Decalogue of principles

Age verification and protection of minors from inappropriate content

December 2023

aepd agencia española protección datos

I. Framework for the protection of minors

The United Nations Convention of 20 November 1989 on the Rights of the Child enshrines the child's best interests as a principle to which its signatory states will take care of all measures affecting them.

The Committee on the Rights of the Child, which monitors the implementation of the Convention, in General Comment No. 15, 2013, on the right of minors to the enjoyment of the highest attainable standard of health, pointing out in paragraph 38, and at such an early date, the problems that excessive use of the Internet is generating in minors by:

"The Committee is concerned by the increase in mental ill-health among adolescents, including developmental and behavioural disorders; depression; eating disorders; anxiety; psychological trauma resulting from abuse, neglect, violence or exploitation; alcohol, tobacco and drug use; obsessive behaviour, such as excessive use of and addiction to the Internet and other technologies; and self-harm and suicide."

And in his General Comment No. 25 of 2021 on the rights of the minors in relation to the digital environment points out, in paragraph 96, the obligation of States to protect minors in their use of digital games or social networks:

"States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector, to prevent the spread of misinformation and materials and services that may damage children's mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights."

The Organic Law 3/2018, of December 5, on the Protection of Personal Data and the guarantee of digital rights establishes in its article 84.1, "*Protection of minors on the Internet*", the role that those who have parental authority must also have in protecting minors concerning the use of the Internet:

1. Parents, guardians, curators, or legal representatives shall ensure that minors make a balanced and responsible use of digital devices and information society services in order to ensure the proper development of their personality and preserve their dignity and fundamental rights.

Some specific data may explain the current situation concerning minors and their Internet use. For example, the National Institute of Statistics survey on Internet use in households in 2022 shows that 90 % of the population under the age of 10 uses the Internet, a percentage that rises to 98.3 % at the age of 15 and that a third of them use the Internet more than 5 hours a day. Transparency Market Research[1] estimated in 2021 that the underage-oriented digital marketing market was $2.9 billion, with a growth outlook of 21 % annually.

Save The Children published studies in 2020 that show that 62.5 % of the adolescent population between 13 and 17 years have consumed pornography, that the average age of onset in consumption is set at 12 years, that 54 % consider pornography a source of inspiration for their sexual relations and 55 % want to put it into practice, performing sexting[2] 20 %. This situation is causing problems in the neurodevelopment of minors, in their attention capacity, in their learning, in their emotional development and in the emergence of aggressive attitudes in an irreversible way.

Considering this situation, the Spanish Data Protection Agency has promoted, together with the Attorney General's Office, the proposal for a State Pact[3] enabled by civil society organizations involved in the rights of children and adolescents.

[1] https://www.transparencymarketresearch.com/kids-digital-advertising-market.html

[2] Sending via mobile phone or other device photographs or videos produced by oneself with sexual connotation.

[3] https://digitalforeurope.eu/pacto-personas minors-online.

II. Age verification within a system for the protection of minors from inappropriate content

The European Commission, in its 2022 Communication on the new strategy for a Better Internet for Kids[4], advocates and supports effective age verification methods as a matter of priority[5]. The best practices and guidance in this Communication should be taken[6] into account, as set out in Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation or DSA).

In Spain, the 2022 General Audiovisual Communication Law[7] requires, as measures for the protection of minors from certain audiovisual content, that providers of video-sharing services through a platform must establish and operate systems of age verification of users concerning content that may harm the physical, mental or moral development of minors and that, in any case, prevent their access to the most harmful content such as free violence or pornography[8]. The appropriateness of these measures must be assessed by the National Commission for Markets and Competition following a mandatory report from the AEPD[9].

A. Definition of terms

The Convention on the Rights of the Child provides that:

Article 1 *For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.*

The DSA, in Recital 89, establishes the requirement to protect minors from content that may impair their physical, mental, or moral development.

Throughout this document the term "minor" or "minors" will be used for those persons who, depending on their age (under 14 years of age, under 18 years of age or other cases depending on the situation) must be protected from inappropriate content, and the term "adult" will be used in the opposite sense.

The term "inappropriate content" shall be used for websites restricted to adults only, content classified as "over 18" (pornography, extreme violence), Internet sites limited to access by users over 14 years, and harmful, addictive or advertising content prohibited to minors.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A digital decade for children and young people: the new European strategy for a better internet for children (BIK+). Com(2022) 212 Final of 11 May 2022.

[5] Paragraph 5.1.

[6] Recital (71).

[7] Law 13/2022, of 7 July, General of Audiovisual Communication.

[8] Art. 89(1)(e).

[9] Art. 93(3).

