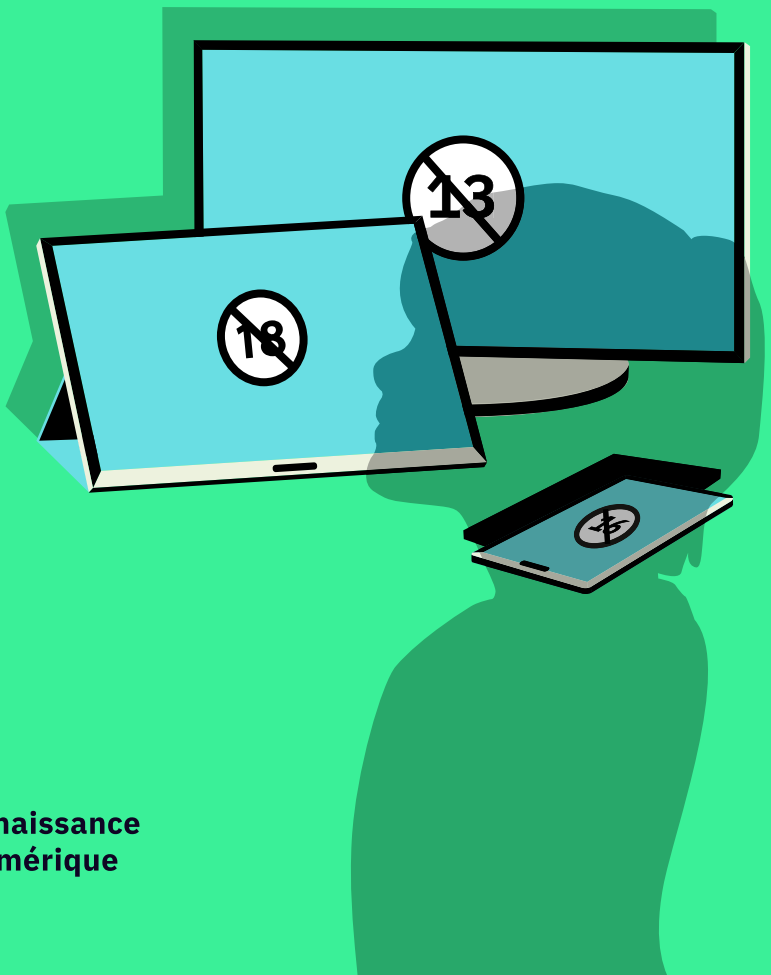
September 2022

# Age assurance online: working towards a proportionate and European approach




Renaissance Numérique

# Table of contents

# About Renaissance Numérique

Renaissance Numérique is an independent think tank dedicated to the digital transformation of society. Its purpose is to shine a light upon the changes brought about by this transformation, and to provide everyone with the tools to master it. To accomplish its mission, Renaissance Numérique offers itself as a place for debate, for the positive confrontation of ideas and expertise. It brings together academics, leading experts, NGOs, and companies, all reflecting the grand variety of actors and points of view in the digital sector. Its reflexions – widely shared and disseminated through written contributions, publications, or events – are brought to the attention of both public and private actors at the French, European and international levels. Renaissance Numérique is a member of the Observatory for online hate led by Arcom – the French Regulatory Authority for Audiovisual and Digital Communication – and of the organising committee of the French chapter of the Internet Governance Forum (IGF).

# Executive Summary

In line with its work on online hate and cyberbullying[1], Renaissance Numérique has launched a working group dedicated to the issue of guaranteeing children's rights online in spring 2021. Beyond the issue of protecting children online, which has dominated the public debate in recent years, this working group aims to examine children's rights in the digital age more broadly. In light of their increasing usage of the Internet at an increasingly early age, should we consider revising their rights, in particular those granted by the International Convention on the Rights of the Child? In contrast, should some of the rights specifically conferred to them online have an equivalent in "offline" life? Are these rights effectively guaranteed? Are public policies designed to guarantee them effective?

In order to shed light on these questions, our working group conducted an initial review of an issue that is widely discussed in French, European, and international public debates: the question of age assurance online. Age assurance is an interesting practical case study, allowing us to examine the way in which political leaders and the various stakeholders concerned deal with the issue of children's presence online. Why are the legal provisions that require the establishment of Internet users' age assurance in order to strengthen child protection online not better enforced? Are they insufficient? What avenues should be pursued in order to strengthen their enforcement? These are the questions addressed in this report.

To complement the expertise of the members of the working group (which includes lawyers, researchers, child protection association representatives and online platform

1 Renaissance Numérique (2017): "Taking action against hate on the internet in a collaborative society", 42 pp: https://www.renaissancenumerique.org/wp-content/uploads/2021/09/renaissancenumerique_note_onlinehate.pdf; and Renaissance Numérique (2019), "Cyberbullying: a review of the literature", 39 pp.: https://www.renaissancenumerique.org/wp-content/uploads/2020/04/renaissancenumerique_cyberbullying.pdf

representatives), more than twenty French, European, and international stakeholders were interviewed. An analysis of the legal provisions applicable to children in the digital space was also carried out. This report, which is an initial contribution to the debate, presents the working group's conclusions. It outlines ways of improving the effectiveness of legal provisions requiring Internet users' age assurance.

Although there is an extensive legal framework establishing the need for age assurance in order to access various online services, the analysis we conducted shows that the implementation of this framework remains largely unsatisfactory. In this report, Renaissance Numérique identifies three major obstacles to the effectiveness of existing measures: the delicate balance between the protection of children online and other rights, such as the right to privacy; certain stakeholders' economic objectives; and the relative lack of homogeneity of the legal framework in the European Union Member States, which makes compliance difficult. In addition, some of the technical solutions used for age assurance are particularly intrusive and may lead to an imbalance in the guarantee of fundamental rights and freedoms.

In order to overcome these obstacles, Renaissance Numérique recommends implementing a common framework of requirements at a European level and outlines its architecture and scope. The concept of proportionality and the accountability of online services providers are at the heart of this approach.

# Recommendations

| | |
|---|---|
| 1 | **IMPLEMENT A COMMON CODE OF CONDUCT AT EUROPEAN LEVEL**<br><br>The minimum conditions that ensure age assurance is done effectively and in a way that is compatible with our fundamental rights must be specified and harmonised at European level. We encourage the European Commission, the Member States and all relevant stakeholders to explore the possibility of a binding code of conduct. |
| 2 | **CONDUCT IMPACT ASSESSMENTS RATHER THAN RISK ASSESSMENTS**<br><br>Providers of online services that may be accessed by minors cannot limit themselves to carrying out risk assessments. Impact assessments have the advantage of encompassing both the opportunities and risks minors may encounter online, as well as other key variables such as the impact of possible measures on other users, how easy it is to circumvent the measures being considered, the costs for the actors that have to implement them, etc. This evolution must also be integrated by the authorities responsible for supervising these services. There is therefore an urgent need to strengthen the human and financial resources available to them. |

3

## IMPOSE "STRICT" AGE ASSURANCE WHERE LEGAL PROVISIONS TO RESTRICT OR PROHIBIT ACCESS DO EXIST

We recommend imposing a strict age assurance (i.e. verification) when legal provisions to restrict or prohibit access do exist. For operators providing such products or services (pornographic content, online betting, sale of alcohol, etc.), the need for age assurance is all the more critical as it aims to determine whether an individual has the right to access the product or service in question or not. However, such a measure requires age verification techniques that are effective, not too intrusive, accessible to all and respectful of the balance between fundamental rights and freedoms. The work underway at French and European level to develop solutions that meet these requirements must therefore be supported.

INTRODUCTION

# Age assurance: an obligation that is not generally complied with

On 5 July 2022, the European Parliament adopted in plenary session the Digital Services Act (DSA) proposed by the European Commission in late 2020. This text, which aims to ensure a safe and responsible online environment, has three objectives: *"give better protection to users and to fundamental rights online, establish a powerful transparency and accountability framework for online platforms and provide a single, uniform framework across the EU"*[2].

In addition to measures relating to online marketplaces, the analysis of systemic risks likely to be induced by very large platforms and search engines, or misleading interfaces (dark patterns), the DSA includes provisions designed to strengthen the protection of children online. In particular, platforms that are accessible to children are obliged to implement specific protective measures to ensure their safety. Furthermore, the text prohibits these players from showing children targeted advertising based on the use of their personal data as defined in European Union law[3] [4]. Although this concern about children's digital habits is not new, it has recently been reinforced following the successive lockdowns imposed in many countries in the context of the health crisis and the resulting increase in online usage[5].

