SciencesPo
CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Towards Harmonised Online Age Verification?

A Comparative Study of French and EU Legal Frameworks

Alexandre HUMAIN-LESCOP
PhD researcher in Law and Regulation
University Institut Polytechnique de Paris (IP Paris)

May 2025

ACKNOWLEDGMENTS

This study was pre-published in January 2025 under the following reference. Humain-Lescop A., *Towards harmonised online age verification? A comparative study of French and EU legal frameworks*, Pre-publication for forthcoming publication by the Digital, Governance and Sovereignty Chair at Sciences Po, January 2025. Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123971
Only formal modifications have been made since, up to this final version.

The first thanks go to Florence G'sell and the *Digital, Governance and Sovereignty Chair at Sciences Po*, which initiated this study, initially submitted in December 2024, and to its partners. Special thanks also go to Magalie Dansac Le Clerc and Marlyse Lissan, lawyers at Baker McKenzie, with whom the topic of online age verification had already been explored through our co-authored article *« Les enjeux de la vérification de l'âge en ligne : entre volontés politiques et réalités techniques »* (*Revue Lamy droit de l'immatériel n°216, 2024*), which, in many ways, laid the groundwork for this study. Thanks also to Maxime Pettinaroli for his participation and assistance with proofreading. Finally, my sincere gratitude goes to Mehdi Arfaoui, Vincent Toubiana and the CNIL and LINC teams for their hospitality and kindness, as well as to Jeremy Bonan, César Boyer, Manon Cassoulet-Fressineau, Laure Fallou and the ARCOM teams for their warm welcome, availability as well as their valuable insights.

The views expressed in this study are those of the author alone and do not necessarily reflect the opinions or positions of the Digital, Governance and Sovereignty Chair of Sciences Po, its partners, or any other entities or individuals mentioned or thanked within the study.

KEYWORDS

Online Age Verification | Protection of Minors | Regulation | Access to Pornography | Access to Social Networks | Access to Online Gambling and Betting | DSA | Double Anonymity | Identity Verification | eIDAS 2.0's EDIW.

ABSTRACT

The growing exposure of minors to digital dangers challenges legislators around the world. The French and European legal frameworks this study intends to compare constitute a rich study field in this regard. They respectively consider various "*age verification scenarios*". In France, these scenarios concern in particular one's access to alcoholic beverages, tobacco and vaping products, online betting sites, social networks within the framework of the "*digital majority*" law (2023), and pornographic content in application of the SREN law (2024). At the EU level, several instruments such as the GDPR (2016), the revision of the AVMSD (2018), the DSA (2022) and the CSAR proposal (2022) also mobilize the notion of online age verification.

This study's aim is to highlight what may result from the confrontation of these different legal frameworks: their potential synergies and eventual difficulties regarding their interaction. While it is possible to identify the challenges these frameworks have in common, their overall coherence and effectiveness seem to need general improvement. These challenges are often linked to the lack of details on the "*age verification system*" that has to be established, i.e. the exact verification methods to implement. While the democratization of AI systems now makes it possible to estimate age notably on the basis of biometric elements, it is appropriate to question what could constitute the future in terms of age verification systems, regarding both the nature of the proof used and the architecture of the system.

Could a common "*European technical solution*" even be considered? In this regard, the 2024 ARCOM framework on access to pornography in France, requiring the use of at least one architectural system in "*double anonymity*", the direction taken for the current application of the DSA and the current implementation of the *EU Digital Identity Wallet* from the 2024 eIDAS 2.0 regulation seem to constitute promising tracks in this ambition of convergence of the different frameworks of online age verification.