B. System for the protection of minors from inappropriate content.

The purpose of protecting minors on the Internet is to protect them from uncontrolled access to inappropriate content, which means that the ultimate goal is different from verifying their age or subjecting them to surveillance and monitoring. Inappropriate content for minors must be freely accessible to those users who, having decided to access them, can prove that they meet the established age conditions.

Verifying the user's age is only the first step in a system to protect minors from inappropriate content. This system will consist of the following elements:

- An age verification mechanism which will provide specific information on the authorization of access to adult-oriented content.
- Policies for the qualification of sites and content for reasons of age, which will allow a criterion of which sites on the Internet, or what content on generalist sites, are considered adult-oriented or have established age-based access limitation requirements.
- A rating of the sites, or the contents, according to and applying the previously established policies. This qualification implies the implementation of the previous policies.
- An execution of the access policies according to the established policies, the qualification of the contents and the access authorization of the user, which will filter the contents. These access policies should apply to entities responsible for websites, social networks, internet search engines, mobile phone companies, and video game manufacturers, among others.

C. Protection of the best interests of minors.

Recital 89 of the DSA emphasizes that the obligation of very large online platforms is not limited only to age verification or protection against adult-oriented content. This obligation must cover the protection of the best interests of minors in all its aspects:

"Providers of very large online platforms and of very large online search engines should take into account the best interests of minors in taking measures such as adapting the design of their service and their online interface, especially when their services are aimed at minors or predominantly used by them."

The best interests of minors should guide the design and implementation of protection systems, taking into account, among others, their right to privacy and limiting the exposure of their minor status to avoid different risks that could be more serious than access to such content. Therefore, such systems cannot be proposed with a narrow view focused only on limiting access or on age verification but must consider the complexity of the processing context and the need to protect the best interest of minors, as well as the general framework of fundamental rights. Among others, it is necessary to protect minors from the illegitimate, continuous, and massive gathering of their personal data, as well as their profile and the permanent exposure of this vulnerable group to the advertising that enriches the web sites.

Implementing a system for the protection of minors from inappropriate content requires the cooperation of multiple actors with a genuine commitment to protecting the best interests of minors in all their dimensions, and the fundamental rights of all Internet users concerning the protection of their personal data. Such actors are all those persons and institutions legally responsible for the health of minors, regulatory bodies, associations, and foundations for the protection of minors, systems suppliers and Internet services providers, among others. A practical, objective, and fair system can hardly, nor should, be implemented unilaterally. Likewise, to the extent that the system for the protection of minors poses a high risk to all citizens, Impact Assessments must be carried out, from both the Data Protection of all interested parties and the protection of the minors' health and development points of view.

D. Protection of the rights of all citizens on the internet.

The systems for protection of minors from inappropriate content, even if they are mainly intended for their protection, in practice apply to all citizens who access the Internet; therefore, these systems must be designed to respect the fundamental rights of all of them. Moreover, they must be oriented to be used by adults and not by minors since they are the ones who must prove their "authorized to access" condition.

These protection systems, as they involve the processing of personal data, must be legitimate, appropriate, necessary, and proportionate. In particular, it is required to consider the prohibitions on treating special categories of data (Articles 9 and 22 of the General Data Protection Regulation (GDPR) of 2016), such as biometric identification and authentication, as well as their exceptions.

In this sense, Article 28 of the DSA "Protection of minors online" states that age verification and the protection of the best interests of the child is not a legal basis that legitimizes the additional processing of data of a minor person:

"3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor."

Systems to protect minors from inappropriate content involve high-risk data processing, but they can also have a significant impact on society. The high risk of these systems implies that the most appropriate strategies to manage it are those that preserve the user's anonymity before Internet service providers and third parties in the context of age verification. In addition, they must be transparent and auditable, the tools to prove the authorization for access to inappropriate contents must be under the user's control, and they must be trusted enough to be widely accepted. And there is an obligation to implement all necessary privacy measures resulting from a Privacy Impact Assessment and to overcome an analysis of suitability, necessity, and proportionality.

III. Principles that a system for protection of minors from inappropriate content must comply

Systems for the protection of minors against inappropriate content must follow the following principles to guarantee the best interests of minors and fundamental rights concerning the processing of personal data of all Internet users.

When applied, these principles should not be understood independently but **addressed together**.

PRINCIPLE 1:

The system for protecting minors from inappropriate content must guarantee that the identification, tracking or location of minors over the Internet is impossible.

PRINCIPLE 2:

Age verification should be aimed at ensuring that users of the appropriate age prove their condition of person "authorized to access" and not at verifying the status of "minor".

PRINCIPLE 3:

Accreditation for access to inappropriate content must be anonymous for Internet service providers and third parties.

PRINCIPLE 4:

The obligation to prove the condition of the person "authorized to access" will be limited only to inappropriate content.

PRINCIPLE 5:

Age verification must be carried out accurately, and the age categorized as "authorized to access".

