, 2025c. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15211.htm. Accessed on: Sept. 22, 2025.

BRAZIL. Ministério da Justiça e Segurança Pública. **Crescer em Paz: Estratégia de Justiça e Segurança Pública para Proteção de Crianças e Adolescentes**. Brasília, DF: MJSP, 2025b. Available at: https://criaprevencao.com.br/wp-content/uploads/2025/04/Crescer-em-Paz-Estrategia-de-Justica-e-Seguranca-Publica-para-Protecao-de-Criancas-e-Adolescentes_Versao-Digital-.pdf. Accessed on: May 22, 2025.

BRAZIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 925, de 10 de abril de 2025**. Institui o Comitê Consultivo para formulação de proposta de metodologia e requisitos mínimos de verificação etária em serviços digitais que podem ser acessados por crianças e adolescentes. Brasília: Imprensa Nacional, Seção 1, 2025e. Available at: https://dspace.mj.gov.br/bitstream/1/14869/2/PRT_GM_2025_925.pdf Accessed on: May 22, 2025.

BRAZIL. Ministério da Justiça e Segurança Pública. Secretaria de Direitos Digitais. **Nota Técnica nº 4/2025/SEDIGI/MJ** – Verificação Etária em Serviços Online. Brasília: Ministério da Justiça e Segurança Pública, 2025d. Available at: https://www.gov.br/mj/pt-br/assuntos/noticias/drci-seleciona-chefe-de-divisao-para-cooperacao-jurid… Accessed on: May 22, 2025.

BRAZIL. Ministério dos Direitos Humanos e da Cidadania. **Resolução nº 245, de 05 de abril de 2024**. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Brasília, DF: MDHC, 2024a. Available at: https://www.gov.br/participamaisbrasil/blob/baixar/48630. Accessed on: Jan. 8, 2025.

BRAZIL. Ministério dos Direitos Humanos e da Cidadania. **Resolução nº 257, de 12 de dezembro de 2024**. Estabelece as diretrizes gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: MDHC, 2024b. Available at: https://www.gov.br/participamaisbrasil/blob/baixar/61597. Accessed on: Jan. 8, 2025.

BRAZIL. Secretaria de Comunicação Social. **Crianças, adolescentes e telas: Guia sobre usos de dispositivos digitais**. Brasília, DF: SECOM, 2025a. Available at: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Accessed on: May 19, 2025.

BSI. **PAS 1296:2018: Online age checking. Provision and use of online age check services. Code of Practice**. Londres, 31mar. 2018. Available at: https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice?version=standard. Accessed on: July 10, 2025.

CAGLAR, Cansu; NAIR, Abhilash. **EU Member State Legal Framework**. [*S.l.*]: euCONSENT, 2021. Available at: https://euconsent.eu/download/eu-member-state-legal-framework/. Accessed on: Sept. 2, 2025.

CNIL. **Online age verification**: balancing privacy and the protection of minors. Paris, 22 set. 2022. Available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors. Accessed on: Nov. 27, 2024.

CNIL. **Recommendation 7**: Check the age of the child and parental consent while respecting the child's privacy. Paris, 9 ago. 2021. Available at: https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy. Accessed on: Nov. 27, 2024.

EDPB. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation**. Brussels: EDPB, 2023. Available at: https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf. Accessed on: Sept. 2, 2025.

EDPB. **Joint Opinion 4/2022**: on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. Brussels: EDPB, 2022. Available at: https://www.edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf. Accessed on: Sept. 2, 2025.

EDPB. **Statement 1/2025 on Age Assurance**. Brussels: EDPB, 2025. Available at: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf. Accessed on: May 5, 2025.

EDRI. **Online age verification and children's rights**. Brussels: EDRI, 2023. Available at: https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf. Accessed on: Nov. 27, 2024.

EFA. **Age Assurance Technology Trial Final Report Released**. Camberra: EFA, 2025. Available at: https://efa.org.au/age-assurance-technology-trial-final-report-released/. Accessed on: Sept. 13, 2025.

