PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS ON VIDEO-SHARING PLATFORM SERVICES FOR CONTENT THAT IS HARMFUL FOR MINORS.

Proceedings: INF/DTSA/329/23

I. BACKGROUND

Spanish Law 13/2022 of 7 July on General Audiovisual Communication (Ley General de Comunicación Audiovisual; hereinafter LGCA) extended the subjective scope of regulated agents. This extension means that, in addition to audiovisual media service providers, video-sharing platform service providers must also comply with this regulation.

The aim of this extension is to guarantee that minors are protected from harmful content, as well as to protect viewers in general from content that incites violence, hatred or the committing of a crime, especially terrorism.

Article 89 of the LGCA imposes a series of obligations on these new agents, including the requirement to implement age verification systems for access to their platforms, as the gold standard measure for protecting minors from harmful audiovisual content.

With the goal of ensuring the implementation of this new regulation is as effective as possible, this Commission considers it appropriate that this public consultation, aimed at the different agents involved -providers, verifiers, child-development-related associations, researchers and other groups-, will allow us to obtain information on state-of-the-art in age verification systems as well as their advantages and disadvantages, which will result in a better application of the regulation.

II. COMPETENCE

The competence of the CNMC to intervene stems from the provisions of the sectoral regulations and, in particular, from Law 3/2013, creating the Spanish National Markets and Competition Commission (hereinafter, the CNMC Law).

Pursuant to Article 9 of the CNMC Law, this Commission is responsible for supervising and controlling the "*correct functioning of the audiovisual communication market*".

In particular, point 9 of the aforementioned Article 9 of the CNMC Law establishes that one of the Commission's functions is to "*Supervise and monitor compliance with the obligations imposed on the providers of video-sharing platform services, in accordance with the provisions of Title V of Law 13/2022, of 7 July, General Audiovisual Communication.*"

Furthermore, Article 93.1 of the LGCA establishes that the CNMC is responsible for monitoring compliance by providers of video-sharing platform services with the obligations established in Title V, relating to the provision of video-sharing services on platforms, and in its implementing provisions.

Similarly, Section 3 of Article 93 states that the CNMC, following a mandatory and non-binding report from the Spanish Data Protection Authority, must assess the suitability of the measures referred to in Articles 89, 90 and 91 adopted by the providers of video-sharing platform services, including the implementation of age verification systems (Article 89.1.e. of the LGCA).

III. COMMUNICATION OF PUBLIC CONSULTATION

In accordance with the above and pursuant to the provisions of aforementioned Article 9 of the CNMC Law and in exercise of the competences in the audiovisual sector provided for in Article 25.1 b) of the CNMC Law and in Article 21 of the Organic Statute of the CNMC (approved by Royal Decree 657/2013, of 30 August), a participatory process is hereby initiated which aims to gather the different opinions and suggestions of the agents in the audiovisual sector on which criteria and recommendations may be used to achieve the greatest possible effectiveness in the implementation of measures for the protection of minors in the area of the provision of video-sharing platform services.

To this end, the CNMC invites all interested parties to express their views on those aspects which they consider important or which affect them, by answering the questions set out in the attached document, which will be published on our website.

Responses to the questions posed and comments should be sent electronically through the CNMC's electronic site https://sede.cnmc.gob.es no later than 31 January, 2024.

The answers submitted will be public unless expressly requested and their confidential nature is justified, in which case a censored or non-confidential version of the written submissions must be attached, in which personal data will also be omitted.

This document is electronically signed by Alejandra de Iturriaga Gandini, Director of the Telecommunications and Audiovisual Sector of the Spanish National Markets and Competition Commission.

ANNEX

PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS IN VIDEO-SHARING PLATFORM SERVICES FOR CONTENT HARMFUL TO MINORS

I. Introduction

The development of new electronic communications networks has led to the emergence of new services and the greater visibility of existing ones, as has been the case with video-sharing platforms (hereinafter, VSPs). These agents, whose legal nature is that of an information society service, have reduced the distance between the creator of the content and the end consumer, favouring and promoting the widespread consumption of these services.