ABBREVIATIONS AND ACRONYMS

AI	Artificial intelligence
AML/CFT	Anti-money laundering and combating the financing of terrorism
ANSSI	*(Agence nationale de la sécurité des systèmes d'information)* National agency for information systems security
ARCOM	*(Autorité de régulation de la communication audiovisuelle et numérique)* French regulatory authority for audiovisual and digital communication
ARF	Architecture and reference framework
Art.	Article
AVMSD	Audiovisual media services directive
AVPA	Age verification providers association
BIK	Better internet for kids
Chap.	Chapter
CNIL	*(Commission nationale de l'informatique et des libertés)* French National Commission for Information Technology and Civil Liberties
CSA	*(Conseil supérieur de l'audiovisuel)* French supreme audiovisual council
CSAR	Child sexual abuse regulation
DGA	Data governance act
DLT	Distributed ledger technology
DSA	Digital services act
E.g.	*(Exempli gratia)* For example
eCommerce (Directive)	Electronic Commerce (Directive)
EDIW	EU digital identity wallet
EDPB	European data protection board

EDPS	European data protection supervisor
EDRi	European digital rights
eID	Digital identity
eIDAS	Electronic identification, authentication, and trust services
ePrivacy (Directive)	(Directive on) privacy and electronic communications
Et al.	*(Et aliī)* And others
Etc.	*(Et cetera)* And so on
EU	European Union
FDJ	Française des jeux
Fig.	Figure
GDPR	General data protection regulation
IBAN	International Bank Account Number
Ibid.	*(Ibidem)* Same source as the previous one
I.e.	*(Id est)* That is
IP	Internet Protocol
JONUM	*(Jeux à objets numériques monétisables)* Games with monetizable digital objects
LCEN	*(Loi pour la confiance dans l'économie numérique)* Law for confidence in the digital economy
LINC	*(Laboratoire de l'innovation numérique de la CNIL)* Digital Innovation Laboratory of the CNIL
OECD	Organisation for economic cooperation and development
Op. cit.	*(Opus citatum)* Source already mentioned
P.	Page
Para.	Paragraph
PEReN	*(Pôle d'expertise de la régulation numérique)* French center of expertise in digital regulation
PID	Person identification data

PSD2	2nd Payment Services Directive
Pt.	Point
PVID	*(Prestataires de vérification d'identité à distance)* Remote identity verification providers
RNIPP	*(Répertoire national d'identification des personnes physiques)* French national directory for the identification of natural persons
SCA	Strong customer authentication
SMS	Short Message Service
SREN (law)	*((Loi) visant à sécuriser et à réguler l'espace numérique)* Securing and regulating the digital space (law)
Tab.	Table
VPN	Virtual private network
ZKP	Zero-knowledge proof

TABLE OF CONTENTS SUMMARY

A detailed table of contents can be found at the end of this study

INTRODUCTION

Regular statistics about minors in the digital environment are generally clear: minors' exposure to screens is increasing[1]. With 46% of minors equipped with a *smartphone* before their 10th birthday[2], pornography consumption among boys aged 10-11 is estimated at 21%[3]. This figure rises to 65% among boys aged 16-17. More broadly, with 59% of 11-14 year olds and 95% of 15-18 year olds registered on one or more social networks[4], 25% of 11-18 year olds[5] report being exposed to shocking content such as war scenes, torture, or executions. This rate increases when considering their exposure to other types of content: 30% of minors have read racist remarks and 45% of them have been exposed to animal abuse content. The risks of exposure to this kind of inappropriate content are directly linked to other related risks: addiction, exposure to self-harm practices, disinformation as well as cyberbullying. Being online also exposes minors to other types of dangers, such as abusive commercial practices, access to dangerous products or even the threat of child crime[6]. In this regard, only 39% of French people, and more generally Europeans as well considered in 2024 that the digital rights and principles of the European Union (EU) were well applied in their own States to ensure *"safe digital environment*

[1] See for France Bousquet-Bérard C. and Pascal A. for the presidency of the French Republic, *Children and screens In search of lost time* ("*Enfants et écrans À la recherche du temps perdu"),* April 2024, and more generally for the EU, Lobe B. *et al., How children (10-18) experienced online risks during the Covid-19 lockdown*, Spring 2020, EUR 30584 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29762-8, doi:10.2760/066196, JRC124034.

[2] Study carried out by Toluna - Harris Interactive for the Association e-Enfance/3018, with the support of Google, Quantitative survey carried out online from February 6 to 14, 2023.

[3] ARCOM, *Visitation of "adult" sites by minors ("La fréquentation des sites adultes par les mineurs"*), Mai 2023, p. 17.

[4] Génération Numérique, *Survey on the digital practices of 11- to 18-year-olds ("Enquête sur les pratiques numériques des 11 à 18 ans"),* January 2024.