EUROPEAN COMMISSION. **eIDAS Regulation**. Brussels: 2025c. Available at: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. Accessed on: Sept. 23, 2025.

EUROPEAN COMMISSION. **EU Age Verification Solution**. Brussels, 2025a. Available at: https://ageverification.dev/. Accessed on: June 16, 2025.

EUROPEAN COMMISSION. **Overall Architecture – European Age Verification Solution: Operational, Security, Product and Architecture Specifications**. Brussels: European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT), 2025d. Available at: https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/. Accessed on: Oct. 6, 2025.

EUROPEAN COMMISSION. **The EU approach to age verification**. Brussels, 2025b. Available at: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification. Accessed on: Sept. 9, 2025.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [...]**. Brussels, 2016. Available at: https://eur-lex.europa. eu/eli/reg/2016/679/oj/eng. Accessed on: Oct. 5, 2025.

FERNANDES, Elora. Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. *E-book*. Available at: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Accessed on: Oct. 5, 2025.

FOSI. **Coming to Terms with Age Assurance**. Washington: FOSI, 2023. Available at: https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf. Accessed on: 5 mai. 2025.

GORIN, Jérôme; BIÉRI, Martin; BROCAS, Côme. **Demonstration of a privacy-preserving age verification process**. França: Laboratoire d'Innovation Numérique de la CNIL, 2022. Available at: https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process. Accessed on: Sept. 3, 2025.

ICO. **Age appropriate design**: a code of practice for online services. Wilmslow: ICO, 2022. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Accessed on: Nov. 28, 2024.

ICO. **Age assurance for the children's code**. Wilmslow: ICO, 2024b. Available at: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/. Accessed on: June 12, 2025.

ICO; IFF RESEARCH. **How online businesses are using age assurance**: Research findings. Wilmslow: ICO, 2024. Available at: https://ico.org.uk/media2/migrated/4030926/20240704-ico-age-assurance-report.pdf. Accessed on: June 11, 2025.

IEEE. **IEEE 2089.1-2024**: IEEE Standard for Online Age Verification. New York: IEEE, 2024. Available at: https://standards.ieee.org/ieee/2089.1/10700/. Accessed on: Oct. 5, 2025.

ISO; **IEC. ISO/IEC FDIS 27566-1**: Information security, cybersecurity and privacy protection — Age assurance systems: Part 1: Framework. Geneva: ISO, 2025. Available at: https://www.iso.org/standard/88143.html#lifecycle. Accessed on: Oct. 5, 2025.

LIVINGSTONE, Sonia; POTHONG, Kruakae. **Child rights by design: guidance for innovators of digital products and services used by children**. London: Digital Futures Commission; 5Rights Foundation, 2023. Available at: https://eprints.lse.ac.uk/119724/. Accessed on: Nov. 4, 2024.

LIVINGSTONE, Sonia; STOILOVA, Mariya; RAHALI, Miriam. **Realising children's rights in the digital age**: The role of digital skills: Principle 4: Age appropriate: Develop policies and products that are age appropriate by design and consider using age assurance. Leuven: KU Leuven; ySKILLS, 2023. Available at: https://eprints.lse.ac.uk/121075/1/4_Age_appropriate.pdf. Accessed on: June 16, 2025.

NACIMENTO, Natália Castro Reis; BERNARDES, Rochele Juliane Lima Firmeza. Perfis Infantis no Instagram: A Responsabilidade Civil dos Pais e da Plataforma Diante da Violação dos Direitos Personalíssimos. Teresina, **Revista FSA**, v. 22, n. 2, fev. 2025. Available at: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/3095/491494663 Accessed on: Apr. 30, 2025.

NIC.BR. **TIC Kids Online Brasil 2023**: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasi. São Paulo: NIC.br, 2024. Available at: https://cetic.br/media/docs/publicacoes/2/20240913124019/tic_kids_online_2023_livro_eletronico.pdf. Accessed on: Dec. 5, 2024.

NIC.BR. **TIC Kids Online Brasil 2024**: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: NIC.br, 2025. Available at: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Accessed on: Apr. 25, 2025.