2 European Commission, "The Digital Services Act: ensuring a safe and accountable online environment": https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

3 European Parliament, "Digital Services Act: agreement for a transparent and safe online environment", Press release, 23 April 2022: https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

4 This proposal was also the subject of debate during the discussions between the European institutions on the Digital Markets Act (DMA). While the European Parliament was in favour of introducing this provision in the DMA, it was not included in the final agreement reached on 24 March 2022.

5 In particular, because of the intensification of certain harmful behaviours such as cyber-bullying (development of "fisha accounts", revenge porn, "digital raids") and addictive practices.

*"Unfortunately, there are still many taboos and conservative ideas in our societies, and talking about sexual and reproductive health is not easy for many teenagers. So they turn to the Internet to find answers to their questions"*

NAJAT MAALLA M'JID
Special Representative to the United Nations Secretary-General on Violence against Children

Searching for information, educational uses, surfing on social networks, playing online video games... children's practices in the digital space are manifold and provide many opportunities for their development and the exercise of their rights. More than any other generation, the new generations live and grow up with and in the digital world, creating new socialities and opportunities for interaction.

*"The media's view of children's digital practices generally focuses on the most dangerous aspects. We often analyse the worst of these practices without also exploring the positive aspects. There is therefore a real need for young people and adults (including teachers) to take ownership of these practices, which have multiplied, while developing effective protection methods"*

ALEXANDRA MIELLE
Head of the "Audience Protection" department, French Regulatory Authority for Audiovisual and Digital Communication (Arcom)

Whilst regulations and political speeches focus on the monitoring (or even surveillance) and prohibition of some of these practices[6], Renaissance Numérique calls, in this new series of works, for the problem to be considered in its entirety. To this end, the think tank launched a dedicated working

6 For example, Bill n°2854 of 28 April 2020 aimed at curbing children's exposure to screens at school, whose purpose is to *"annihilate all screen exposure in schools"*: https://www.assemblee-nationale.fr/dyn/15/textes/l15b2854_proposition-loi

group in spring 2021[7]. This group brings together a dozen expert members of the think tank: lawyers, researchers, child protection association representatives, and online platforms representatives. While the considerations presented here are the result of internal discussions and work by this group, they have also been shaped by twenty-three interviews conducted with key stakeholders at a national, European, and international level[8]. They are only the first step in this working group's process, which aims to examine children's rights in the digital era, with the central question being the effective guarantee of these rights.

This first publication tackles the issue of age assurance, which, in addition to its urgent nature and its omnipresence in the public debate, constitutes an interesting example of how public action and the various stakeholders involved deal with the presence of children online. It also raises issues related to guaranteeing children's rights in the digital space, such as the necessary balance between their different rights, like the right to be protected from violence, abuse, and any form of exploitation, and the freedom of information, expression, and participation. It also raises the question of the balance between children's rights, and those of Internet users in general.

There are 10 children's rights, guaranteed by the International Convention on the Rights of the Child (CRC)[9]:

- the right to have a name, a nationality, an identity;
- the right to be cared for, protected from diseases, to have an adequate and balanced diet;
- the right to go to school;

7 This thinking is also in line with previous work carried out by the think tank on related subjects, notably the fight against online hate and cyberbullying. See: Renaissance Numérique (2017): "Taking action against hate on the internet in a collaborative society", 42 pp.: https://www.renaissancenumerique.org/wp-content/uploads/2021/09/renaissancenumerique_note_onlinehate.pdf; and Renaissance Numérique (2019), "Cyberbullying: a review of the literature", 39 pp.: https://www.renaissancenumerique.org/wp-content/uploads/2020/04/renaissancenumerique_cyberbullying.pdf

8 For a full list of the members of the working group and stakeholders interviewed as part of this study, see this report's "Acknowledgements" section.

9 United Nations, Convention on the Rights of the Child, 1990: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

- the right to be protected from violence, maltreatment, and all forms of abuse and exploitation;
- the right to be protected from all forms of discrimination;
- the right not to engage in or be subjected to war;
- the right to have a refuge, to be rescued, and to have decent living conditions;
- the right to play and take part in leisure activities;
- the right to freedom of information, expression and participation;
- the right to have a family, to be cared for and loved[10].

The CRC came into force in France on 6 September 1990. In March 2021, it was complemented by the UN General Comment on the Rights of the Child in relation to the Digital Environment[11], which aims to ensure the compatibility of the digital environment with children's rights. In particular, the Comment encourages States to *"mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment"*[12]. As an official interpretation of the Convention, this Comment helps to provide States Parties with the necessary guidance for the implementation of the Convention to ensure that children's rights are guaranteed online.

European provisions such as the revised Audiovisual Media Services (AVMS) Directive, the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the proposed Artificial Intelligence Act (AI Act), and the Commission's recently proposed Regulation laying down rules to prevent and combat child sexual abuse online complement this framework.

10 The Convention on the Rights of the Child was adopted by the UN General Assembly on 20 November 1989 and ratified by France on 7 August 1990. Unicef, "The International Convention on the Rights of the Child (CRC)": https://www.unicef.org/child-rights-convention

11 United Nations, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021: https://digitallibrary.un.org/record/3906061

12 *Ibid.*

In its strategy on children's rights published on 24 March 2021, the European Commission also calls on tech companies to *"ensure that children's rights, including privacy, personal data protection, and access to age-appropriate content are included in digital products and services by design and by default"* and to *"strengthen measures to help tackle harmful content and inappropriate commercial communication, such as through easy-to-use reporting and blocking channels or effective age-verification tools"*[13]. The UK's Age Appropriate Design Code (or Children's Code), a code of practice on data protection for online services likely to be accessed by children[14], is inspiring many governments and legislators around the world[15].

In France, recent developments in this area include the law of 30 July 2020 aimed at protecting victims of domestic violence[16], the law of 19 October 2020 aimed at regulating the commercial exploitation of children under the age of 16 on online platforms (known as the "Studer I law" or the "child influencers" law)[17], and the laws of 2 March 2022 aimed at reinforcing parental control over means of access to the Internet ("Studer II law")[18] and aimed at combating school bullying[19] [20].

13 European Commission, "EU Strategy on the Rights of the Child", 24 March 2021, p. 20: https://ec.europa.eu/info/sites/default/files/ds0821040enn_002.pdf

14 For more information on the Age appropriate design code, see the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

15 For example, in the United States, several bills are under consideration in the Senate and House of Representatives, including the Children and Teens' Online Privacy Protection Act and the Kids PRIVCY Act. See: https://www.congress.gov/bill/117th-congress/senate-bill/1628 and https://castor.house.gov/news/documentsingle.aspx?DocumentID=403677.

16 Law of 30 July 2020 aimed at protecting victims of domestic violence: https://www.vie-publique.fr/loi/273137-loi-du-30-juillet-2020-proteger-les-victimes-de-violences-conjugales

17 Law of 19 October 2020 aimed at regulating the commercial exploitation of images of children under the age of sixteen on online platforms: https://www.vie-publique.fr/loi/273385-loi-19-octobre-2020-travail-enfants-youtubeurs-influenceurs-sur-internet

18 Law of 2 March 2022 aimed at strengthening parental control over means of access to the Internet: https://www.vie-publique.fr/loi/283359-loi-studer-2-mars-2022-controle-parental-sur-internet-par-defaut

19 Law of 2 March 2022 aimed at combating school bullying: https://www.vie-publique.fr/loi/282708-loi-balanant-2-mars-2022-combattre-le-harcelement-scolaire

20 We should also note the call to "Stand up for children's rights in the digital environment" launched by the French President and UNICEF at the Paris Peace Forum in November 2021. See: https://www.elysee.fr/en/emmanuel-macron/2021/11/11/standing-up-for-childrens-rights-in-the-digital-environment

Among the concerns that have emerged in the public debate regarding these issues[21], the question of age assurance is now at the forefront, particularly in France. Granting children greater protection than other Internet users, as the above-mentioned legislation intends to do, assumes that it is possible to determine whether or not a user is a child. In France, the question arises, for example, when it comes to preventing any Internet user under the age of 18 from accessing websites hosting pornographic content or to obtaining parental consent for the processing of data of children under the age of 15[22]. For the time being, these legal obligations are not generally complied with. Although the law has forced them to do so since 2020, the vast majority of pornographic websites do not carry out age assurance on their visitors. According to an Ifop (*Institut français d'opinion publique*, an international polling and market research firm) study published in April 2022, 51% of French teenagers aged 15 to 17 have already been exposed to online pornography, on average over the last 25 days, 41% of whom have visited specialised sites[23]. With regard to obtaining the consent of a legal representative for the processing of personal data of minors under 15 years of age, the application of the law also raises questions. According to a survey carried out in February 2020 by Ifop for the French data protection authority (the CNIL), 39% of children aged 10 to 14 who have an account on a social network (which generally involves the processing of their personal data), have opened it alone or with the help of another child[24].