[5] Génération Numérique, *Survey on shocking content accessible to minors ("Enquête sur les contenus choquants accessibles aux mineurs"),* January 2024.

[6] Which can be classified into different categories (e.g. aggressive, sexual, values or commercial) via different analysis grids such as those detailed in Livingstone S. and Stoilova M., *The 4Cs: Classifying Online Risk to Children*, (CO:RE Short Report Series on Key Topics), Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence, 2021). Also see for more details on risks Forbrukerrådet, *COMMERCIAL EXPLOITATION OF CHILDREN AND ADOLESCENTS ONLINE - How to ensure a rights-respecting digital childhood*, November 2024, p.12-25.

and content for children and young people"[7]. The insufficient protection of minors on online platforms is therefore among the most pressing concerns for 38% of French people and 33% of Europeans[8].

The protection of minors on the internet is mandated across several legal systems. At the European Union level, the principle of the "best interests of the child," enshrined in the 2000 "*Charter of Fundamental Rights"*[9], applies equally within the digital environment[10]. Other initiatives more explicitly mention the issues related to minors' exposure to digital risks, such as the 2012 "*European Strategy for a Better Internet for Children"*[11], updated in 2022 under the name "*European strategy for a better internet for kids" (BIK+)*[12]. The 2021 "*EU strategy on the rights of the child"*[13] and the *"European Declaration on Digital Rights and Principles for the Digital Decade"*[14] also acknowledge the specific challenges posed by the digital presence of minors, including in emerging contexts such as the metaverse[15].

---

[7] European Commission, *Special Eurobarometer 551 on 'the digital decade' 2024 Summary Fieldwork: March-April 2024,* July 2024, QC8.13, p. 42.

[8] *Ibid.*, QC5.T, p. 27.

[9] Charter of Fundamental Rights of the European Union, (2000/C 364/01), art. 24.2.

[10] Livingstone S. *et al.*,*The best interests of the child in the digital environment,* Digital Futures for Children centre, LSE and 5Rights Foundation, 2024.

[11] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - European Strategy for a Better Internet for Children*, COM(2012) 196 final, 2 May 2012.

[12] European Commission, *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 youth: the new European strategy for a better internet for kids (BIK+),* COM/2022/212 final, 11 May 2022.

[13] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU strategy on the rights of the child*, COM/2021/142 final, 24 March 2021.

[14] European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, 26 January 2022, p. 4.

[15] See at the EU level Niestadt M. for the European Parliamentary Research Service, *Protecting children in virtual worlds (the metaverse), PE 762.294, April 2024,* more generally on the topic of metavers De Cicco D., Downes J., Helleputte C., *No Children in the Metaverse? The Privacy and Safety Risks of Virtual Worlds (and How to Deal with Them)*, in: Rannenberg K., Drogkaris P., Lauradoux C. (eds) Privacy Technologies and Policy. APF 2023. Lecture Notes in Computer Science, vol 13888. Springer, Cham, 2024.

While many Council of Europe texts also apply to the protection of minors online[16], one of them, from 2007, explicitly aims at the "*Protection of Children against Sexual Exploitation and Sexual Abuse*"[17]. The *"best interests of the child"* are also mentioned in the 2018 Council guidelines on children's rights in the digital environment[18]. Other texts exist at the international level. Although the 1989 United States "*Convention on the Rights of the Child"*[19] also mentions the general notion of "*best interests of the child*"[20], it is the 2021 "G*eneral comment no. 25"*[21] that specifies the application of this convention in the context of the digital environment[22]. The *Organisation for Economic Cooperation and Development (OECD)* can also be mentioned, as it addresses certain aspects of minors' exposure to the digital world[23].

[16] O'Reilly J. for the Council of Europe, *The protection of children against online violence,* Rapport | Doc. 15954 | 27 March 2024, pt. 35-37.

[17] Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,* (CETS no. 201), Lanzarote, 25 october 2007.

[18] Council of Europe, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States*, 4 July 2018, pt. 2.1.

[19] United Nations, *Convention on the Rights of the Child*, New York, 20 November 1989.

[20] *Ibid.,* art. 3.1.

[21] United Nations*, General comment no. 25 (2021) on children's rights in relation to the digital environment,* 2 March 2021.