OECD. **The legal and policy landscape of age assurance online for child safety and well-being**: Technical paper. Paris: OECD, 2025. Available at: https://www.oecd.org/en/publications/the-legal-and-policy-landscape-of-age-assurance-online-for-child-safety-and-well-being_4a1878aa-en.html. Accessed on: July 1, 2025.

OECD. **Towards digital safety by design for children**. Paris: OECD, 2024. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children_f1c86498/c167b650-en.pdf. Accessed on: Sept. 2, 2024.

OFCOM. **Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services**: Annex 2. London: OFCOM, 2023. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272586-consultation-guidance-for-service-providers-publishing-pornographic-content/associated-documents/annex-2-guidance-for-service-providers-publishing-pornographic-content-online?v=368675. Accessed on: May 5, 2025.

OFCOM. **Guidance on highly effective age assurance**: For Part 3 services. London: OFCOM, 2025. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680. Accessed on: May 5, 2025.

OFCOM. **Quick guide to children's access assessments**. London: Ofcom, 2024. Available at: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-access-assessments. Accessed on: May 5, 2025.

OLSZEWSKI, Bruna Dezevecki. **Overshareting e Responsabilidade Parental**: a necessidade de proteção da criança no ambiente digital e da conscientização sobre o uso das redes sociais. São Paulo: Dialética, 2025. Available at: https://books.google.com.br/books?id=8cxJEQAAQBAJ&lpg=PR97&dq=lgpd%20garantia%20de%20idade%20crian%C3%A7as%20e%20adolescentes&lr&hl=pt-BR&pg=PP5#v=onepage&q=lgpd%20garantia%20de%20idade%20crian%C3%A7as%20e%20adolescentes&f=false. Accessed on: Apr. 30, 2025.

PENTEL, Avar. Predicting user age by keystroke dynamics. In: COMPUTER SCIENCE ON-LINE CONFERENCE, 7., 2018, [s.l.]. **Proceedings** [...]. Cham: Springer, 2018. p. 336-343. Available at: https://link.springer.com/chapter/10.1007/978-3-319-91189-2_33#citeas. Accessed on: Oct. 5, 2025.

PEREN. **Détection des mineurs en ligne**: peut-on concilier efficacité, commodité et anonymat? France: Pôle d'expertise de la régulation numérique, 2022. Available at: https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf Accessed on: Oct. 6, 2025.

SAFERNET. **O que é ciberbullying?**. [2019?]. Available at: https://new.safernet.org.br/content/o-que-e-ciberbullying Accessed on: Oct. 6, 2025.

SAS, Martin; MÜHLBERG, Jan Tobias. **Trustworthy Age Assurance?** A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. Brussels: The Greens/EFA in the European Parliament, 2024. Available at: https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance. Accessed on: Aug. 20, 2025.

SHAFFIQUE, Mohammed Raiz; HOF, Simone van der. **Research report**: Mapping age assurance typologies and requirements: Executive summary. Luxembourg: European Commission, 2024. Available at: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements. Accessed on: Oct. 5, 2025.

SPAIN. Ministerio de Juventud e Infancia. Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. **Informe del comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia**. Madrid: Ministerio de Juventud e Infancia, 2024. Available at: https://www.juventudeinfancia.gob.es/sites/default/files/noticias/Informe%20del%20comit%C3%A9%20de%20personas%20expertas%20para%20el%20desarrollo%20de%20un%20entorno%20digital%20seguro%20para%20la%20juventud%20y%20la%20infancia.pdf. Accessed on: Apr. 5, 2025.