21 We can cite, for example, the issues of misinformation, screen time, image rights and the right to be forgotten...

22 A procedure stipulated by Article 45 of the French Data Protection Act (*Loi informatique et libertés*), which complements Article 8(1) of the GDPR.

23 Ifop, "Étude sur les effets et conséquences de la loi du 30 juillet 2020 sur le visionnage de contenus pornographiques par les adolescents français", 24 April 2022: https://www.ifop.com/publication/etude-sur-les-effets-et-consequences-de-la-loi-du-30-juillet-2020-sur-le-visionnage-de-contenus-pornographiques-par-les-adolescents-francais/

24 "Les comportements digitaux des enfants — Regards croisés parents et enfants", Ifop survey for CNIL (French data protection authority), February 2020, p. 23: https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf

It is therefore urgent to collectively think about possible improvements and identify the sources of these shortcomings. Why are the legal provisions that require age assurance of Internet users not better applied? Are they insufficient? What avenues should be explored to strengthen their compliance? How can we implement age assurance that respects the balance between the various fundamental rights and freedoms?

PART I

# A protective legal framework, which establishes age assurance...

While children's digital practices offer them immense opportunities to exercise their rights (right to education, information, freedom of expression, etc.), it can also expose them to risks: cyberbullying, online hate, grooming, exposure to illegal or harmful content, incitement to dangerous behaviour, addiction, exploitation of their personal data... For this reason, specific provisions for the digital environment, which introduce the need to check the age of Internet users, have been designed both at a European and national level.

The General Data Protection Regulation (GDPR) states that children deserve specific protection with regard to the processing of their personal data, as *"they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data"*.[25] More specifically, Article 8(1) states that *"the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child"*. This article also allows EU Member States to set a lower age for these purposes by law, provided that the age is not lower than 13. In France, Article 45 of the Data Protection Act (*Loi informatique et libertés*) sets this age at 15. Moreover, it introduces the principle of dual consent: when the child is under fifteen years of age, the processing is only lawful if consent is given jointly by the child concerned and the person or persons who have parental authority over the child. The GDPR further specifies that *"The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology"* (Article 8(2)).

25 Recital 38, Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

In addition, the revised Audiovisual Media Services Directive (the so-called AVMS Directive) introduces an obligation for Member States to take *"appropriate measures to ensure that audiovisual media services [...] which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them"* (Article 6a).

Other texts relating to the digital environment which will soon come into force or are being discussed at a European level, such as the Digital Services Act (DSA) and the proposed legislation on artificial intelligence (AI Act), include specific provisions for children, in particular concerning the prohibition of using their personal data for commercial purposes. On 11 May 2022, the European Commission also presented its proposal for a Regulation laying down rules to prevent and combat child sexual abuse online, which aims to require online platforms to track Child Sexual Abuse Material (CSAM) among the content they host[26] [27].

In France, Article 227-24 of the Penal Code, Article 45 of the Data Protection Act (*Loi informatique et libertés*), Article 23 of the law aimed at protecting victims of domestic violence, the law on "child influencers", the law aimed at reinforcing parental control over means of access to the Internet, and the law aimed at combating school harassment, complete the international and European legal arsenal.

26 However, in its opinion of 15 February 2022, the review committee that examined the first impact assessment that accompanied this text warned the Commission of the risks of generalised surveillance and of undermining the encryption of communications. Despite the introduction of additional safeguards, the text presented by the European Commission introduces measures that would have an impact on the balance between our various fundamental rights. As revealed by *Contexte*, the coordinators of the European Parliament's Civil Liberties Committee have asked the Directorate-General for Parliamentary Research Services for a new impact assessment of the regulation. "Le Parlement européen veut sa propre étude d'impact sur les abus sexuels sur mineur", *Contexte*, 23 June 2022: https://www.contexte.com/actualite/numerique/le-parlement-europeen-veut-sa-propre-etude-dimpact-sur-les-abus-sexuels-sur-mineur_152729.html

27 See the "Balancing child protection and the right to privacy" section of this report.

## THE FRENCH LEGISLATIVE PROVISIONS AIMED AT PREVENTING CHILDREN FROM ACCESSING PORNOGRAPHIC CONTENT

**Penal Code, Article 227-24:**

"The production, transport, or dissemination by whatever means and whatever the medium of a message of a violent nature, inciting terrorism, that is pornographic, including pornographic images involving one or more animals, or of a nature that seriously undermines human dignity or incites children to engage in games that physically endanger them, or trading of such a message, is punishable by three years' imprisonment and a 75,000 euros fine when this message is likely to be seen or noticed by a child [...].

The offences specified in this article shall be constituted even if the child's access to the messages mentioned in the first paragraph is the result of a simple declaration by the child that he or she is at least eighteen years old."

**Law of 30 July 2020 aimed at protecting victims of domestic violence, article 23:**

"When the President of the High Council for Audiovisual Media[28] finds that a person, whose job is to offer an online public communication service, allows children to have access to pornographic content in violation of Article 227-24 of the Penal Code, he or she shall send this person, by any means capable of establishing the date of receipt, a formal notice ordering them to take any measure likely to prevent children from having access to the incriminated content. The person to whom the injunction is addressed shall have a period of fifteen days in which to submit its observations.

On expiry of this period, if the injunction provided for in the first paragraph of this article has not been complied with and if the content is still accessible to children, the President of the High Council for Audiovisual Media may refer the matter to the President of the Judicial Tribunal of Paris for the purpose of ordering, in accordance with the accelerated procedure on the merits, that the persons referred to in Article 6(1) of Law No 2004-575 of 21 June 2004 on confidence in the digital economy terminate access to the service. The public prosecutor shall be notified of the decision of the president of the tribunal.

The President of the High Council for Audiovisual Media may, on request, refer the

28 *Conseil supérieur de l'audiovisuel*, or CSA, which has since then become Arcom.

matter to the President of the Judicial Tribunal of Paris for the same purpose when the online public communication service is made accessible from another address.

The President of the High Council for Audiovisual Media may also ask the President of the Judicial Tribunal of Paris to order, in accordance with the accelerated procedure on the merits, any measure intended to stop the listing of the online communication service by a search engine or a directory.

The President of the High Council for Audiovisual Media may take action of his own accord or on referral from the public prosecutor or any natural or legal person with an interest in taking action.

The conditions for the application of this Article shall be specified by decree[29]."

29 This decree was published on 7 October 2021. "Décret n°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": https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044173388?s=03

PART II

# ...but whose implementation is unsatisfactory

In terms of the national, European, and international legal framework for the protection of children in the digital environment, cyberspace is not a "no-go area" for this audience. If this legal framework, and in particular age assurance, is struggling to come to fruition, it is primarily due to a lack of enforcement. Therefore, supplementing this framework with additional provisions does not seem necessary at present.

## LACK OF ENFORCEMENT OF THE LEGAL FRAMEWORK ON AGE ASSURANCE

As already mentioned, Article 45 of the French Data Protection Act (*Loi informatique et libertés*), which complements Article 8(1) of the GDPR, prohibits the processing of data belonging to children under 15 years of age in France, unless their consent and that of their parents have been obtained.