The existence of freely accessible and unrestricted VSPs aimed at disseminating content which by its nature is harmful to minors, such as violence or pornography, is a matter of social concern. Particularly when the consumption of this type of content is made available to minors, given that it may alter their capacity for understanding and impair their physical, mental or moral development.

In this context, it is particularly important to note that the development of the new European audiovisual regulatory framework included the obligation for VSPs to establish measures that guarantee the protection of minors and, in particular, measures to prevent minors from accessing particularly harmful content. These obligations were incorporated into Spanish law through the LGCA of 7 July, 2022.

II. Characterisation of video-sharing platforms

The LGCA has empowered this Commission to supervise those websites that meet the legal definition of a "video-sharing platform" or VSP.

Article 2.13 of the LGCA defines a video-sharing platform service as a service whose principal purpose, or one of its dissociable parts or whose essential functionality consists of providing, to the general public, by means of electronic communications networks, programmes, user-generated videos, or both, for which the video-sharing platform provider does not have editorial responsibility, for the purpose of informing, entertaining or educating, as well as broadcasting commercial communications, and the organisation of which is determined by the provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.

From the interpretation of the aforementioned Article, it follows that a service is considered to be a video-sharing platform service when the following seven requirements are cumulatively met[1]:

A) The service provided involves an economic activity.

B) The owner of the service is not editorially responsible for the content disseminated therein, but does organise the content by automatic means.

C) The service must be aimed at the general public.

D) The service is intended for entertainment purposes.

E) The principal purpose of the service, or of one of its separable parts, or as an essential functionality, is the distribution of audiovisual content.[2]

F) The service distributes audiovisual programmes, user-generated videos, or both.

G) It is provided over electronic communications networks.

Additionally, it should be taken into consideration that, in accordance with the Country of Origin Principle[3], only VSPs established in Spain are obliged to comply with the LGCA and are, therefore, susceptible to supervision by the CNMC.[4]

Conversely, VSPs established in other Member States are not subject to supervision by the CNMC.

III. Scope of action of the CNMC

As mentioned above, the Audiovisual Directive, aware of the role and importance of VSPs in people's lives, included them as new subjects subject to the

[1] In the following cases, the CNMC has provided an appraisal of the practical appplication of these seven requirements: IFPA/DTSA/147/22, IFPA/DTSA/266/22 and REQ/DTSA/002/23.
[2]In the case where more than one service is provided, the analysis should take into account the Guidelines on the practical application of the essential functionality criterion of the definition of "video-sharing platform service" under the Audiovisual Media Services Directive (2020/C 223/02) of 7 July, 2020.
[3] The Country of Origin Principle mandates that only one Member State, the one in which the audiovisual provider is established, has jurisdiction over the audiovisual media services broadcast by that provider, irrespective of where it is broadcast. This is because the aim of this principle is to provide legal certainty (a necessary foundation for the implementation of new business models) and the provider is only bound by the rules of the Member State of origin, which has harmonised legislation, and thus avoids having to comply with additional controls in each Member State of reception. Article 28 bis 1 of the Audiovisual Directive makes it clear that this principle also applies to providers of video-sharing platform services: *"1. For the purposes of this Directive, a video-sharing platform provider established in the territory of a Member State within the meaning of Article 3.1 of Directive 2000/31/EC shall be under the jurisdiction of that Member State."*
[4] The establishment of VSPs in Spain is set out in Sections 3 to 6 of Article 3 of the LGCA.

obligations for the protection of minors and designated the independent audiovisual regulators as the competent organisations for their supervision.

Thus, Article 88 of the LGCA indicates that VSPs must adopt measures to protect minors from audiovisual content that may impair their physical, mental or moral development and protect the general public from audiovisual content that incites violence, hatred or discrimination or that contains a public provocation to commit a crime.

Although all the obligations to be fulfilled by VSPs are included in Articles 89, 90 and 91 of the LGCA, in this public consultation this Commission is focusing on those new obligations that will guarantee adequate protection of minors against the most harmful content for that collective, such as violence and pornography, and which are specifically provided for in the regulations for these subjects.