[22] Although other United Nations' texts can be mentioned such as the *optional protocol on the sale of children, child prostitution and child pornography,* 25 May 2000, or the *optional protocol on a communications procedure*, 19 December 2011.

[23] See OECD, *Declaration on a Trusted, Sustainable and Inclusive Digital Future,* OECD/LEGAL/0488, 15 December 2022, "*WE ARE COMMITTED"* pt. 8-9.

The issue of minor protection is addressed across various regions, including Africa[24], Asia[25], Canada[26], EU[27], Latin America[28], the United States[29]. It is thus unsurprising that numerous laws regarding the protection of minors online have emerged globally. Many of these laws require determining whether an online service user is an adult or a minor. In this context, different "age verification scenarios" arise, referring to distinct use cases based on the type of service or its provider, where legislators mention age verification for users.

France provides an insightful case study illustrating the diversity of these scenarios. Its recent regulatory efforts highlight this variety, including through the 2023 law aimed at *"establishing a digital majority and fighting against online hatred*" (mentioned as the "*digital majority law*" hereafter)[30] and the 2024 law "*securing and regulating the digital space"* (*visant à Sécuriser et à Réguler l'Espace Numérique - SREN*)[31]. These laws contain provisions addressing specific age verification requirements, respectively concerning access to social networks and access to pornographic content.

---

[24] Tsebee D, Boshe P. and Oloyede R, *Child online protection in Africa : Safeguarding youth in the digital age,* blog article on the Privacy Lens Africa website, 20 November 2024, https://privacylens.africa/2024/11/20/child-online-protection-in-africa-safeguarding-youth-in-the-digital-age/ , accessed 1 December 2024.

[25] See Rahamathulla M., *Cyber Safety of Children in the Association of Southeast Asian Nations Region: a Critical Review of Legal Frameworks and Policy Implications*, in: Journal on Child Malt. 4, p 375-400, 2021.

[26] Jolicoeur M.-P., *Checking the age of Internet users on pornographic sites to limit access to minors: an innovative and necessary measure for Canadian law ("Vérifier l'âge des internautes sur les sites pornographiques pour en limiter l'accès aux personnes mineures : une mesure novatrice et nécessaire pour le droit canadien"), in:* Zannou L. R., Gaumond E. and et Lang M. (dir.), Meetings. Crossed views on justice (Rencontres. Regards croisés sur la justice), Lex Electronica, 28-2, p. 79-121, 2023.

[27] European Commission: Directorate-General for Communications Networks, Content and Technology, *New Better Internet for Kids Strategy (BIK+) - Compendium of EU formal texts concerning children in the digital world - 2024 edition*, Publications Office of the European Union, 2024.

[28] Dos Santos Lemos Fernandes S., *Protecting Children from Cybercrime: Legislative Responses in Latin America to Fight Child Pornography*, Online *Grooming, and Cyberbullying through Information and Communication Technologies,* World Bank, Washington, DC, 2015.

[29] See the *US state age assurance laws for social media* page on the Age Verification Providers Association (AVPA) website https://avpassociation.com/us-state-age-assurance-laws-for-social-media/ , accessed 1 December 2024.

[30] France, LAW no. 2023-566 of July 7, 2023 aimed at establishing a digital majority and fighting against online hate *("visant à instaurer une majorité numérique et à lutter contre la haine en ligne").*

[31] France, LAW no. 2024-449 of May 21, 2024 aimed at securing and regulating the digital space *("visant à sécuriser et à réguler l'espace numérique").*

In addition to these frameworks, France has regulations governing access to alcoholic beverages, tobacco products, and even online gaming sites. At the EU level, similar regulatory efforts complement and influence these national frameworks. Several age verification scenarios, comparable to those established in France, are gradually being regulated by the EU. One example is the 2018 revision of the Audiovisual Media Services Directive (AVMSD)[32] concerning minors' access to inappropriate content, in relation to the measures of the French framework on access to pornography. Another example is the 2022 Digital Services Act (DSA)[33], which regulates intermediary service providers and is related to France's framework on access to social networks, though France aims[34] to export its *"digital majority at 15*" within the EU. Older frameworks, such as the 2016 General Data Protection Regulation (GDPR)[35] and the 2022 proposal of a Child Sexual Abuse Regulation (CSAR)[36], also incorporate age verification measures. The interrelationship between age verification provisions in French and European frameworks raises important questions about potential synergies and the risk of regulatory conflict.