In order to check whether the social networks and video-sharing platforms that are most popular with young people take this obligation into account, we tried to create accounts on these services by indicating, when registering, a date of birth corresponding to a 14-year-old (which would normally prompt the services in question to verify the consent of parental authority holders)[30]. Of the five services tested[31], only one explicitly requires some form of parental consent, and two require a code to be sent to a mobile phone. For the others, the need for parental consent is not mentioned at any point in the registration process. In the United Kingdom, researchers from the children's digital rights group 5Rights conducted a similar experiment. Using Android and iPhone mobile phones registered to children aged 8, 13 and 15, they were able to download 16 dating apps from the App Store that are not allowed to be used

30 Test performed on 31 March 2022.

31 Instagram, Snapchat, TikTok, Twitch and YouTube.

by under-18s[32]. More recently, the French Digital Regulation Expertise Centre (PEReN) found that *"to date, virtually no online service uses a satisfactory process to verify the age of its users. Despite their multiplicity, few methods are at the same time easy to implement, not very restrictive and respectful of users' privacy, efficient and robust against fraud attempts."*[33]

One topic that has been at the heart of the public debate on age assurance over the last 12 months in France is the issue of age verification for access to pornographic content. Given the current situation, one might think that the pornography sector is poorly regulated, particularly in comparison to other sectors such as gambling or online betting. However, as mentioned earlier (see box p. 20-21), Article 227-24 of the Penal Code and Article 23 of the law aimed at protecting victims of domestic violence strictly regulate access to such content. However, the implementation of these provisions is not effective: most of the websites concerned continue to simply ask their visitors, on a declarative basis, to confirm that they are over 18 years old[34]. The fact that most of the players in this industry are non-European makes the effectiveness of this framework even more complex[35]. Faced with this situation, Arcom has issued a formal notice or requested that Internet Service Providers

32 "Dozens of leading apps accused of putting children in danger", *Financial Times*, 8 October 2021: https://www.ft.com/content/bed30c91-03b2-4508-b708-8073b5ec8462

33 PEReN, "Online underage users detection: can we reconcile efficiency, convenience and anonymity?", *Éclairage sur...*, n°4, May 2022: https://www.peren.gouv.fr//rapports/2022-06-23%20-%20Eclairage-sur-detection-mineurs_EN.pdf

34 This lack of enforcement also applies to other types of websites, such as those offering online alcohol purchases.

35 During a round table organised by the French senatorial delegation for women's rights on 8 June 2022 regarding the regulation of access to online pornographic content, Guillaume Blanchot, Arcom's Managing Director, recalled that the checks carried out by the authority on these websites were subject to procedural constraints within the European Union, in particular the "principle of origin" set out in the e-Commerce Directive. Under this principle, Arcom must, prior to any formal notice to a website, inform the Member State where it is established of the breaches observed, ask them whether they intend to take action against these websites and, in parallel, inform the European Commission. To see a replay of the round table: https://www.senat.fr/commission/femmes/missions/pornographie.html

(ISPs) block seven websites[36] [37]. This procedure, which Arcom is using for the first time, has revealed the extent of the challenge that monitoring the implementation of existing legal provisions represents for the authority. Indeed, although the targeted websites are the most significant in terms of number of visitors, nearly 2,000 others are thought to be concerned[38].

While a variety of technological age assurance tools exist (see box below), ranging from age verification (devices that seek to determine the exact age of the person, often resulting in identification) to age estimation (those that seek to estimate the age or age range of a person, based on artificial intelligence or keyword analysis), to declaration or self-declaration[39], with different degrees of accuracy and robustness depending on the objective, the current situation remains unsatisfactory, for several reasons.

## SELF-DECLARATION, DECLARATION, VERIFICATION, ESTIMATION: THE DIFFERENT TECHNIQUES FOR CARRYING OUT AGE ASSURANCE[40]

When it comes to age assurance on the Internet, a distinction must be made between different techniques (themselves based on different technologies), which are more or

36 The hearing before the Paris judicial court, initially scheduled for 24 May 2022, is now set for 6 September 2022.

37 "Deux nouveaux sites porno dans le collimateur de l'Arcom", *Contexte*, 9 March 2022: https://www.contexte.com/actualite/numerique/deux-nouveaux-sites-porno-dans-le-collimateur-de-larcom_147479.html

38 "Un site pornographique menacé de blocage signale près de 2 000 autres sites X oubliés par le CSA", *NextInpact*, 28 December 2021: https://www.nextinpact.com/article/49280/un-site-pornographique-menace-blocage-signale-pres-2-000-autres-sites-x-oublies-par-csa

39 In a recent report, the 5Rights Foundation identifies ten different age verification approaches. See: 5Rights (2021), "But how do they know it is a child? Age Assurance in the Digital World", p. 25: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

40 This list of age assurance techniques is not intended to be exhaustive, but rather to present the broad range of available solutions. In addition, different approaches are very often used together. It is also only one of the various possible ways of categorising these techniques. The French data protection authority (CNIL), for example, distinguishes between declaration, certification, and artificial intelligence, while 5Rights lists ten different techniques. See: CNIL, "Recommandation 7: vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée", 9 June 2021: https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee ; 5Rights (2021), *op. cit.*, pp. 22-44.

less restrictive for Internet users and online service providers, more or less accessible for the operators who have to implement them, and more or less reliable.

### Self-declaration

This is the least restrictive age assurance technique, but also the least secure (44% of 11-18 year olds, for example, say they have already lied about their age on social networks[41]), since it is based on a simple declaration by the Internet user that he or she is of the minimum age required to access the service in question. This declaration can be made in different ways. It can be a simple button to click or a box to tick, to self-certify that you are over the minimum age. It can also be as simple as filling in your date of birth. In order to limit the possibility of misrepresentation, some digital services providers, including some social network platforms, such as TikTok, limit the number of times a user can attempt to fill in their date of birth. Sometimes, self-declaration is combined with verification of an email address or mobile phone number. Some services use self-declaration as a first step to check the age of their users, before asking them to provide other information, such as a passport photo or facial image, against which they can compare the declared age.

### Declaration by a third party

Some online services, for example video streaming services, may allow adult account holders (who have had to provide bank details or official identification to activate the service) to create a restricted account for their child. This is the case, for example, with the "Kids" (7+) and "Teen" (13+) accounts on Netflix, or YouTube Kids on YouTube. In these cases, it is the adult's responsibility to indicate the age group to which their child belongs. Once logged in to their account, children cannot change the settings related to this category, unless they have at least the password used by the adult who created their account.

### Verification

Age verification involves asking the user to upload either an official identity document (e.g. a national identity card or passport) or (if the purpose is to verify majority) a credit card (in some countries, such as the United Kingdom, you have to be 18 to be a credit card holder). In order to ensure that the person attempting to access the service is indeed the holder of the official document, the verification can be combined

41 Génération Numérique (2021), "Les pratiques numériques des jeunes de 11 à 18 ans", 24 pp.: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf

with a real-time facial scan (photo or video). This is necessary, for example, to access certain online banking services, which offer a connection via facial recognition. This is equivalent to identity verification, which is not always the case. This method can be carried out directly by the service in question, or via one (or more) private or institutional trusted third party, such as a digital identity provider, like FranceConnect or Facebook Connect (especially in cases where the service provider does not need to check the identity of the person, but only their age). There are also "age token" providers, which pass on to the relevant services the information that the user is of the right age to access the service or not, without revealing their identity, or even their exact age.

**Estimation**

Age estimation is the process of estimating the age of the user, often using artificial intelligence (AI) algorithms, sometimes via keyword analysis, without identifying the user. Facial analysis estimation, for example, is done by comparing a photo and/or video snapshot of the person with large databases containing millions of faces of people of various ages. The estimation can also be made by processing and analysing behavioural data and metadata (time and length of connection, types of content "liked", viewed or shared, age of the people to whom the user subscribes or with whom they interact, type of language used, etc.). This technique can be likened to profiling.

## BALANCING CHILD PROTECTION AND THE RIGHT TO PRIVACY

The current situation is difficult to overcome partly because the nature of the solutions proposed to control child access to certain online content (in particular content of a pornographic nature, or content likely to impair their physical, mental or moral development, as required by the AVMS Directive) or to offer them a higher degree of protection than other users (in terms of the processing of personal data, for example, as required by the GDPR), may entail encroaching not only on their own rights, but also on those of adult Internet users. Applying differentiated protection rules depending on whether a user is a child or not, or whether he or she is 13, 14, 15 or 16 years old, requires, first of all, being able to determine the age or age

range of this user. Regardless of the technology chosen to carry out the age assurance, this is relatively intrusive. Among the various technical solutions available, there is a range of options that are more or less intrusive, more or less effective and more or less accessible to the operators likely to implement them. In a recent note entitled *Online underage users detection: can we reconcile efficiency, convenience and anonymity?* PEReN (the French Digital Regulation Expertise Centre)[42] has drawn up a critical overview of these solutions (see Table 1 below).