PRINCIPLE 6:

The system for protecting minors from inappropriate content must ensure that users cannot be profiled based on their browsing.

PRINCIPLE 7:

The system must guarantee the non-linking of a user's activity across different services.

PRINCIPLE 8:

The system must guarantee the exercise of parental authority by parents.

PRINCIPLE 9:

Any system for protecting minors from inappropriate content must guarantee all people's fundamental rights in their Internet access.

PRINCIPLE 10:

Any system for protecting minors from inappropriate content must have a defined governance framework.

The development of the following principles provides some examples of solutions to the issues they raise, which are not intended to exclude other possible options.

PRINCIPLE 1:

The system for protecting minors from inappropriate content must guarantee that the identification, tracking or location of minors over the Internet is impossible

A protection system must preserve the best interests of minors. This interest is much broader than merely limiting their access to inappropriate content; it must, among others, maintain their privacy, safety, physical and mental health, education and right to the free development of their personality and personal abilities[10].

Systems to protect minors from inappropriate content must prevent identifying them in Internet. Potential aggressors, pedophiles, addictive schemes, or anyone who seeks to locate or broadcast specific content for minors for malicious purposes should be unable to create deceptive services to find them. Any system based on the disclosure of the minor status should be avoided.

The obligation that different parties may have to verify the age of those who wish to access inappropriate content is not a legal basis for processing minors' data. A system based on the collection of minor data implies processing the data of a minor, which must be legitimized, suitable, necessary, and proportional.

Systems based on profiling Internet users on servers of service providers or third parties that act as intermediaries between the user and the content allow the identification of minors. Likewise, systems based on facial recognition or biometric information executed on such servers, not exclusively on the personal device, have the danger of being incorporated into malicious services to identify minors. These systems may generate additional risks when they are built using centralized databases in which extensive information is accumulated regarding the identity and browsing habits of a large part of the citizenry, especially minors.

When applying policies to limit access to content, the processing of the "authorized to access" condition must be as little spread as possible to avoid the detection of minors. That is, if one person fails to get the "authorized to access" condition, that information must be processed in a way that avoid inferring that such person is a minor. It should be avoided in the process of accreditation of access authorization, in the content filtering process, or by the analysis of their browsing patterns. Systems for the protection of minors against inappropriate content must prevent identifying minors. Therefore, potential aggressors, pedophiles, addictive schemes, or anyone who intends to locate or issue specific content for minors for malicious purposes should be unable to build misleading services to discover minors. Any system that is based on the child having to disclose his or her minor status should be avoided.

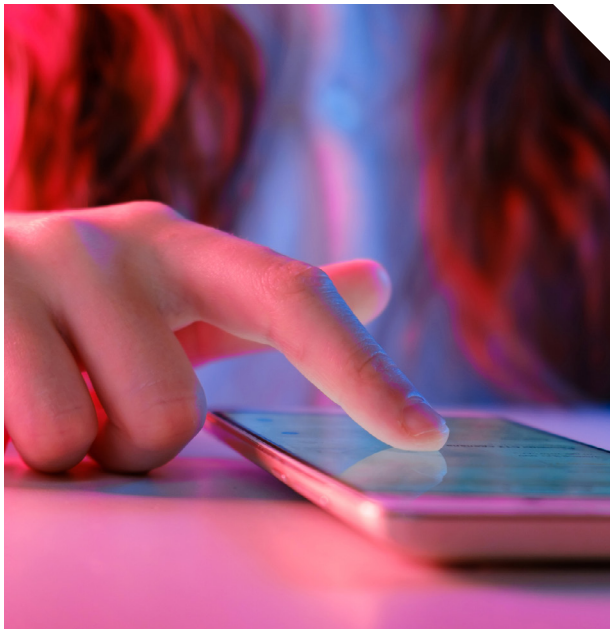
The duty that different actors may have to verify the age of those who wish to access adult content is not a legal basis for processing minors' data. A system based on the child's data collection involves the processing of data of a minor which must be legitimate, suitable, necessary, and proportional.

[10] In this sense it is set out in recital 89 and Article 28(3) of the DSA.

It is also necessary to remove, from the design, the impact that personal data breaches of third-party verification services or Internet services could have on minors.

A possible solution is to process the identity information, the "authorized to access" condition and the execution of access limitation policies on the devices held by users without relying on the servers of the service providers or third parties. In this sense, the requirements of Article 25.2 of the GDPR regarding the minimization of personal data must be considered.

An example of an additional guarantee could be that the system provides zero information or, at most, the "no authorized to access" condition, in multiple circumstances, not only when the user is a minor: when an adult has decided not to be accredited, when the protection system is not present in the device when the age verification has failed, when it is a person who does not meet the age requirements, or that the "authorized to access" condition applies to more cases (which would depend on the type of service). Another possible guarantee is that user browsing activity can be masked or obfuscated so that no access patterns allow finding minors[11].