Specifically, this consultation will focus on the measures provided for in Articles 89.1.e) and 91.1 of the LGCA referring to the use of age verification systems to prevent minors from accessing inappropriate content and commercial communications:

- Article 89.1: *"(e) Establish and operate age verification systems for users with respect to content that may impair the physical, mental or moral development of minors which, in any case, prevent minors from accessing the most harmful audiovisual content, such as gratuitous violence and pornography."*

- Article 91.1: *"Video-sharing platform service providers must ensure that the audiovisual commercial communications that they market, sell or organise comply with the provisions of Section 1 of Chapter IV of Title VI (...). In any case, commercial communications that promote harmful or detrimental behaviour for minors must require age verification and access for users of legal age."*

It should be noted that the implementation of age verification systems is the exact and specific tool that the legislator has specifically required of VSPs offering the most harmful content, such as violence or pornography, in order to prevent minors from accessing their content, without undermining possible access to this content by adults.

Article 93 of the LGCA on "supervision and control" determines that the CNMC is the authority responsible for monitoring the compliance of VSPs with the obligations established for them. In the exercise of this task, this Commission will assess the suitability of the age verification systems adopted by VSPs, following a mandatory and non-binding report from the Spanish Data Protection Authority (Agencia Española de Protección de Datos; hereinafter, AEPD). In other words,

the CNMC is the national authority designated by the legislator to rule on the effectiveness of these mechanisms, taking into account the criteria of the AEPD with regard to the compatibility of such mechanisms with data protection.

To highlight the importance that the legislator has placed on the obligation to establish age verification mechanisms, it should be noted that Section 4 of Article 93 of the LGCA expressly states that *"failure to comply with the obligations set out in Article 89.1(e) will constitute the offence defined in Article 157.8, without prejudice to the criminal liability that may derive from such action"*. In other words, it reiterates that the lack of these age verification mechanisms may constitute a criminal offence as well as a very serious administrative offence.

IV. Subject of the consultation

Having set out the existing problems that are subject to the supervision of this Commission, characterised the regulated subjects, and outlined the scope of action that derives from the limits imposed by the Law, it is necessary to determine the subject matter of this public consultation.

Of all the measures envisaged in the LGCA, this Commission considers that the measure to establish and operate age verification systems particularly impacts the protection of minors when it comes to video platforms that offer content that may be very harmful to this collective, such as violence or pornography. It is therefore submitting different aspects of this obligation to consultation in order to clarify its application, as already announced in its 2023 Action Plan[5].

This initiative seeks to identify those criteria that contribute to protecting minors from the most harmful content, such as violence and pornography on VSPs, and which will be taken into account when carrying out a detailed analysis of the systems that must be implemented by VSPs established in Spain. By specifying these criteria, the aim is to increase the legal security and predictability of this Commission's agreements, stating the minimum and essential elements that age verification systems must have in order to be considered to comply with the objective set out in the LGCA[6].

---

[5] Within Strategic Line 4: *"Terms and Conditions for Efficient, Transparent and Autonomous Management"*, in the section on Telecommunications and Audiovisual communication: https://www.cnmc.es/sites/default/files/editor_contenidos/Notas%20de%20prensa/2023/Plan_Act_2023%20_web_oficina.pdf

[6] The EU Consent Project has pointed out that more concrete guidelines and guidance from the relevant regulatory authorities would be useful for the effective enforcement of laws requiring age verification tools. *EU Member State Legal Framework. WP2: Existing Methods, User Needs and Requirements*. September 2021. p. 6. In this regard, the German regulator *Kommission für Jugendmedienschutz* (Commission for the Protection of Minors in the Media or KJM) has set criteria for assessing the suitability of age verification systems and the French audiovisual regulator *Autorité de régulation de la communication audiovisuelle et numérique* (ARCOM) is legally empowered to formulate such criteria. In this respect see: Art. 3 *Décret no*

To this end, it is considered essential to carry out the following public consultation and thereby elicit the different opinions of the actors involved, be they researchers, service providers, associations linked to child development, trustworthy verifiers, users in general or other groups.

