[IT] AGCOM adopts draft regulation on age verification

IRIS 2024-9:1/10

Francesco Di Giorgi
Autorità per le garanzie nelle comunicazioni (AGCOM)

On 24 September 2024, the Italian Communications Authority (AGCOM) approved the regulatory framework governing technical and procedural methods for verifying users' age (age assurance, or age verification), as outlined in Article 13-bis of Decree-Law No. 123 of 15 September 2023, converted with amendments by Law No. 159 of 13 November 2023 (the so-called *Decreto Caivano*).

More specifically, Article 13-bis of the *Decreto Caivano* (Provisions for Age Verification for Access to Pornographic Websites) introduced a prohibition in Italian law on minors accessing pornographic content, as such content “undermines respect for their dignity and compromises their physical and mental well-being, constituting a public health issue”. This provision requires website operators and video-sharing platform providers that distribute pornographic images and videos in Italy to verify the age of their users so as to prevent minors under the age of eighteen from accessing such content.

AGCOM has been assigned the task of defining the technical and procedural methods that website operators and video-sharing platform providers must adopt to verify users' age, ensuring an adequate level of security proportional to the risk and respecting data minimisation principles in relation to that purpose. The final regulation is the result of a public consultation initiated by means of Resolution No. 61/24/CONS, which included the participation of various stakeholders, such as other institutions, industry associations, consumer groups, and video-sharing platforms (see IRIS 2024-4:1/6). Additionally, the Data Protection Authority (*Garante per la protezione dei dati personali*) provided a favourable opinion during and after the public consultation phase.

The regulatory scheme, qualifying as a technical rule under Article 1, paragraph 1, letter f) of Directive (EU) 2015/1535, has been immediately notified to the European Commission, in accordance with the procedure provided by the aforementioned directive. Its entry into force is therefore subject to the expiration of the 90-day standstill period starting on 16 October 2024, as well as any comments that the Commission and other Member States may provide during that period.

The technical specifications adopted in the regulation outline an age verification system that uses the "double anonymity" model. Therefore, providers of age

verification tools are not allowed to (1) know for which service the age verification is being conducted, (2) know whether two age verifications come from the same source, or (3) know whether a user has already used the system before.

The system designed by AGCOM involves the participation of certified independent third parties for providing age verification, through a process that includes two logically separate steps: (1) identification and (2) authentication of the identified person, every time the regulated service is used (i.e. the provision of pornographic content via website or platform).

The age verification process is divided into three distinct phases (excluding systems based on applications installed on the user's device):

1. The first phase involves the issuance, e.g. by accessing a website via a browser, of a "proof of age", following identification, issued by various parties who are independent of the content provider and who know the Internet user. These could be digital identity providers or organisations that have identified the user in another context. The entity providing the "age verification proof" does not know how the user will use it and must be certified by a public body to ensure the reliability of the identification system used.

2. The second phase involves communicating the age verification proof, which is transmitted exclusively to the user, who will then present it to the visited website or platform. The "age verification proof" can, for example, be downloaded directly by the user through the certifier's website and then sent by the user to the visited website or platform.

3. Finally, the last phase concerns the website or platform visited by the user, which will analyse the age verification proof presented and grant or deny access to the requested content (authentication).

In the case of systems based on applications installed on the user's device, the third-party entity providing the age verification will make an app available for certifying and generating the "age verification proof" (e.g. digital identity wallet apps or digital identity management apps). The user can then authenticate and provide the age verification proof directly to the website or platform using the installed app and the service dedicated to this purpose.

AGCOM has adopted a technologically neutral approach, leaving regulated entities responsible for implementing age assurance systems with reasonable freedom to evaluate and choose the specific processes.

AGCOM has also established several principles and requirements that must be met by the implemented systems, including:

- Proportionality: a fair balance between the means used for age verification and their impact on individual rights.

- Data protection (confidentiality requirement): age assurance systems must comply with data protection laws and principles established by the GDPR (minimisation of data, accuracy, storage limitation, etc.); therefore, systems involving the processing of personal data, such as ID documents, photos or videos of the user, credit card information, or user profiling, are not permitted.

- Security: the age assurance system must take into account potential cyberattacks and include sufficient security measures to mitigate risks (in compliance with the GDPR and the proposed Cyber Resilience Act – CRA); it must also prevent circumvention attempts.

- Accuracy and effectiveness: the system must be effective in minimising errors in age determination. Age assurance must be conducted each time the website or platform sharing pornographic content is accessed. The validity of an age verification ends when the user leaves the service, the session ends, the browser is closed, or the operating system enters standby mode, and in any case, after 45 minutes of inactivity.

- Functionality, accessibility, ease of use, and non-interference with access to Internet content: age assurance systems must be user-friendly and appropriate for the capabilities and characteristics of minors.

- Inclusivity and non-discrimination: age assurance systems should avoid or minimise unintended biases and discriminatory outcomes for users.

- Transparency: regulated entities should be transparent with users regarding the systems and data processed, with clear, simple, and comprehensive explanations for both adults and minors.

- Education and information: AGCOM emphasises the importance of informing and raising awareness among minors, parents, educators, and youth workers about good digital practices and the risks associated with the Internet.

- Complaint management: service providers must offer at least one channel for receiving and promptly handling complaints regarding incorrect age decisions.

Finally, AGCOM has mandated that the technical methods described above should also apply to other types of content that could harm the physical, mental, or moral development of minors, beyond pornographic material. Additionally, AGCOM has planned the establishment of a technical committee to monitor and analyse technological, legal, and regulatory developments in age assurance systems.

Schema di provvedimento su modalità tecniche e di processo per l'accertamento della maggiore età degli utenti

https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-del-07-ottobre-2024

Draft regulation on the technical and procedural methods for verifying users' age

TRIS - Notification detail

https://technical-regulation-information-system.ec.europa.eu/en/notification/26368