## Table 1 — Summary analysis of age verification solutions

| | Platform | Users | | | Efficiency | | |
|---|---|---|---|---|---|---|---|
| | Ease of implementation | Readibility | Practicality | Minimally intrusive | Fraud-resistant | Performance | Flexibility |
| Credit card check | √ | ! | ! | √ | √ | ! | ! |
| Verification by a newsagent's | √ | ! | × | √ | ! | ! | √ |
| Use of a national database | √ | × | √ | √ | √ | √ | √ |
| ID and photo check | √ | × | × | × | √ | √ | √ |
| Digital Identity Assurance Service (DIAS) | √ | √ | × | √ | √ | √ | √ |
| Parental control | √ | √ | √ | √ | √ | ! | √ |
| Content-based social profiling | × | × | √ | ! | × | × | × |
| Use of biometrics | √ | × | × | ! | × | × | ! |
| Self-declaration | √ | √ | √ | √ | × | ! | √ |

√ Satisfactory ! Not very satisfactory × Unsatisfactory

Source: PEReN

42 PEReN is placed under the joint authority of the French Ministers of Economy, Culture and Digital Technology.

By checking an official document (for example, an identity card) and a photo or video taken at a given moment, it is possible to verify a person's age (or even identity) with almost 100% certainty. This is for instance the case with FranceConnect, the online identification and authentication service provided by the French Interministerial Digital Directorate (Dinum), which allows access to several online public services[43] (French public healthcare insurance, tax office, etc.). Although verification via official documents is one of the most reliable solutions, the nature of the documents in question (passports, ID cards) is particularly sensitive. In this respect, this solution is rather intrusive.

In order to avoid verification procedures that require the use of official documents, some online services turn to age or age range estimation systems, developed either in-house or by third party organisations which then act as a "trusted third party". The use of such a third party may, depending on the modalities, prevent the restricted website from linking personal or sensitive data[44] in its possession to the identity of the individual (as opposed to cases where the restricted service completes the age check itself). In the United Kingdom, for example, company Yoti has developed a system for estimating age by facial analysis[45]. In order to access the services (websites, applications, etc.) that use this solution, a person must take a photo and video capture of their face. Once the capture is made, an algorithm instantly estimates the person's age or age range. Depending on the parameters defined by the restricted service, it receives an indication of the user's age, for example 13-, 13+,

43 For more information, see: https://franceconnect.gouv.fr

44 Sensitive in the traditional meaning of the word, "to be treated with particular care and vigilance", not in the sense of the GDPR.

45 For more information, see: https://www.yoti.com/business/age-verification/ and https://yoti.world/age-scan/

18+ or 21+, but no directly identifying personal data[46]. Although the algorithms underlying these solutions are becoming increasingly accurate, margins of error remain. For example, the margin of error for Yoti's facial age estimation solution is 2.96 years for 6-70 year olds, 1.52 year for 13-19 year olds, and 1.56 year for 6-12 year olds[47]. While these margins of error are relatively low, they can be particularly problematic when estimating the age of a person who is very close to the limit set by the service. They may also lead to the exclusion of some people who should be able to access the service, or even to the provision of a different service without people being aware of it, if their age is underestimated.

The same applies to age estimation systems that rely on the analysis of behavioural data or metadata or on natural language processing[48] (time and length of connection, types of content "liked", viewed or shared, age of the people to whom the user subscribes or with whom they interact, type of language used, etc.). The results deduced by the algorithms on which these solutions are based are in fact only predictions, which by definition include margins of error. Furthermore, some techniques, such as language analysis, may have additional biases if not implemented correctly. For example, just because someone makes a lot of spelling mistakes or is a fan of manga, does not mean that they are underage[49]. While age estimation techniques based on artificial intelligence are sometimes perceived as less intrusive than strict age verification, it is important to stress that these usually rely

46 Yoti, on the other hand, is sent the person's image, which does not necessarily constitute "sensitive" data in the GDPR sense. Indeed, Recital 51 of the GDPR states that *"the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."*

47 Yoti, "Age estimation White Paper", May 2022: https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-May-2022.pdf

48 Natural language processing (NLP) is based on training artificial intelligence algorithms using very large databases.

49 To find out more about the limitations of natural language processing, and the difficulties of processing unnatural language (e.g. emojis), listen to the "La modération: défis et dilemmes" podcast, by Xavier de La Porte for *France Inter*: https://www.franceinter.fr/emissions/le-code-a-change/la-moderation-defis-et-dilemmes

heavily on the processing of sensitive data[50], including personal data. In its recent note, PEReN considers these systems to be "unsatisfactory" in terms of the degree of intrusiveness (see Table 1). Beyond purely technical considerations, it should also be noted that, insofar as nothing biologically happens on the evening of 17 years and 364 days, no algorithm can be "sufficiently" accurate to be 100% reliable, ever.

Although the road to standardisation is still not well explored in the field of age verification, some standards are beginning to emerge. This is the case, for example, of the British standard PAS 1296:2018[51], which defines "levels of certainty" based on "trust vectors" for age estimation tools via facial analysis. In order to take into account the principle of proportionality[52], which is at the heart of European law, these standards cannot however be limited to purely technical aspects such as accuracy or performance. They must also incorporate legal criteria, such as compliance with the Charter of Fundamental Rights of the European Union and, depending on use cases, compliance with the GDPR and other norms specific to the Member States[53].

When it comes to choosing between one solution or the other (self-declaration, declaration, verification or age estimation), the whole issue lies in a trade-off in terms of privacy, between the need to verify the age of Internet users in order to be able to guarantee some of their rights in the most appropriate way, on the one hand, and the minimisation of the data collected and processed for this purpose, on the other. In Article 6a, the AVMS Directive thus recommends the use of technical measures that

50 Sensitive in the traditional meaning of the word, "to be treated with particular care and vigilance", not in the sense of the GDPR.

51 For more information, see the British Standards Institution's website: https://shop.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice/standard/preview

52 The principle of proportionality is defined as a *"weighting mechanism between legal principles of equivalent rank, simultaneously applicable but antinomic"*, G. Xynopoulos, "Proportionnalité", in D. Alland and S. Rials (2003), *Dictionnaire de la culture juridique*, PUF, 2003, p. 1251.

53 Renaissance Numérique has also made this recommendation on standards for facial recognition technologies. For more information, see: Renaissance Numérique (2020), "Facial Recognition: Embodying European Values", 103 pp.: https://www.renaissancenumerique.org/wp-content/uploads/2022/06/renaissancenumerique_report_facialrecognition.pdf

*"shall be proportionate to the potential harm of the programme"*. Similarly, the UK's Age Appropriate Design Code requires digital services likely to be accessed by children to determine the age of their users with a degree of certainty that is proportionate to the risks to which children are exposed and that does not infringe their rights. Although some thought is beginning to be given to this issue at European level[54], the jury is still out.

## THE NECESSARY BALANCE BETWEEN DIFFERENT FUNDAMENTAL RIGHTS IN THE CONTEXT OF ONLINE CHILD PROTECTION: THE CSAM REGULATION EXAMPLE

Despite the addition of safeguards in the proposed Child Sexual Abuse Material (CSAM) regulation presented by the European Commission in May 2022, the text, as drafted, introduces serious risks to the right to privacy, in particular with regard to the confidentiality of private electronic correspondence.

According to Article 3 of the proposal, online content hosts and messaging services will have to carry out an assessment of the risks of CSAM being found on their platform. This analysis must be shared with the competent national authority and should include measures aimed at eliminating these risks (Article 4). If the authority deems that *"there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse"* and that *"the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties"*, it may then request[55] a competent judicial authority to issue a detection order against the service in question (Article 7). As stipulated in Article 10 of the proposed regulation, the service would then be obliged to install and operate *"technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children"*. While the European Commission does not name specific technologies for this purpose[56], it does specify

54 See in particular the new strategy for a Better Internet for Kids (known as "BIK+") announced by the European Commission on 11 May.

55 After consulting the ad hoc European Centre, established by the Regulation. For more information, see: "Un nouveau centre européen contre les abus sexuels sur mineurs", *Contexte*, 11 May 2022: https://www.contexte.com/actualite/numerique/un-nouveau-centre-europeen-contre-les-abus-sexuels-sur-mineurs_150538.html

56 It entrusts this responsibility to the European Centre.

that these technologies must be effective for the purpose intended, and must *"not be able to extract any other information from the relevant communications than the information strictly necessary"* to achieve the objective in question, in accordance with the indicators that will be laid down by the European Centre to prevent and counter child sexual abuse (Article 10(3)b).