V. Issues for public consultation

The CNMC invites all interested parties to comment on the issues that they consider important or that affect them by answering the questions set out below, as well as by raising any other issues that they consider to be of interest.

7.1. On the material scope of the obligation to establish and operate age verification systems to prevent access by minors

The LGCA mentions two cases in which age verification systems would be applicable.

On the one hand, Article 89.1.e) of the LGCA stipulates that VSPs must *"Establish and operate age verification systems for users with respect to content that may impair the physical, mental or moral development of minors which, in any case, prevent minors from accessing the most harmful audiovisual content, such as gratuitous violence and pornography."*

On the other hand, in relation to audiovisual commercial communications marketed, sold or organised by VSPs, Article 91.1 of the LGCA establishes that *"[i]n any case, commercial communications that promote harmful or detrimental behaviour for minors must require age verification and access for users of legal age."*

Commercial communications offered by the VSPs in question follow the same pattern as the main content of their services, namely, they are freely accessible and explicit images are used in their presentation.

In general, the advertising offered by these providers encourages behaviour that is equally harmful to minors, since in many cases the advertising refers to pornography sites, medicines of dubious origin, violent or sexually explicit video games, dating sites, or direct contact telephone numbers for sexual services.

2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

From the above, it follows that access to commercial communications managed by these VSPs may also encourage behaviour that is harmful or detrimental to minors.

Consequently, it seems justified that the obligation to establish and operate age verification systems should apply to all audiovisual content, including commercial communications managed by VSPs subject to Article 89.1 e).

Question 1: Do you consider it appropriate to establish age-verification mechanisms for all audiovisual content, including advertising, by VSPs providing more harmful content?
Question 2: Should the age verification system be implemented before accessing any content offered by the VSP, or would it be sufficient to include such a verification system at a later stage, when accessing the actual audiovisual content, making it possible to access a censored version of the content without having passed through the verification system?

7.2. On the minimum elements of age verification systems preventing access by minors

Based on an analysis of the different age verification services carried out by this Commission, as well as on the experience of regulators in our environs, especially in France and Germany, this Commission is in a position to set out a series of minimum elements that it understands the different age verification systems must meet in order for this Commission to be able to classify them as suitable in accordance with the requirement set out in Articles 89.1.e) and 91.1:

- **The age verification system must ensure, at all times, that the person accessing and consuming the harmful content is of legal age.**

The age verification systems implemented by VSPs must ensure that the person accessing is of legal age.

Access to this type of services tends to be recurrent. For this reason, it will be necessary to guarantee that the person who -in the first instance- accredits that they are of legal age is also the only person who will be able to use this accreditation to access the service in the future.

In other words, the verification system must guarantee that the person who wants to access the content is really the person identified as being of legal age, avoiding possible cases of identity theft or violation of the system, so that minors cannot use adult documents to access the content.

Identification and authentication can be carried out on the basis of accreditation based on identity documents or digital certificates. In some cases with prior registration, where there is age-verified identification of the registered person and a subsequent check that this person (previously identified) is the one who is being authenticated to access the service.

When assessing different age verification mechanisms, it may be understood that these solutions will consist of two phases[7]: the first corresponds to the unique identification of the person, and the second to an authentication confirming that the previously identified person is the one accessing the adult service in each subsequent use.

The first step of **unique identification** concerns the necessary personal identification with age verification. It should be noted that this could be anonymous identification, when it is a matter of accrediting legal age, without the verification needing to know the name or any other personal data.

In order to collect identification and age verification data, it has traditionally been necessary to carry out a face-to-face check and use official identity documents (national identity card, residence card, passport), comparing the photograph or fingerprint.

However, the technological progress observed in the formulation of this type of solution seems to make the need for a face-to-face check dispensable when using digital identity mechanisms that have reached an appreciable degree of reliability.

Consequently, solutions that rely on a personal contact for identification with age verification, as well as solutions that do so by electronic means could be considered appropriate, provided that such verification avoids the risk of falsification and circumvention. In any case, it is up to the provider to decide which age verification mechanisms to implement for their service, and ultimately up to each user to choose from among the possibilities offered to them.