PRINCIPLE 2:

Age verification should be aimed at ensuring that users of the appropriate age prove their condition of person “authorized to access” and not at verifying the status of “minor”

The purpose of protection systems should not be to verify the age of minors. Verifying the status of "minor" would mean that mechanisms must be built to validate minors' identity, to give tools to minors to prove age and identity, and such mechanisms and tools should be usable by minors.

These mechanisms could include biometric analysis, profiling, or obtaining credentials from minors. All of them would put the minor at risk, either by exposing them to malicious services, collecting excessive data, or identifying a person as a minor to service providers or third-party intermediary entities between the user and the content. Furthermore, they involve minors’ data processing, which would have to be legitimized and comply with other requirements of the RGPD relating, among others, to give information specifically oriented to minors, or to fulfil the limitations lay down regarding consent and carrying out service contracts by minors.

Therefore, the verification mechanisms must be aimed at being used by those people who can prove they have an "authorized to access" condition; that is, they should not be tools for minors, exposing them to additional processing activities, nor conditional on having accreditation and identity verification resources, which are currently available for adults[12].

[11] For example, if a minor intends to access adult content that is blocked in a mobile app, it generates traffic patterns that hides it from a mobile app.

[12] In cases of persons under the age of 18 who are in the ranges that allow access to specific contents, obtaining such documents is possible, and, in many cases, recourse to them may be under the responsibility of the person exercising parental authority.

PRINCIPLE 3:

Accreditation for access to inappropriate content must be anonymous for Internet service providers and third parties

The protection system must guarantee people's privacy when browsing the Internet and not expose their identity, especially that of minors. Applying this principle must be carried out without prejudice to the fact that, for other processing activities offered by the Internet service provider, such as the sale of products, the identification of the client is necessary or required by Union or State Law Members. The age verification for accessing content inappropriate for minors and the identity accreditation to third parties for other purposes are two different processing activities. The processing by Internet service providers and third parties of the certification of access to inappropriate content must be anonymous and independent of the processing for other legitimate purposes.

Adults' content can vary. It could be videos, texts, books, audio, or other products. It must be remembered that access to services and products over the Internet is not a residual option but, increasingly, the only option for many citizens to develop their personal and economic lives. Therefore, any logging or tracking of these accesses can significantly impact users' overall privacy. In particular, when digital identity systems are developed aimed explicitly at accessing adult content.

The loss of anonymity may occur when the identity is verified at the Internet service, when third-party intermediaries are involved, or when a provider of identity credentials or access credentials can link the credential's generation with effective access to a service or content. A case, for example, may occur when a third party must authorize the user, and it forwards a positive or negative value to the Internet service provider regarding the result of the authorization process. Another case may occur when a third party authorizes the user and links the person identity with a unique identifier that allows access to the services. Although third parties may be trustworthy, they are not free from the intervention of judicial authorities, intelligence services, personal data breaches, future regulatory changes, changes in their ownership, etc. Furthermore, those third parties that monetize authorization processes have the duty to implement traceability and access auditing for accounting and billing purposes.

Anonymity will be lost when signed certificates or attributes associated with unique identifiers linked to an identifiable person are used instead of certificates or attributes that cannot be linked to the user. Anonymity will be even more exposed when third parties process biometric data (through photos or videos, for example) to extract biometric templates.

The system for protecting minors from inappropriate content must prevent third entities from acting as intermediaries between the user and the Internet service provider using strategies that allow identification, browsing monitoring and/or profiling of the person. This could be achieved, for example, by providing tools so that the personal device is the one that executes all the verification mechanisms without using external resources, including the execution of content access limitation policies on the same device. Another strategy could be that the identity providers provide accreditation of the "authorized to access" condition unlinked with the user identity, that the aim to access adult content is not linked to the user, and that the process to get the accreditation does not generate meta-information linked to the person.