Renaissance Numérique considers these safeguards insufficient to preserve the balance between our fundamental rights and freedoms. The think tank therefore encourages the European Commission to ban any measure that would lead to a disproportionate encroachment on the right to privacy or that could introduce cybersecurity risks. This would be particularly the case for tools that weaken end-to-end encryption of private communications, or that install detection mechanisms directly on people's devices[57] [58].

Article 8 of the GDPR, which sets the minimum age for consenting to the processing of personal data, does not differentiate between the different types of content to which individuals may have access. It sets specific conditions for the collection and processing of children's personal data, but does not prohibit it. As such, it applies to all online services providers, and does not impose stricter obligations than others depending on the data controller's line of business[59]. On the other hand, following a proportional approach with regard to the potential risks incurred, some national regulations, such as the French Penal Code, Public Health Code and Homeland Security Code, impose restrictions or bans on access to certain goods and services (pornographic content, online betting, sale of alcohol, etc.) below a certain age. For operators providing these products or services, the age assurance requirement is all the more critical, as it seeks to determine whether or not an

57 "Pourquoi l'outil de détection de la pédopornographie d'Apple fait polémique", *Le Monde*, 26 August 2021: https://www.lemonde.fr/pixels/article/2021/08/26/pourquoi-l-outil-de-detection-de-la-pedopornographie-d-apple-fait-polemique_6092405_4408996.html

58 "Apple delays plan to scan iPhones for child abuse images", *CNET*, 3 September 2021: https://www.cnet.com/tech/mobile/apple-delays-plan-to-scan-iphones-for-child-abuse-images/

59 In line with the principle of proportionality, however, checks are strengthened for certain "special categories of personal data" as defined in Article 9 of the GDPR (genetic data, biometric data, data revealing racial or ethnic origin, political opinions, etc.).

individual has the legal right to access the product or service in question. In favour of a proportionate approach to age assurance, Renaissance Numérique recommends that, where provisions for restricting or prohibiting access exist, a "strict" age assurance should be imposed through verification. In these instances, the risk of fraud through misrepresentation or error in age estimation is too significant.

While age verification has the advantage of being the most accurate age assurance technique, it does imply, in the light of existing solutions, that Internet users over the age of 18 must accept that accessing certain content (e.g. pornography) will not be as straightforward. Furthermore, although verifying age does not necessarily mean verifying identity, this approach may be considered particularly intrusive and likely to dissuade certain uses. As pointed out in a recent report co-written by the French General Inspectorate of Finance and General Council for the Economy, Industry, Energy, and Technology, *"it is likely that these measures may lead to a feeling of restriction of individual freedoms"*[60]. In its recent position paper, PEReN also stressed, in relation to age assurance, that it is also "the social acceptability of the control" that should guide the choice of the tool used. Renaissance Numérique supports the recommendation made by the centre of expertise, which advocates leaving users the choice of the technical solution they wish to use in order to verify their age. However, this means that the online services concerned must offer several solutions, which is rarely the case at present. This is a major issue, which will have to be addressed and thought through in the context of discussions on future digital identity systems. In this respect, the interoperable proof-of-age reporting mechanism developed as part of a partnership between PEReN, the CNIL (French data protection authority) and Olivier Blazy[61], professor at *École*

60 General Inspectorate of Finance and General Council for the Economy, Industry, Energy and Technology (2019), "Prévention de l'exposition des mineurs aux contenus pornographiques sur Internet": https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2019_12_Prevention_mineurs.pdf

61 "Demonstration of a privacy-preserving age verification process", LINC (CNIL's digital innovation lab), 21 June 2022: https://linc.cnil.fr/fr/demonstration-privacy-preserving-age-verification-process

*Polytechnique*[62] and researcher in cryptography, published on 21 June 2022, deserves particular attention. It could help to materialise the recommendation made by the CNIL in its opinion of 3 June 2021, namely the use of a *"double anonymity system preventing, on the one hand, the trusted third party from identifying the website or application from which a verification request was made and, on the other hand, preventing the transmission of identifying data relating to the user to the website or application offering pornographic content".*

## OBLIGATIONS THAT CLASH WITH ECONOMIC OBJECTIVES

However, the complexity of balancing children's online protection with the protection of their privacy (and that of Internet users in general) is not the only obstacle to the implementation of legal provisions imposing age assurance. In order to understand different digital services providers' behaviour in this respect, we need to take into account the diversity of these stakeholders and their business models.

As researcher Anne Cordier explains, the main social networks and some other services, such as video streaming platforms, are based on an "attention economy", which consists in "attracting" users by suggesting an infinite amount of content that they are bound to like, and thus prolong their usage time. In particular, she cites scrolling or automatic video playback practices, which she says encourage people to get "locked-in" to a platform or application[63]. The more a person spends time and interacts with such a service, the more data the service can collect on the person and their usage, and then exploit or resell it to third parties. These commercial strategies, which are based in particular on interface design, and which aim to attract as many

62 A top engineering school in France.

63 "Quand les GAFA captent l'attention des enfants", podcast, *France Culture*, 20 December 2021: https://www.franceculture.fr/emissions/entendez-vous-l-eco/quand-les-gafa-captent-l-attention-des-enfants

active users as possible and to ensure that they spend as much time as possible on the service in question, are not necessarily compatible with an obligation of age assurance: "filtering" users at point of entry can lead to a reduction in user numbers.

Setting up systems aimed at restricting access to certain content for children or granting them greater protection than other users can lead to a deterioration in the user experience, which can then lead to the user abandoning the service altogether. As mentioned in an interview with Yoti, some pornographic websites that had set up age assurance systems to access their content gradually abandoned them, noticing a massive diversion of their traffic to other websites. This reaction shows how difficult it is to reconcile the economic objectives of certain players with the challenges of protecting children's rights online. In their conversations with Yoti's teams, these websites specifically identified the cause of this diversion as being the lack of incentive from national and regulatory bodies to require all players in the online pornographic content industry to implement age verification measures, generating a distortion of the market and a set of obligations of varying magnitude for certain players.

*“There is a concern that age assurance not done well will end up being the next "cookie issue", resulting in friction that could lead to people not using the services.”*

MICHAEL MURRAY,
Head of Regulatory Strategy, Information Commissioner's Office (ICO)

Furthermore, the introduction of entry barriers may lead to users resorting to technical circumvention systems, if they do not wish to give up the service in question. Virtual private networks (VPNs) are often cited as a means of accessing websites blocked by ISPs or content that is geo-blocked (e.g. Netflix's content catalogue).

## A LACK OF HOMOGENEITY, WHICH MAKES COMPLIANCE DIFFICULT

The lack of homogeneity of the legal provisions introducing the need for age assurance is a third factor that contributes to their lack of enforcement.

First of all, there is a certain legislative fragmentation within the European Union regarding parental consent verification. Admittedly, the GDPR has allowed a certain harmonisation between Member States with regard to the protection of personal data in general. However, at the same time, Article 8(1), which sets out the obligation of consent from a person with parental responsibility for the child, for the processing of personal data of children under the age of 16, stipulates that: *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years"*. Thus, this age varies within the EU from one country to another: 13 in Belgium, Denmark, Finland and Sweden[64], 14 in Austria, Italy and Spain, 15 in France and the Czech Republic, 16 in Ireland, the Netherlands and Slovakia...While these variations reflect societal habits and the child protection culture in different European states (e.g. the choice of 15 years in France reflects, for example, the age of sexual majority), they are a challenge for the different online service providers.

64 The age is also set at 13 in the UK.

*"Depending on the country, the age at which a person can give consent to their personal data being processed varies between 13 and 16 in Europe, according to the GDPR. There is thus a wide range of consent ages across the EU and, as a result, it is complex for industry to apply this law. Actions in the Commission's recently adopted Better Internet for Kids+ strategy include a comprehensive code of conduct on age appropriate design and a technical standard to address what constitutes effective age verification. Such actions will support practical implementation of this and other legal provisions on child online safety."*

JUNE LOWERY-KINGSTON,
Head of the "Accessibility, Multilingualism and Safer Internet" Unit,
DG CNECT, European Commission

However, some recent developments show not only the willingness but also the ability of private stakeholders to align themselves at an international level on certain crucial points. With regard to age assurance tools, in addition to developments in the UK, a standard is currently under consideration within the International Organisation for Standardisation (ISO)[65]. Based on a proposal submitted by the UK in April 2021 (supported by the Department for Digital, Culture, Media and Sport (DCMS)), ISO has launched a preliminary work item (PWI), PWI 7732, to address three dimensions of this potential future standard: Framework, levels of assurance and privacy protection; Conformity assessment; and Interoperability[66]. While a draft version of the standard was expected by the end of 2021, it has not yet been published.