It seems reasonable to discard as inadequate certain solutions such as the mere presentation or sending of a copy of the identity document, as well as the identification and age verification via the presentation of a photograph, as these do not present adequate safeguards.

[7]The German regulator *Kommission für Jugendmedienschutz* (KJM), an organisation with more than 20 years of experience in supervising access to audiovisual and information society services, has established criteria for evaluating age-verification systems. You can access their criteria here: https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022__004_.pdf (en alemán).

To conclude this unique identification step, it is also necessary to ensure the correct transmission of access keys to the user, in accordance with the use that each particular solution makes of these. If the keys are not given to the user personally during the registration process or are generated during this process, but their delivery or other subsequent transmission is required, it must be ensured that the access keys are only transmitted to the person identified as being of legal age.

The second **authentication** step is to ensure that only the respectively identified and age-verified person has access to the service in question.

For this purpose, authentication must take place at the start of each use or login process and access to content must be dependent on an individually assigned authentication element.

Furthermore, given that in most solutions, after the unique identification, the user, who is recognised as being of legal age and therefore authorised, receives a form of "password" for all subsequent usage processes, the authentication step is intended to make it more difficult to pass on access authorisations to unauthorised third parties.

Disclosure or multiplication of passwords can be prevented by technical measures that make it difficult to multiply access authorisations, but also by informing the user of the personal risks of unauthorised use of their password, such as financial risks (for use of bank accounts associated with their access) or risks involving the disclosure of secrets (sensitive user information).

Question 3: Do you consider it appropriate for each provider to decide on the age verification mechanisms it implements in its service and, if so, should it ultimately be up to each user to choose the most convenient of the systems offered?
Question 4: What are your views on the general approach to solutions that may or may not be based on face-to-face control?
Question 5: How can the correct transmission of access passwords to the pre-identified user be ensured? How can the disclosure or multiplication of access authorisations be adequately prevented?

- **The system must be robust and accurate in order to avoid possible impersonation.**

In this respect, it is important that the system accurately determines the age of the person seeking access.

Irrespective of the type of identification implemented, it is essential that the elements of judgement applied make it possible to ensure that the identified person is of legal age.

In the case of personal identification, which, as noted above, may not be efficient at the present time, this step would seem to be insured by *in situ* verification of whether or not the person requesting identification is of legal age.

For cases of identification by electronic means, the solutions could even present a certain risk of error.

In this respect, if such a system were to be adopted, the solution must be transparent and take into account this risk of error to ensure that the person accessing the content is of legal age.

Question 6: If electronic identification is implemented, what are the risks of the system providing erroneous results?
Question 7: What other solutions could ensure accuracy and precision when identifying and specifying the age of the person requesting access?

- **Technological neutrality**

Given the different ways of accessing pornographic, violent and other harmful content, the age verification system should be capable of being used on any technological device and operating system, in such a way that minors are unable to circumvent or bypass the controls and access the content.

Question 8: ¿Do you consider that it is more appropriate for the protection of minors that the age verification system should be the same or horizontal regardless of the access device or operating system used or, conversely, do you feel that there are significant differences in these elements that would recommend an age verification system adapted to each access device or operating system?
Question 9: What technological drawbacks or limitations can you foresee in the implementation of age verification systems?

7.3. Regarding available technological solutions for age verification

As this Commission has stated in several pronouncements, simply declaring to be of legal age without any subsequent verification does not provide an adequate level of security to prevent minors from accessing this content[8].

There are currently age verification solutions on the market that could be effective. The validity of a technological age verification solution is dependent on how reliably it prevents minors from accessing content. These must also, in any case, comply with personal data protection regulations.

These solutions can be broadly grouped into two types. Below, the main characteristics of each will be set out, specifying, where appropriate, the possible disadvantages of each.

Note that the use of online age verification mechanisms is not exclusive to accessing adult audiovisual content, but is also used in other areas such as the purchase of alcohol or tobacco over the internet and for accessing online gambling services.

