

# AGE VERIFICATION SYSTEMS



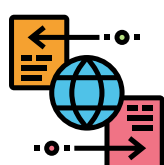
Self-declaration  
of age to the content  
provider



Sharing credentials  
or attributes with the  
content provider



Age estimation  
made by the content  
provider



Third parties as  
intermediaries between  
the user and the content  
provider



## THREATS

### LACK OF ADEQUACY

There is no certainty about the verified age.



### IDENTIFICATION

The provider could infer the real identity of the user.



### NON-REPUDIATION/LINKING OF ACTIVITIES ACROSS DIFFERENT SERVICES

The user cannot deny their activity in one or more services.



### DETECTION

A third party (provider or not) can locate minors.



### DISCLOSURE, APPROPRIATION OR TRANSFER

Unnecessary data is collected, additional treatments or transfers are carried out.



### LOSS OF CONTROL

Lack of transparency concerning the user or lack of control of those who exercise parental authority to make informed decisions.



These aspects may pose the following

## RISKS FOR RIGHTS AND FREEDOMS



### LACK OF ADEQUACY:

Risks for the minor's best interest (minors accessing inappropriate content: impacts on mental health, emotional development, etc.) or risks for the right to freedom of communication, information, and expression in adults (limitation of access to adult content)

### IDENTIFICATION, NON-REPUDIATION, LINKING OF ACTIVITIES ACROSS DIFFERENT SERVICES:

Risks for the right to honour and privacy (impacts on prestige or reputation); for freedom of communication, information, and expression (self-censorship); for freedom of opinion and participation (manipulation and propaganda), for security and right to work (stigmatization, discrimination)

### DETECTION

Risks for minor's best interest (right to security)

### DISCLOSURE, APPROPRIATION OR TRANSFER, LOSS OF CONTROL

Risks for the rights related to the GDPR (access, rectification, etc.), risks for the freedom to make informed decisions of those who exercise parental authority

# DECALOGUE OF PRINCIPLES

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

**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".

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

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

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



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

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

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

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

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