The euConsent initiative, funded by the European Commission and initiated by the European Parliament, is working towards a secure and certified pan-European system for age verification and parental consent[67]. Currently, a user

65 See: https://genorma.com/en/project/show/iso:proj:82892
66 See: https://avpassociation.com/standards-for-age-verification/
67 For more information, see: https://euconsent.eu/

must verify their age on every website or application that uses an age assurance service. euConsent's aim is to achieve a fully interoperable system at EU level, which allows a user who has already done an age assurance check via one age assurance provider to be recognised and not to have to repeat the process on websites using other providers[68]. The project also aims to simplify the process of obtaining parental consent. After a year of internal work, a pilot project was launched with 1,600 people (adults and children) in five Member States. The network's aim is to have an operational solution by summer 2022.

This is a priority for the European Commission, which reiterated in its Better Internet for Kids+ (BIK+) strategy[69] announced on 11 May 2022 that it will *"support methods to prove age in a privacy-preserving and secure manner, to be recognised EU-wide. The Commission will work with Member States [...], relevant stakeholders and European standardisation organisations to strengthen effective age verification methods, as a priority. This work will encourage market solutions through a robust framework of certification and interoperability"*[70]. These developments indicate a move towards more harmonisation, which Renaissance Numérique commends. In order to promote the application of existing legal provisions, it seems crucial to put a common framework of requirements in place for all Member States.

68 In this respect, see euConsent Project Manager Iain Corby's intervention, at the "Helping young people to better protect their privacy and safety online" webinar, organised by Privacy Laws & Business on 16 March 2022: https://www.privacylaws.com/events-gateway/events/youth22/

69 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2022) 212 final, "A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)", p. 12: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN

70 *Ibid.*, p. 13

PART III

# Implementing a common framework of requirements at European level

## ESTABLISHING A EUROPEAN BINDING CODE

In the absence of a common set of requirements, there are challenges in ensuring age assurance for children's online protection at a European level. Thus, companies' competitive and commercial considerations often take precedence over this protection issue (although there are exceptions). It therefore seems essential to specify, at a European level, the minimum requirements for effective internet user age assurance, that is compatible with our fundamental rights when situations require it.

Since the legal requirements do exist, it is not a question of enriching or expanding the existing legal framework. Instead, it is a matter of translating these requirements into operational and technical terms. In this respect, the British approach should inspire European players. The Children's Code, which came into force on 20 September 2020, lists fifteen principles that providers of online services likely to be consulted by children must respect in terms of personal data protection[71]. As the Code is legally binding (it is based on the UK GDPR), the Information Commissioner's Office (ICO) can issue fines and penalties for non-compliance with the principles set out in it. In order to add to and clarify these general principles, the Information Commissioner's opinion of 14 October 2021 on "age assurance for the Children's Code" proposes a number of guidelines. In particular, it lists six practices that are likely to result in particularly high risks for children in relation to data processing:

- large-scale profiling (e.g. identifying a child as belonging to particular groups);
- 'invisible' data processing (e.g. sharing their data with third parties);
- targeting of children for marketing and advertising

71 For the list of principles, see: ICO (2020), "Age Appropriate Design: A Code of Practice for Online Services", pp. 7-8: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

purposes (e.g. personalising marketing content based on their data);

- tracking (e.g. by geolocation);
- ISS activities that may lead to risks of physical or developmental harm (e.g. through leakage of data concerning the child's health);
- ISS activities that may entail a risk of harmful usage (e.g. data processing that is clearly detrimental to the child's welfare)[72].

In its new BIK+ strategy, the European Commission announced its intention to help implement a *"comprehensive EU code of conduct on age-appropriate design"* by 2024[73]. This text, most likely inspired by the Children's Code but intended to go beyond data protection considerations, would be based on the new rules contained in the Digital Services Act, on the AVMS Directive and on the GDPR. As set out in its strategy, the Commission sees this code as a co-regulatory initiative, but one that would not be binding, as adherence to the code would be voluntary. In order to strengthen its scope and effectiveness, Renaissance Numérique encourages the European Commission, the Member States, and all relevant stakeholders to explore the possibility of a binding code of conduct, following the example of the UK Children's Code.

In addition to the GDPR, the AVMS Directive and the DSA, this code could be based on non-binding texts, such as the guidelines of the European Data Protection Board (EDPB)[74]

72 ICO, "Information Commissioner's opinion: Age Assurance for the Children's Code", 14 October 2021: https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf

73 "New European strategy for a Better Internet for Kids – Questions and Answers", European commission, 11 May 2022: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826

74 In its "Guidelines 5/2020 on consent under Regulation (EU) 2016/679", adopted on 4 May 2020, the EDPB states, for example, that *"A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors."* These guidelines also include considerations on how to carry out age verification (§ 135). See: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

and the Council of Europe[75]. The European code should define, among other things, the cases where an age declaration or estimation is not sufficient and where verification is required. It should also provide clear principles enabling stakeholders to carry out impact assessments, and a toolbox made available to them. In addition, it would be useful to set up a regulatory dialogue, bringing together all the stakeholders concerned, with a view to defining the tools to be used depending on the use cases. This approach would ensure that, among the range of solutions offered to users to verify their age, all are proportionate and based on a full impact assessment.

In order to be proportionate, any such approach needs to be able to assess the risks to which children are exposed, but also the opportunities they are likely to encounter by accessing these online services, the impact of possible measures on other users, on competition in the sector, the cost to the parties concerned, how easy it is to circumvent the measures being considered, etc. For this reason, online services providers who are likely to be accessed by children cannot simply carry out risk assessments. Instead, the preferred course of action is to carry out impact assessments, which allow for the inclusion of both opportunities and risks, as well as other key variables.

In order to ensure the Code's maximum effectiveness, its development and implementation should be subject to enhanced cooperation between Member States and the relevant regulatory authorities (at least data protection authorities, rights advocates, and the authorities that make up the European Regulators Group for Audiovisual Media Services (ERGA)). Furthermore, it is crucial that the latter have the necessary means (human and financial, but also in terms of skills) to verify the application of the Code.

75 In particular, its "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", 2018: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a; and "Children's data protection in an education setting - Guidelines", 2021: https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html

## HOLDING ONLINE SERVICES PROVIDERS ACCOUNTABLE

Renaissance Numérique encourages the introduction of obligations of means in terms of age assurance, in an approach that combines prescription and sanctions, in the same vein as that envisaged for the regulation of online content[76]. Through its relative flexibility, this type of approach encourages stakeholders to go about completing their work using a "trial and error" method[77]. The idea is not to sanction the slightest deviation from the code, but the absence of an action plan to rectify the deviations identified and to demonstrate that the risks have been clearly identified, prioritised, etc. This is precisely the general thrust of the Digital Services Act.

*"The GDPR does not dictate one default organisational procedure, because we know very well that there are as many types of organisations as there are players, whether they are public, private, large companies, small associations, etc. But from the moment you handle personal data, it is a great responsibility, and you have to get organised. You are free to do it as you like; you won't be asked to fill in 42,000 Cerfa forms[78] to prove that you have complied with everything, you just need to document what you are doing to achieve these personal data protection objectives."*

ALEXANDRE ARCHAMBAULT,
Lawyer at the Paris bar, expert in digital law

Additionally, while the public sector is perfectly legitimate in setting the objective (age assurance in cases where it considers it necessary) and a common set of requirements, it must be careful not to tailor or fine-tune the system by imposing certain

76 It should be noted, however, that the idea is not to encourage impunity. For the most serious cases, non-compliant players should be sanctioned from the very first error. This could typically be the case, for example, for pornographic websites that do not offer any age assurance system.

77 For more information on the "trial and error" method, see: https://en.wikipedia.org/wiki/Trial_and_error

78 Official forms for carrying out administrative procedures in France.

age assurance technologies. It must, however, ensure that these technologies are available and accessible. As Mathieu Weill, Head of the Digital Economy Department at the French General Directorate for Enterprise (DGE), said at the closing event of the French Presidency of the European Union, *"the subject is too important to be totally privatised"*. In order to avoid developing regulations that would create competitive advantages for certain players, he recommends working according to the "digital commons" approach[79], which he says is *"feasible for age assurance"*. This is precisely what is at stake in the regulatory dialogue referred to above, which is intended to serve as a means of specifying the general framework developed by the public authorities.