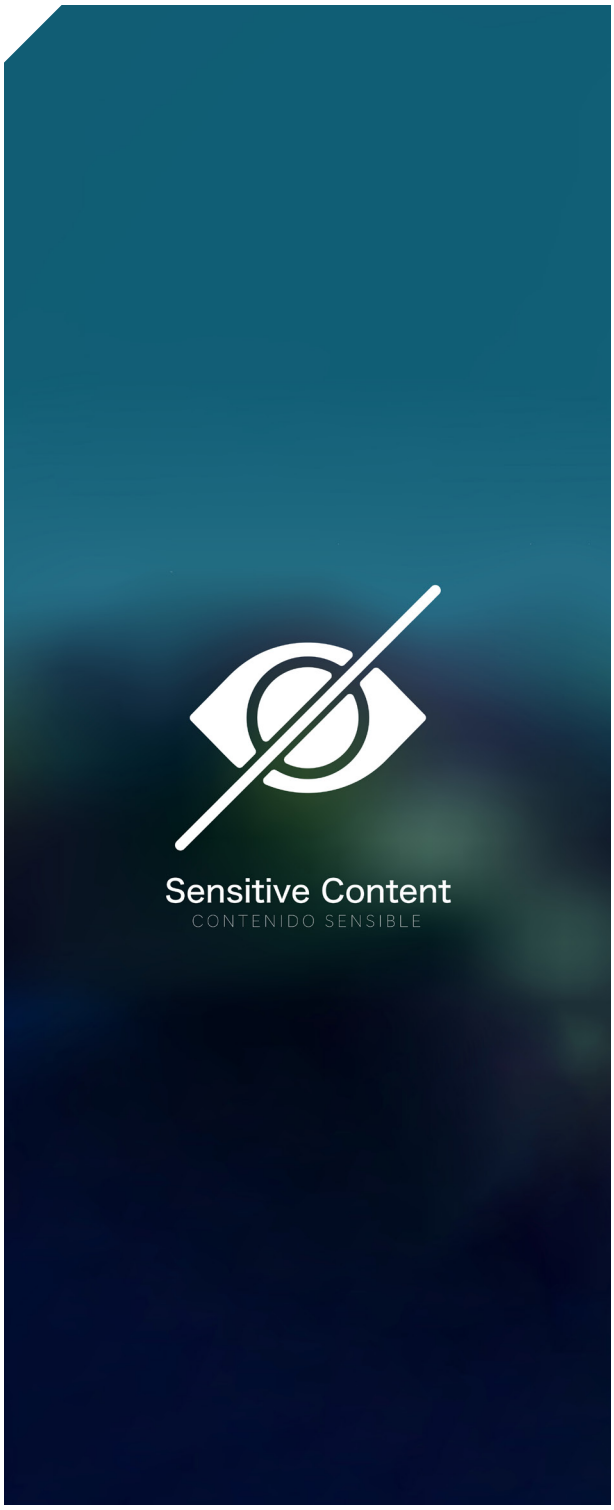
PRINCIPLE 4:

The obligation to prove the condition of the person "authorized to access" will be limited only to inappropriate content

The fact that every person must prove their "authorized to access" condition before accessing any content would not comply with the principles of data minimization, nor with the requirement of necessity, and would identify all minors who access the Internet by default. The general rule should be free and anonymous browsing without proving any age conditions. Only in the case of requesting the access to specific sites with age limitations or to content inappropriate for minors, then the "authorized to access" condition should be required (for being over 18 years of age or 14 years of age, such as, for example, in the case of access to a social network).

For example, protection systems based on profiling Internet users to determine whether they are minors involve systematic processing of personal data. This processing would link to each person who accesses the Internet an analysis of their browsing activity, relationships, conversations, reactions to content, etc. The use of profiling techniques implies the continuous supervision of all people even when they are not accessing content inappropriate for minors and involves disproportionate processing of personal data.

Therefore, a protection system must allow a person not to be forced to define themselves as an "authorized to access" person on all occasions. In a service that provides adult content and content without age restrictions, it should only be necessary to prove the "authorized to access" condition when accessing adult content. An important aspect is not to extend the protection to all possible content in Internet. Protection must not systematically affect cultural content in such a way that protection policies could be used to implement policies beyond the strict protection of minors; it should not limit freedom, diversity of thought or family education tasks.



PRINCIPLE 5:

Age verification must be carried out accurately, and the age categorized as "authorized to access"

Age verification must be carried out in a certain way, not probabilistic or estimated. It should be oriented towards categorization as "authorized to access". In no case should it imply the specific disclosure of age or date of birth.

On the one hand, verifying (as established in different regulations) is not the same as estimating. Furthermore, age estimation is inevitably subject to errors, biases and discrimination[13], and often even requires verification of more information about the person (gender, race, etc.) to be sufficiently accurate.

Verifying the "authorized to access" condition differs from providing the age value or date of birth. The generation of quantitative attributes about age poses a significant risk in the case of minors, especially in cases between 14 and 18 years old, but also in the case of older adults. All this without prejudice to the fact that it may be necessary to collect the age accurately in processing activities for other purposes, but these processing activities must be kept independent from the age verification to protect minors from inappropriate content.

It must also be considered that age verification strategies for minors by groups (for example, under 14 years of age and between 14-18 years of age) must be implemented in such a way that they cannot disclose information about the age group (or even the minor status). Then, successive accesses should not be linked to the same person attempts to access unauthorized adult content in a way that they disclose age information.

Therefore, age verification mechanisms must give a specific value, categorized only as "authorized to access", and in no case they should allow service providers or third parties to process a person's specific age or infer it.