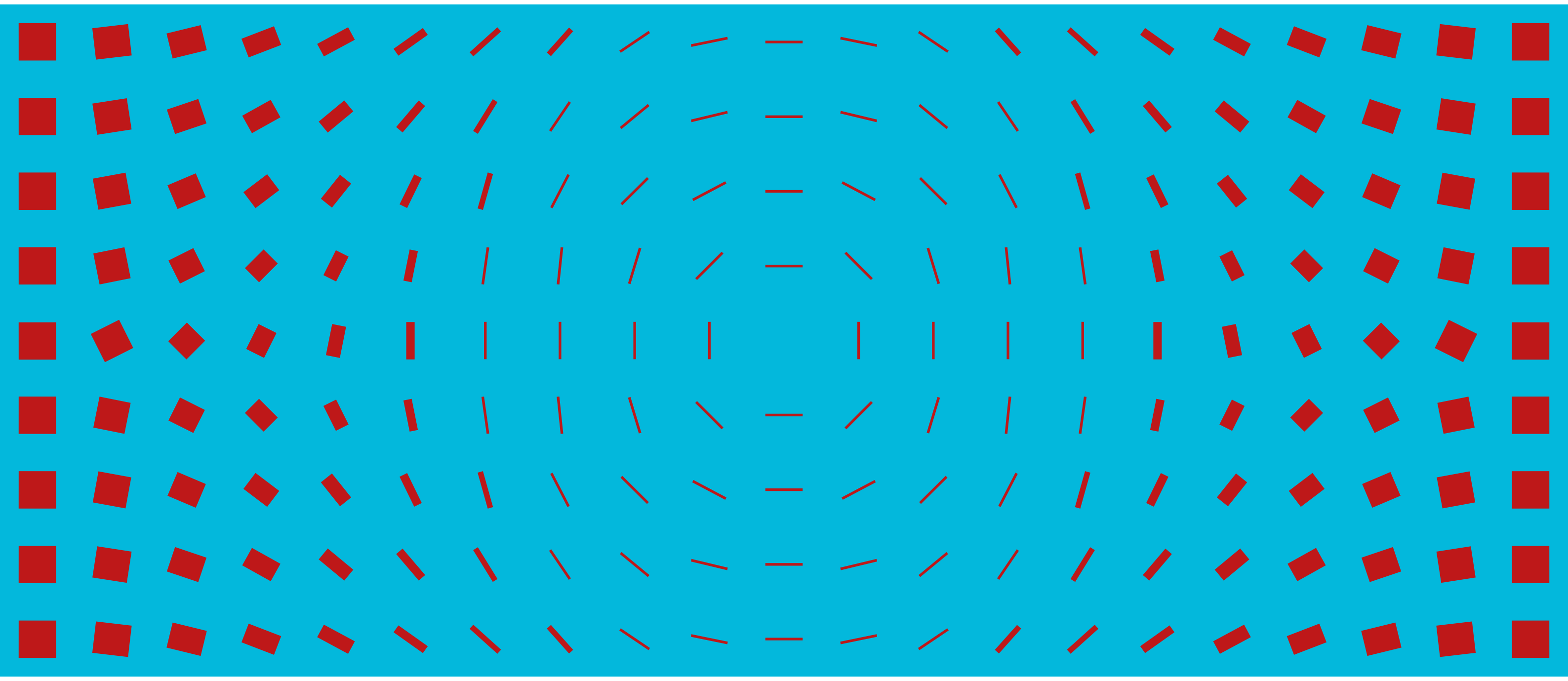
STEINBERG, Stacey. Sharenting: Children's privacy in the age of social media. [*S.l.*], **Emory Law Journal**, v. 66, n. 4, p. 839-884, 2017. Available at: https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/. Accessed on: May 13, 2025.

UN. Committee on the Rights of the Child. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration *(Art. 3, para. 1)***. Geneva: United Nations, 2013. Available at: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Accessed on: May 2, 2025.

UN. Committee on the Rights of the Child. **General comment No. 25 (2021) on children's rights in relation to the digital environment (seção E)**. Geneva: UN, 2021. Available at: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=ZFIB6YHG%2FGsPZWN0RxLScHq9GiMBdnF6%2FJbmpl3osWkgGhvw49aL7h%2B8Vn0mCi2e0q8gmJS2YdjNrWEF706%2FDw%3D%3D. Accessed on: May 2, 2025.

W3C. **Verifiable Credentials Data Model 2.0**. W3C Recommendation, 1 May 5, 2025. [*S.l.*]: W3C, 2025. Available at: https://www.w3.org/TR/vc-data-model/. Accessed on: Aug. 20, 2025.

www.gov.br/anpd



ANPD