Furthermore, this approach, which is both prescriptive and punitive, would help to hold digital services providers accountable. The Children's Online Privacy Protection (COPPA) Rule[80], a US law aimed at protecting children's privacy on the Internet, is an inspiring example in this respect. In terms of data protection, the COPPA Rule explains how to verify parental consent before collecting, using, or disclosing children's personal data, but does not impose a specific method for doing so. However, the Federal Trade Commission (FTC) has identified a number of consent methods[81] that are considered to meet the COPPA Rule's requirements. Operators may also submit new parental consent methods to the FTC for review and approval. In an effort to ensure transparency, the FTC publishes the proposals that it has approved and rejected. Operators thus have a list of solutions deemed compliant and non-compliant by the regulator.

79 For more information on "digital commons", see: https://en.wikipedia.org/wiki/Digital_commons_(economics)

80 Federal Trade Commission, "Verifiable Parental Consent and the Children's Online Privacy Rule": https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule

81 Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business", step 4: https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4

In France (as in Europe), we have not yet achieved this type of co-construction between regulators and operators, and best practice sharing. Some progress has been made, however, with the recent publication by the CNIL of clarifications concerning its position on age assurance on the Internet[82]. Despite some encouraging signs, it would appear that the relevant national independent authorities, notably the CNIL and Arcom, are still struggling to fulfil their role. Due to recent developments in digital regulation at a European level, these authorities are faced with an accelerated broadening of their responsibilities, which obliges them to gain expertise on many subjects, and to do so very rapidly. In addition, the monitoring of the impact assessments recommended within the context of this report requires significant resources, which these authorities do not currently have. It is therefore essential to provide these authorities with the means to fully carry out their duties, by prioritising harmonisation of regulation at a European level. Without this, they will never be able to keep up with the technological pace of the players that they have to regulate.

82 "Vérification de l'âge en ligne: trouver l'équilibre entre protection des mineurs et respect de la vie privée", CNIL, 26 July 2022: https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie

CONCLUSION

# Building a common vision for children online

Behind age assurance lie the main challenges involved in protecting children and, more broadly, guaranteeing their rights in the digital environment. With regard to the existing legal provisions, the legal framework surrounding children's use of digital services appears relatively comprehensive. In particular, it is supposed to provide greater protection for their personal data and prevent their exposure to illegal or harmful content. However, certain provisions, such as Article 8(1) of the GDPR and Article 227-24 of the French Penal Code, which require an age assurance of Internet users, are not systematically applied. It is therefore urgent to provide the independent authorities in charge of their enforcement with additional resources so that they can carry out their tasks and monitor and, if necessary, sanction online services that do not comply with their obligations. These additional resources should also enable them to conduct a quality regulatory dialogue with all the stakeholders concerned, in order to ensure the proper implementation of these regulations.

Current developments at a European level[83] should be an opportunity to move towards greater harmonisation between Member States. In this respect, the drafting of the future EU code on age-appropriate design will require substantive dialogues to develop a common vision for children online. At the heart of the issue of the use of digital services by children is the question of "digital maturity". Beyond the respect of legal ages for accessing certain content and services[84], the quality of children's experience in the digital environment depends above all on their command of this space. Thus, faced with the risks and opportunities that digital technology can represent, one of the main responses should be to support children in gradually acquiring a certain degree of digital maturity. However, as the interviews conducted as part of this study revealed, the very

83 The latter (the euConsent initiative, the draft CSAM regulation which intends to create an EU centre responsible for preventing and combating sexual abuse of children online, the future EU code on age-appropriate design) testify to an awareness of the relevance of the European level to deal with this issue. Still, they introduce the need to consider their articulation to prevent redundancies or possible lack of harmonisation at European level.

84 Which some people incorrectly refer to as a "digital majority".

notion of digital maturity is still struggling to be thought through by all the stakeholders involved.

*"Digital maturity should not only be assessed based on age. It also relates to how children are educated, informed, and supported. When we talk about digital maturity, we must also take psychological factors into account. This maturity is not only biological, it is also societal and psychological, which is why it is important to work together with other stakeholders such as psychologists or child psychiatrists, teachers, educators, and parents."*

NAJAT MAALLA M'JID,
Special Representative to the United Nations Secretary-General on Violence against Children

Following on from this report, and in order to help shed light on these issues, Renaissance Numérique is preparing to launch a second study, which will question the need to develop children's rights in view of their digital practices. To do this, our working group will focus on particular categories of young people, such as unaccompanied minors, children that are placed in child welfare care, juvenile detainees, and children with disabilities. This reflection will occupy the think tank in the coming months and will lead to a second publication in the course of 2023.

# ACKNOWLEDGEMENTS

We would like to thank the various stakeholders who were interviewed as part of this study for their contribution, namely:

**Alexandre Archambault**, Lawyer at the Paris Bar, expert in digital law

**Florian Chevoppe-Verdier**, Policy and Legal Advisor, Yoti

**Julianna Cotto**, Privacy Policy Manager, Youth, Meta

**Julie Dawson**, Director of regulatory and Policy, Yoti

**Sharone Franco**, Head of Legal, Yubo

**Rachael Gallagher**, Privacy Policy Manager, EMEA, Meta

**Antonio Garcia Valdes**, Education Product Manager, Apple

**Stéphane Harrouch**, Senior Manager Government affairs and Public policy, YouTube

**Almudena Lara**, Child Safety Senior Manager, Google

**Margaux Liquart**, Lead Safety Product Manager, Yubo

**June Lowery-Kingston**, Head of the "Accessibility, Multilingualism and Safer Internet" Unit, DG CNECT, European Commission

**Najat Maalla M'jid**, Special Representative to the United Nations Secretary-General on Violence against Children

**Jean-Marc Merriaux**, French Ministerial Delegate for "21st Century Skills"

**Alexandra Mielle**, Head of the "Protection of Audiences" department, French Regulatory Authority for Audiovisual and Digital Communication (Arcom)

**Michael Murray**, Head of Regulatory Strategy, Information Commissioner's Office (ICO)

**Chris Payne**, Director of Digital Responsibility, Government and Public Affairs, LEGO Group

**Lucile Petit**, Head of the Online Platforms Department, French Regulatory Authority for Audiovisual and Digital Communication (Arcom)

**Léo Sicouri**, Partnerships Lead, Yoti

**Bruno Studer**, Member of the French Parliament (Bas-Rhin's 3rd constituency)

**Dania Tanur**, Privacy Policy Manager, Youth Products, Meta

**Capucine Tuffier**, Public Policy Manager, France, Meta

**Nicolas Vignolles**, Executive Director, *Syndicat des éditeurs de logiciels de loisirs* (French Union of Entertainment Software Producers)

**Charlotte Yarrow Cockings**, Child Safety Counsel, Apple

## MEMBERS OF THE WORKING GROUP

**Justine Atlan** (co-pilot), Director General, e-Enfance/3018 Association

**Thomas Bellaïche**, Senior Legal Counsel, Yubo

**Lucien Castex**, Public Affairs and Partnership Development Representative, AFNIC

**Samuel Comblez**, Director of Operations, e-Enfance/3018 Association

**Maxime Drouet**, Associate Professor, Gustave Eiffel University

**Olivier Esper**, Senior Manager Public Policy, Google

**Sarah Khemis**, Senior Manager Institutional Relations and Public Affairs, France, TikTok

**Julie Lavet**, Senior Government Affairs Manager, France, Apple

**Samuel Le Goff**, Consultant, CommStrat

**Noémie Minster,** Corporate Communications Manager, Kaspersky

**Annabelle Richard** (co-pilot), Associate lawyer in the "Technologies, Media, and Telecommunications" division, Pinsent Masons

**Capucine Tuffier,** Public Policy Manager, France, Meta

## AUTHORS

**Jessica Galissaire**, Studies Manager, Renaissance Numérique

**Annabelle Richard**, Associate lawyer in the "Technologies, Media, and Telecommunications" division, Pinsent Masons

## PROOFREADING

**Jennyfer Chrétien**, General Manager, Renaissance Numérique

**Henri Isaac**, Associate Professor, Paris Dauphine University - PSL

## TRANSLATION

**Jen Smith**, Founder and Translator, Camaleon Translations

We would also like to thank **Audrée Latinaud,** project assistant at Renaissance Numérique, who supported the working group at the beginning of its discussions.

**Renaissance Numérique**

32 rue Alexandre Dumas — 75011 Paris
https://www.renaissancenumerique.org/en/

**Septembre 2022**