PRINCIPLE 6:

The system for protecting minors from inappropriate content must ensure that users cannot be profiled based on their browsing

Some labeling is necessary to determine that a specific site or content is only suitable for an adult. This labeling can be done through a "pass/fail" rating, as is the case with applying age restrictions on websites. It can also be done by assigning multiple labels to each content ("violent", "explicit sex", "racist", "consumption of toxic substances", etc.[14]) to assess whether the content is inappropriate for minors. Tagging of sites or content could be done by human reviewers or automatically[15], statically or through dynamic analysis (the latter, for example, in chats).

At some point between the server, which provides the content, and the user, who requests the content, the access limitation policy must be executed. The execution of those policies on the servers themselves or third-party intermediary entities between the user and the websites entails risks to privacy. Among these risks are those derived from the profiling or monitoring of the person who accesses it, which in

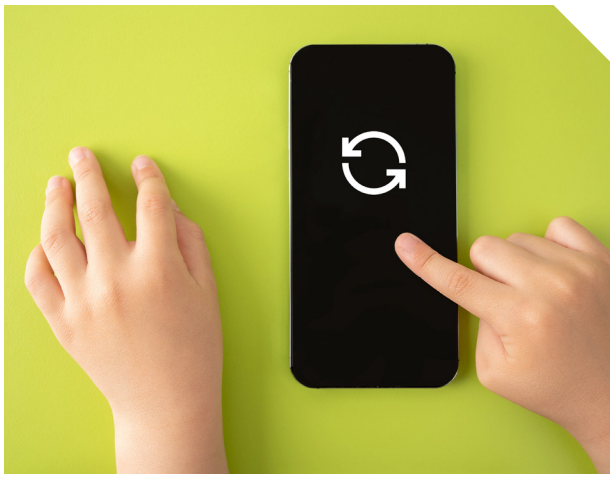
[13] Some of the estimation mechanisms do not have the same precision depending on the color of the subject's skin.

[14] In the same way that movies are rated on video servers or streaming platforms.

[15] As, for example, with artificial intelligence tools.

this type of content could include special categories of data. Adding several tags to the content accessed by a person could mean building a profile/tagging of such person based on the content they have accessed. The risk will be more significant when the same third party filters all the traffic corresponding to the same person. Profiling and monitoring, in particular with special categories of data, is a high-risk processing that would have to pass a proportionality assessment, and previously to lift the prohibition to process such data and to have a legal basis.

Executing access restrictions locally on Internet users' devices would eliminate the risks of profiling or monitoring. Local content filtering is technically viable, as demonstrated by existing malware protection systems or some tools used for parental control. Local protection by checking the "authorized to access" condition, including dynamic local tagging, would be possible on the devices themselves, either in their operating systems or by adapting the applications (apps) of Internet services (whether social networks, search engines, chats, etc.). It even allows for developing more effective strategies, such as applying regional, cultural, or family criteria in the labeling process and interpretation of labels. Dynamic labeling, including filtering, could be carried out on home or educational center routers without prejudice to using the previous strategies. The objective would always be the same: implementing protection based on age with minimization of the personal data being processed to avoid the risk of locating minors or general profiling.



PRINCIPLE 7:

The system must guarantee the non-linking of a user's activity across different services

A system that allows linking the Internet user's activity in various services can identify and profile them, inferring behavioral characteristics of the interested subject.

For age verification, systems that use unique codes between multiple platforms allow the person to be tracked between different services. The same occurs with systems based on signed attributes that include unique identifiers. It must be taken into account that the interaction of the user with the service is usually more complex than just access to content; for example, it may include comments or conversations, or in some specific services, the identification of the person will be required (for example, on online gambling sites).

When websites or services that offer content classified as inappropriate for minors extend to multiple areas of digital life, linking accesses can allow not only very intrusive profiling but even reveal more identification attributes.

This can also occur with any unique identifier reused across services, platforms, or content, such as biometric patterns[16]. Even more complex situations may arise when adult content is linked to access to certain premises, and downloading credentials for age verification collects geolocation information, for example.

Therefore, the system must avoid unique identifiers shared along different services or using mechanisms that reveal metadata that allow the user to be identified directly or by the enrichment with additional information.

[16] It has already been demonstrated that patterns generated using different biometric systems can be linked to each other.

PRINCIPLE 8:

The system must guarantee the exercise of parental authority by parents

Any system to protect minors from inappropriate content must ensure the right of those who exercise parental authority to participate in the education of minors in their care actively, maintaining respect for their cultural, political and belief diversity as well as the particular conditions of the minor. The protection from certain content could be part of the education of a minor.

Families, educational institutions, associations,and foundations for the protection of minors, academic researchers and experts, and the State have the right to actively participate in establishing the criteria for what they consider inappropriate. A commercial entity cannot lay down the content that a minor can access. The reality is that, in many cases, the economic interest of those entities and the monetization of the data of minors could take precedence, allowing and even promoting content that is inappropriate for them.