A. Age verification by means of an ID card or a digital certificate deriving from this

Age verification can be carried out by checking a traditional physical identity document, a physical electronic identity document, or a digital identity document. These documents could be, for example, ID cards, passports, residency certificates (EU citizens), residence cards (non-EU citizens), or a digital or virtual identity medium not based on a physical document.

Similarly, as an alternative to identity per se, it is possible to envisage the use of coming-of-age credentials, such as those envisaged in the eIDAS2 Regulation[9], which is expected to be adopted soon, based on digital identity. In this way, this legal age can be independently accredited without the need to disclose further information about the user, in accordance with the principle of minimisation, and preserving the user's anonymity.

In terms of authentication, face-to-face or remote procedures based on keys, fingerprints, or the person's photograph could be used. Some authentication

[8] In the following cases, the CNMC has pointed out that self-declaration of legal age is not an effective measure to prevent minors from accessing harmful content: IFPA/DTSA/147/22, IFPA/DTSA/266/22 and REQ/DTSA/002/23.
[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a Framework for a European Digital Identity. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0281.

solutions involve bringing one's face close to the camera of the device with which the age verification request is being made, to ensure that a photograph is not used.

In face-to-face solutions, adults of legal age can obtain adult-only cards, whereby they obtain a username and password that would give them access to age-restricted content. Such cards would be offered at certain points of sale, such as supermarkets or tobacconists, whose staff are familiar with age controls relating to the sale of alcohol or cigarettes. The main disadvantage is that such a measure introduced only for viewing pornographic or violent sites could stigmatise the interested party and discourage its use. Another disadvantage would be the resale of cards on a parallel market.

Any of these mechanisms could be implemented through apps, e.g., apps for the most common smartphone operating systems, that facilitate identification and authentication. This facility could be a feature of digital identity wallets.

As noted above, it is ultimately up to the user to choose one or other mechanism.

B. Age verification via bank card

In existing solutions of this type, users enter their name and bank card details (card number, expiry date, CVC code), and this data is checked against a payment database to verify that the card is valid.

This could be a simple check that the number provided is in the correct format, a request for pre-authorisation of a payment, or a micro-payment to obtain the highest level of certainty.

In general, this system protects younger children (under 10-12 years of age) who do not have a bank card that allows them to make an online payment and who are less likely to use a third party's card.

The disadvantage of this solution is that it offers a lower level of security, as minors may be in possession of bank cards that allow them to make purchases on the internet[10]. Another disadvantage is that bank cards may not be accessible to everyone as they are usually linked to a certain income.

Question 10: What do you consider to be the strengths and weaknesses of each of the age verification systems described? Are there any other

[10] However, it is true that the protected universe is extended when considering that there are bank cards for minors on the market that have their online payment functionality capped, according to the decision of those responsible for the minor.

mechanisms in addition to those considered that you consider suitable for verifying age?
Question 11: How do you assess the different systems considered, taking into account the desirable balance between reliability, protection of personal data and cost?
Question 12: What should the audit safeguards be for each of these systems, so that the CNMC can verify that they are complying with the expected reliability?

7.4. On the organisations that could carry out age verification

Age verification can be carried out by the provider itself or by an independent third party. The latter has certain advantages for the provider, such as outsourcing a service that can be complex to perform, but primarily by not discouraging the use of the services by those adults who are more reluctant to give their data to VSPs.

In this sense, independent age verification organisations can also be used to purchase alcohol or tobacco, or to enable online gambling. And, in addition to the examples given above for proof of legal age, third-party verifiers are widely used by telecommunications companies and banking organisations in order to validate their customers' data before entering into online contracts[11].

In this way, the third party providing proof of age knows the internet user's identity or age attribute, but does not know which site the latter is visiting, and the service holder knows that the user is of legal age, but does not know any other personal or identity-related information about the user[12].

Although it follows from the above, it is necessary to clarify that the user must know whether the third party is independent of the owner of the service to which access is sought.