The pursuit of global coherence becomes even more critical when examining "age verification systems,"[37] specifically the procedures to be established for conducting the verification. Legislation that mandates or suggests online services verify users' ages is typically not very specific about the exact methods

[32] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. Sometimes also referred to as *AMSD.*

[33] 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 Act).

[34] President of the French Republic Macron E., *Speech on Europe*, Sorbonne University, 25 April 2024.

[35] 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).

[36] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final, 11 May 2022.

[37] The implementation of which is recommended by the United Nations' General comment no. 25, (2021), *op. cit.*, §114.

that should be used for this verification. Some age verification scenarios are simply not implemented, while others rely on *"circumventable and intrusive"*[38] systems. However, the situation appears to be evolving, as demonstrated by the framework of the Regulatory Authority for Audiovisual and Digital Communication (*Autorité de Régulation de la Communication audiovisuelle et numérique - ARCOM*)[39], from October 2024, on "*age verification systems set up for access to [...] pornographic content [...]"*[40] (mentioned as the "*ARCOM framework on access to pornography",* hereafter). This framework aims to clarify the minimum technical requirements for the systems that should be established in this area.

A comparable dynamic is emerging at the EU level with regard to the application of the DSA, which opens the door to discussions on the possibility of a "*European technical solution*"[41]. The emergence of such a common age verification system raises questions both about its feasibility and its ability to apply to other age verification scenarios beyond the DSA. However, alongside concerns about the protection of minors, the EU is planning, through the 2024 eIDAS 2.0 regulation[42], to offer its citizens the possibility of using *EU Digital Identity Wallets (EDIW).* This *EDIW* would notably allow users to verify their identity in order to access online services. The capacity of this infrastructure to certify the age of its users, and its interoperability at the EU level, could therefore also position it as a strong candidate in this quest for a common system to address the issue of online age verification at the EU level.

---

[38] CNIL, *Online age verification: balancing privacy and the protection of minors* web page*, 22 September 2022,* https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors , accessed 1 December 2024.

[39] The ARCOM, created in 2022, has taken over the missions of the Supreme Audiovisual Council (Conseil supérieur de l'audiovisuel - CSA). ARCOM will sometimes be mentioned hereafter even though CSA it is the one cited in the legislation prior to 2022.

[40] ARCOM, *Framework setting out the minimum technical requirements for age verification systems set up for access to certain online public communication services and video-sharing platforms that make pornographic content available to the public*, October 2024.

[41] European Commission's Commissioner for Internal Market, Breton T., *Detailed opinion in response to Notification 2023/461/FR,* (7417 final), 25 October 2023, p. 5.

[42] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. eIDAS means "*electronic identification, authentication, and trust services".*

This study seeks to navigate the regulatory complexities surrounding online age verification in France and at the EU level, aiming to identify elements that could contribute to more consistent and harmonized measures in the future. Currently, the various age verification scenarios and their associated systems appear fragmented in their implementation, resulting in potential challenges when they interact with one another.

To this end, the present study begins by examining the diversity of online age verification scenarios in France and at the EU level. For each scenario, it will investigate whether there are specific details regarding the systems to be implemented, as well as the general or specific objectives they aim to achieve. It will then be shown that the majority of these verification scenarios are established by legislators to address issues that are often similar across different contexts. Additionally, it will be established that the verification systems themselves could pose risks to users (part I). This observation, combined with the lack of clarity in legislation regarding the age verification systems to be implemented, will lead to an exploration of what might constitute the future of age verification systems, potentially offering a point of convergence for all such scenarios. The study will then propose theoretical frameworks for classifying age verification systems, which could potentially allow for their ranking. By way of illustration, the EU's digital identity framework, and its application in France, will be analyzed, particularly in relation to online age verification. The recent update of this framework at the EU level will culminate in an assessment of the potential for the EDIW to serve as a future European online age verification system (part II).