Therefore, systems must establish policies that take families into account, either directly or through their representatives, associations and foundations aimed at the protection of minors.

PRINCIPLE 9:

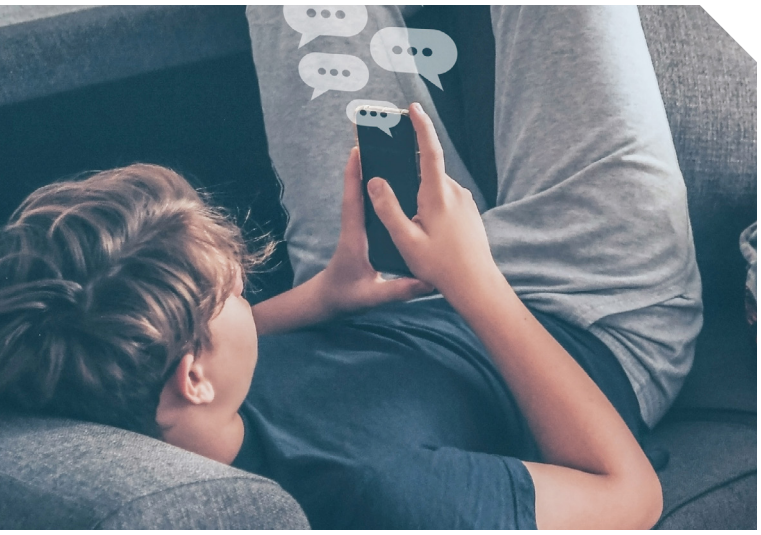
Any system for protecting minors from inappropriate content must guarantee all people's fundamental rights in their Internet access

The importance of digital life, enhanced daily by all institutions, implies that any limitation or control over digital development, if not applied correctly, could represent a limitation of fundamental rights for adults and minors.

Thus, an interference with the fundamental right to personal privacy would occur whenever the systems for the protection of minors from inappropriate content allow content to be linked to an identifiable person, allow their intimate aspects to be profiled, or connect them with other information coming from the metadata that is generated in the entities involved in the protection system. Even the mere declaration that a person has wanted to access content inappropriate for minors can constitute an intrusion into their privacy.

Regarding the right to personal freedom, information, thought, conscience, and religion, which are all rights of minors too, a protection system cannot restrict access to certain content due to excessive zeal or by applying specific values, interests, or beliefs. It must be considered that content inappropriate for minors could include books, opinions, or educational material. When systems are so intrusive to privacy that they generate self-censorship, there may be cases of limitation of freedom of information. Self-censorship will also appear when the desire to access inappropriate content has to be accredited to third parties. Also, in the case in which probabilistic or biased systems are being used that prevent certain people, for example, those of age in the limit or belonging to minorities, from accessing content to which they have the right to access.

In the same sense, and as previously mentioned, the concept of inappropriate content for minors should not have an expansive nature that regulates all aspects of digital content, such as cultural content, nor should it be established by commercial services or States based on ideology.



Regarding the right to personal integrity, it is evident that the possibility of systems allowing minors to be located through the Internet can pose a physical risk to their integrity. However, it can also make it possible to identify adults in a situation of vulnerability, mainly psychological, who are profiled for their habits concerning certain content.

Regarding the right to one's image, the rights of citizens would be restricted in those protection systems that store or process their personal image through facial recognition systems by the Internet service provider or third entities when it is not technically necessary to carry out this kind of processing activity, and when it could be carried out, in any case, on the devices under the users' control.

The right to the capacity to act, such as the ability to validly carry out legal acts, exercise rights, and assume obligations, is closely linked to the person's identity and the possibility of identification. Much of the ability to act must be developed in the digital environment. Therefore, this right could be violated in systems that limit the ability to act based on service conditions and without a legal basis.

Regarding the right to non-discrimination, among other examples, these systems should not hinder older adults or any other group from accessing content simply due to the choice of specific technological options that do not accept diversity. Nor should verification systems or access to additional identity information allow or implement biases based on gender, race, age, nationality, etc.

PRINCIPLE 10:

Any system for protecting minors from inappropriate content must have a defined governance framework

Any system for the protection of minors from inappropriate content must have a defined governance framework to guarantee compliance with these principles, protect fundamental rights and articulate the participation of those who hold parental authority, educational institutions, associations, and foundations for the protection of minors, researchers and privacy experts, the State or technological and service providers of the digital society, among others.

The governance framework must implement and deploy the protection system with technologies that preserve privacy. It also must meet a minimum level of effectiveness, assuming that no technological system is perfect. This effectiveness must be evaluated objectively and critically, including analyzing the collateral effects on users and society. In its use and way of operating, the system must be transparent for these users, particularly concerning the browsing anonymity and content limitation criteria, in addition to being effectively auditable by independent authorities and third parties.