In any case, account should be taken of the negative incentives that could be generated by economic links between the third parties and the service holders, and extreme vigilance should be exercised where the provider itself carries out

[11] At the international level, social media such as Instagram are also adopting age verification systems for their users. INSTAGRAM. Introducing new ways to verify age on Instagram. June 2022. See: https://about.instagram.com/es-la/blog/announcements/new-ways-to-verify-age-on-instagram.

[12]The French data protection agency, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), has taken the same line, although its proposal is based on reasons linked to the protection of personal data. See: https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

the age verification.

Question 13: What is your assessment of a third-party organisation independent of the VSP carrying out age verification versus the provider itself? How do you think it would affect their sales success if a VSP did not offer users the possibility of age verification through an independent third party?
Question 14: How do you think the user can be informed about the fact that age verification is carried out by an independent third party?

7.5. On additional aspects to be fulfilled by age verification

Aspects related to the nature of the content and the type of consumption that may condition or place special requirements on age verification systems have been discussed throughout this document.

In this sense, there may be additional aspects related to the security of age verification mechanisms, such as the existence of backdoors, the maximum duration of a session or the time limit for considering inactivity, which may also be considered relevant when deciding whether an age verification system is appropriate.

An additional aspect to be taken into account among all the possibilities available on the market for age verification is to choose a service that adequately collects age data in the least intrusive way possible, respecting the privacy of individuals. This issue, as established in Article 90 of the LGCA, should be analysed by the Data Protection Agency, and is therefore not an aspect on which this Commission believes it should take a position.

For this reason, the Commission would like to know which other issues specific to these services should be taken into account in the market to which this public consultation is addressed.

Question 15: Which specific aspects relating to access procedure, type of consumption, duration of stay or duration of access to harmful content through VSPs should be taken into account when implementing age verification systems?
Question 16: How often do you consider that the system should request the renewal of the user's accreditation?
Question 17: Of the aspects identified in the previous question, which do you consider to have an impact on the effectiveness of age verification measures? Please explain your answer.

7.6. On co-regulation

The LGCA is primarily committed to the use of complementary mechanisms to traditional regulation in order to increase the legal security of the sector's agents, as well as to achieve a higher level of protection and safeguards for the users of audiovisual services, especially minors.

In this sense, as stated in the LGCA's Explanatory Memorandum, *"the role that effective self-regulation and co-regulation can play as a complement to the legislative, judicial and administrative mechanisms in force and their valuable contribution to achieving the objectives of this law and, in particular, to the protection of users, should not go unrecognised. Likewise, in a sector as dynamic as the audiovisual sector, self-regulation and co-regulation mechanisms contribute to achieving the legal objectives insofar as they allow the obliged parties themselves, namely audiovisual media service providers and video-sharing platform service providers, to advance in their commitments to protect the user as necessary beyond what is initially foreseen by the regulations."*

Based on this consideration, Articles 12 and 14 of the LGCA regulate self-regulation and co-regulation, respectively. For its part, Article 15 sets out the promotion, characteristics and scope of self-regulatory and co-regulatory codes of conduct.

Article 15.1 of the LGCA states that *"the competent audiovisual authority must promote the use of the self-regulation and co-regulation provided for in the two previous articles through the voluntary adoption of codes of conduct drawn up by audiovisual media service providers, video-sharing platform service providers or the organisations representing them, in cooperation, where necessary, with other interested parties such as industry, commerce, professional or user associations or organisations."*

Among the codes which, according to Article 15.4 of the LGCA, must be promoted by the authorities, both at state and regional level, is the one set out in Section k) relating to the *"Protection of users with regard to content containing gratuitous violence and pornography."*

In view of the above, this Commission would like to know from the sector the following:

Question 18: Do you consider that co-regulation can be a useful tool to help establish such age verification systems to ensure the safety of children and the agents who implement them?

Question 19: What incentives or disadvantages are there in using co-regulatory systems to implement age verification systems in this area?
Question 20: Are you aware of any co-regulatory arrangements in this area? If so, please attach or forward appropriate information for consideration.

7.7. Other issues and contributions

Question 21: Are there any other issues that you consider should be addressed in the scope of this consultation?