PART I: COMPARATIVE ANALYSIS OF FRENCH AND EU AGE VERIFICATION SCENARIOS: IDENTIFYING OVERLAPS

The aim of this section is to shed light on the different scenarios in which age verification may be required online, while highlighting significant gaps in their implementation and effectiveness. Indeed, certain age verification scenarios present notable shortcomings. The frequent lack of details regarding the verification systems to be implemented, among other things, and a complex distribution of prerogatives between France and the EU on this matter can explain these gaps.

To illustrate this, we will first examine four age verification scenarios outlined in French legislation (chap. 1), followed by an analysis of four additional scenarios defined by EU legislation (chap. 2).

Chapter 1: Analysis of Age Verification Scenarios in French Legislation

France adopts a proactive approach to online age verification, with four key verification scenarios being regulated over several years. Since it is not feasible to examine these scenarios in strict chronological order, they will be categorized based on their most recent "substantial" modification, from the most established to the most recent. The analysis will cover age verification scenarios for access to: alcoholic beverages and tobacco products remotely (I), online gambling and betting (II), social networks (III) and finally online pornographic content (IV).

I - Remote Access to Alcoholic Beverages and Tobacco Products

A. Legal Framework

1) Legal provisions calling for a verification

Offering for free or selling alcoholic beverages and tobacco products to minors is subject to the same types of prohibitions in France. The historical

formulations of these access scenarios, respectively "*in drinking establishments and all shops or public places*"[43] and "*in tobacco shops and all shops or public places*"[44], allow the inclusion of remote sale of these products. Some elements have nevertheless evolved in recent decades in order to adapt the legal framework to the needs of the time. First, the minimum age to legally have access to these products, initially set at 16, was raised to 18 in 2009[45]. A second element specifically concerns tobacco products, with the emergence of vaping products. Access to these was first regulated in 2014 under the same provisions as tobacco products[46]. Each type of products has its own article since 2016[47] but the two regimes remain almost identical. Additionally, in 2016, a specificity was introduced regarding alcoholic beverages: it is prohibited to offer or sell to minors "*object directly inciting excessive alcohol consumption*"[48]. A decree specifies that it concerns *"games, clothing, fashion accessories, decorative elements, utensils and accessories for electronic devices whose presentation, logo, name or slogan directly encourage excessive consumption of alcohol*"[49].

---

[43] "*Dans les débits de boissons et tous commerces ou lieux publics",* wording of part of art. L3342-1 of the French Public Health Code in its version from 22 June 2000 to 23 July 2009, which is reused in its current version for the free offer, and generalized for sale by the wording "*the sale of alcoholic beverages to minors is prohibited*" (*"la vente des boissons alcooliques à des mineurs est interdite")*.

[44] "*Dans les débits de tabac et tous commerces ou lieux publics",* wording of part of art. 3511-2-1 of the French Public Health Code in its version from 25 May 2006 to 23 July 2009, which is unchanged in the article mentioned below governing this prohibition nowadays.

[45] By French LAW no. 2009-879 of July 21, 2009 relating to hospital reform and relating to patients, health and territories ("*portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires"), via its articles* 93 for alcoholic beverages and 98 for tobacco products. It is interesting to point out that the age threshold on these topics differs between EU Member States. See the age mapping on the European Union Agency for Fundamental Rights website for alcoholic beverages https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/purchasing-and-consuming-alcohol , and for tobacco products https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/purchasing-and-consuming-tobacco , both accessed 1 December 2024.

[46] French Public Health Code, art. L3511-2-1 as amended first by LAW no. 2014-344 of 17 March 2014 relating to consumption ("*relative à la consommation"*), art. 36, then LAW no. 2016-41 of 26 January 2016 on the modernization of our health system ("*de modernisation de notre système de santé"*), art. 24.

[47] Via the French ordinance no 2016-623 of 19 May 2016, art. 1 repealing art. L3511-2-1 of the French Public Health Code to replace it with an article L3512-12 dealing with tobacco products, and an article L3513-5 for vaping products.

[48] French Public Health Code, art. L3342-1 as amended by LAW no. 2016-41, *op. cit.*, art. 12.