A system that does not have minimal effectiveness will not meet the requirement for adequacy. A clear example is those systems based on the age self-declaration made by the users themselves, which have only served to provide purely formal legal guarantees to Internet service providers. Another example is some of the current parental control systems, which in many cases have not been adequately validated for their robustness against manipulation. Also, those systems that generate distrust and are rejected by citizens are not effective.

The collateral effects of applying protection systems for minors must be assessed critically. Specifically, it is necessary to consider what could be the impact of personal data breaches in the entities involved. This will be particularly serious when third-party services, whether identity or age verification, accreditation of the "authorized to access" condition, or content filtering, suffer security breaches, corruption or blackmail for credential theft or intervention by States.

Other collateral effects can occur when protection systems discriminate against people who, for whatever reason, cannot use those systems, or the systems do not interact correctly with them due to the incorporation of some bias. In particular, concerning people with functional diversity or older adults.

The protection system requires offering different options, overlapped or not, that respond to different platforms and social situations. It must also consider its integration with present and future national and European identity management systems, as in the Digital Wallet established in the eIDAS2 proposal[18].

A key aspect of effectiveness is the trust of users, who cannot be required to have blind faith in technological services and stakeholders. Therefore, the systems must be configured to be audited by both, supervisory authorities, and independent research centers, with complete competence to carry out this task. The auditability of these systems and the platforms on which they are executed must make it possible to obtain evidence that there is no manipulation, lack of diligence, that profiling or monitoring of users' activity is not possible or being carried out, that there is no discrimination, that they are not vulnerable systems and that they comply with all the principles, rights and obligations laid down in the GDPR, in particular, that of accountability. Concentration on a few third-party services that are not accessible to independent oversight for audit increases the impacts of gaps, collateral effects, and the difficulty of effective oversight.

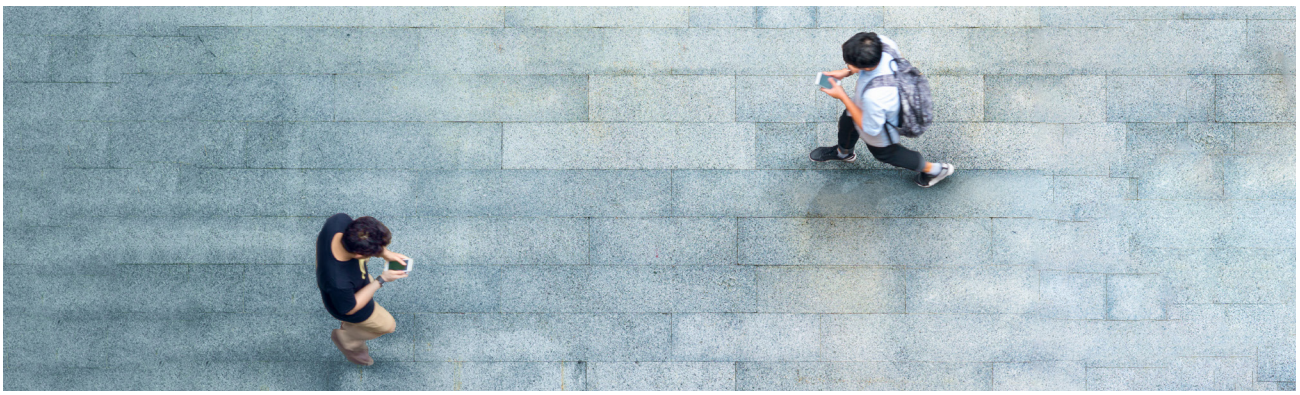
IV. CONCLUSIONS

The protection of minors is the responsibility of society as a whole. All its participants must form the network of care, defense, help and support of the minor on the path to their development as an adult. The protection of minors is complex and extends to many more aspects than content filtering on the Internet. Seeking simplifications based on "technological solutionism" that ignore fundamental social dysfunctions could aggravate the problems they cause.

Technology can be a great support in the defense of minors if it is integrated into a general protection framework with the involvement of all social stakeholders: families, authorities, educational institutions, associations and foundations for the protection of minors, privacy researchers and experts, technology providers and digital society services, etc.

Perfect technology does not exist. However, there is suitable technology that acts harmoniously with the educational, cultural, social, responsibility and security elements to protect best interests of minors and citizens' fundamental rights effectively.

The education of minors, particularly in the digital environment, and the selection of appropriate content is a shared responsibility between families, governments that must promote effective public policies and protection regulations in this area, and the industry. It is urgent to adopt measures to protect children and youth in the digital environment, in line with the actions proposed in the already mentioned State Pact.



[17] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards the establishment of a Framework for a European Digital Identity.

www.aepd.es
AEPD_es
AEPD
@aepd.es