[49] French Public Health Code, art. R3342-1 created by decree no. 2016-1329 of 6 October 2016 determining objects directly inciting excessive consumption of alcohol and the sale or offering of which is

It can also be observed that in France, advertising for these products has also been regulated since the 1991 "Evin" law[50]. The legal framework as it has evolved to date prohibits online advertising of tobacco[51] and vaping[52] products. The situation is different regarding alcohol, for which advertising is limited to certain media listed exhaustively by law[53], including, since 2009[54], online communications services "*excluding those which, by their character, presentation or purpose, appear to be primarily aimed at young people* ". However, the law does not impose any age verification in this respect.

2) Specifications about the age verification system to implement

The age verification procedures have undergone some reformulations. Early versions of articles cited above[55] remain silent on this point. In 2009, the ban on access to alcoholic beverages took a first step. It provides that "*the person delivering the drink may require the customer to provide proof of majority*"[56]. This flexible formulation was hardened in 2016 with the more restrictive formulation *"the person delivering the drink requires the customer to provide proof of majority"*[57], then also used for tobacco and vaping products[58].

---

prohibited to minors (*"déterminant les objets incitant directement à la consommation excessive d'alcool et dont la vente ou l'offre est interdite aux mineurs"*), art. 1.

[50] France, LAW no. 91-32 of 10 January 1991 on the fight against smoking and alcoholism *("relative à la lutte contre le tabagisme et l'alcoolisme").*

[51] French Public Health Code, art. L3512-4, providing for exceptions that do not, in principle, expose minors to online risks.

[52] French Public Health Code, art. L3513-4, providing for exceptions that do not, in principle, expose minors to online risks.

[53] French Public Health Code, art. L3323-2.

[54] France, LAW no. 2009-879, *op. cit.*, art. 97.

[55] French Public Health Code, art. L3342-1 in its version from 22 June 2000 to 23 July 2009 with regard to alcoholic beverages, and art. L3511-2-1 in its version from 25 May 2006 to 28 January 2016 with regard to tobacco and vaping products.

[56] French Public Health Code, art. L3342-1 as amended by LAW no. 2009-879, *op. cit.*, art. 93.

[57] French Public Health Code, art. L3342-1 as amended by LAW no. 2016-41, *op. cit.*, art. 12.

[58] French Public Health Code, art. L3511-2-1 as amended by LAW no. 2016-41, *op. cit.*, art. 24, and today included in the respective articles dealing with each of these products.

The verification system is not further specified. Worse still, concerning access to alcoholic beverages, there is even a lack of accountability, unchanged since 2000, for the person providing access to the product, if they can "*prove that they were misled about the age of the minor*"[59]. This legal framework of the sale of alcoholic beverages, tobacco products or vaping has not been specifically adapted to remote selling. This results in a purely theoretical application of the verification obligation. The sale of vaping products is, in fact, freely accessible for online purchase: most of the time, no verification of the buyer's age is ever carried out. The same observation can be made regarding the purchase of alcohol online. At best, a self-declaration of being of age has to be made by the buyer. It is generally not verified, even in the cases of home delivery of meals or Click & Collect shopping.

B. Issues and Challenges at Stake

The risks associated with regulating minors' access to alcoholic beverages, tobacco, and vaping products are clearly identifiable and are primarily health-related. Alcohol consumption poses immediate risks to minors' health and safety, as well as long-term risks of dependence. In contrast, the use of tobacco products often leads to dependence from the first use, with long-term detrimental effects on health. While these health risks are not exclusive to minors, their ongoing physical and cognitive development makes them particularly vulnerable to such harms.

The legal framework governing access to these products remains insufficiently adapted to the specific context of remote access. In the absence of detailed legislative guidance on the age verification systems to be implemented, the existing regime is relatively ineffective. At best, it creates a false sense of security rather than ensuring meaningful protection[60].

---

[59] French Public Health Code, art. L3353-5.

[60] European Digital Rights (EDRi), *Position Paper: Age verification can't 'childproof' the internet,* 4 October 2023, pt. 4.6, p. 29.

II - Access to Online Gambling and Betting

A. Legal Framework

1) Legal provisions calling for a verification

The explicit ban on access to gambling for individuals under 18 results from article L320-8 of the French Internal Security Code. It contains a general ban on selling or offering for free gambling games to minors[61]. The article goes further on several matters. On the one hand, it establishes an obligation to verify the identity and date of birth of users when they directly access the betting service through gaming terminals, without human intermediation[62]. On the other hand, it provides a general obligation for the gambling operators to adopt proactive measures in order to prevent a minor from participating in the games they offer[63].

The emergence in recent years of certain economic models in the video game sector has raised the question of broadening the legal regime regarding online betting. The mechanism of "*loot boxes*" is one example. It is a kind of treasure or surprise bag, opened by the player to receive a random reward that can be used within the game, such as in-game money, new outfits or new objects for his character. These loot boxes can sometimes be obtained by the player when completing certain in-game or game-related tasks. But they usually can also be directly purchased by the player with in-game currency, and/or real money. A useful parallel can be drawn with online betting games, where the potential reward may be either relatively insignificant, resulting in a net loss for the player who has paid to participate, or highly valuable, in which case it could be resold to another player for real money. As far back as 2017, the French association "*UFC que Choisir*" denounced this practice, as it was then very common among

[61] French Internal Security Code, art. L320-8, para. 2.

[62] French Internal Security Code, art. L320-8, para. 4.

[63] French Internal Security Code, art. L320-8, para. 1.

a young audience[64]. Other models have emerged with the growing mainstream use of blockchain technology[65]. Video games called "*PlayTo Earn*", for example, also offer their players the opportunity to receive rewards, but in the form of non-fungible tokens or crypto assets. In this context, the SREN law has just established a three-year experimental regime aimed at authorizing "*games with monetizable digital objects" ("Jeux à Objets Numériques Monétisables - JONUM)*[66]. Among the measures governing entities offering these games, there is an obligation to use an age verification system[67], which is not, however, specified in the law.

2) Specifications about the age verification system to implement

Given that the regulation of games incorporating monetizable digital objects remains at a preliminary stage, it is currently too early to evaluate its implementation, which will notably depend on the issuance of a regulatory decree.[68] At present, the broader regulatory framework governing online betting platforms, pursuant to Article L. 320-8 of the French Internal Security Code, appears to be more firmly established. The law has specified the verification system to be implemented in this context. Upon the creation of an online account, the user must provide identifying information, including their date of birth.[69] The procedure is not only declarative, since the identity of the user must be verified, either through the use of a certified means of electronic

---

[64] UFC que Choisir, "*Paid content in video games - Winning games, naughty games ("Contenus payants dans les jeux vidéo - Jeux de gains, jeux de vilains") webpage,* 22 Novembrer 2017, https://www.quechoisir.org/action-ufc-que-choisir-contenus-payants-dans-les-jeux-video-jeux-de-gains-jeux-de-vilains-n48636/ , accessed 1 December 2024.

[65] Term used for the sake of simplicity, even though the discussion is in fact more generally applicable to the Distributed Ledger Technologies (DLT).

[66] SREN law (2024), *op. cit.*, art. 40 and 41.

[67] *Ibid.,* art. 41.II.

[68] *Ibid.,* art. 41.III.

[69] France, Decree no. 2010-518 of 19 May 2010 relating to the offer of games and bets from gaming operators and the provision of gaming data to the National Gaming Authority ("*relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux"),* art. 2.1.

identification[70], or by the provision of a document provided by the user proving their identity[71]. In this second hypothesis, the user's address must then be verified by providing a document proving their place of residence. They will then receive a code at the declared address, which allows them to activate their account.

B. Issues and Challenges at Stake

1) Especially for minors

The regulation of access to online gambling raises issues that are comparable to those arising from prohibitions on the sale of alcohol, tobacco, or vaping products. In the short term, however, the nature of the protected interest differs: the objective is not to safeguard the minor's physical integrity, but rather to protect their financial interests, or, more often in practice, those of their parents. In the long term, the two scenarios tend to intertwine, both aiming to limit the minor's risks of addiction, which is a public health concern. This second concern invites us to focus on a particularity of the access to online betting sites. In France, the regulation of the access to online gambling is not designed with the sole aim of only protecting minors, but also the interests of all users in a wider effort. Verification not only of age, but more generally of identity, is supplemented by mechanisms aimed at protecting users with "*excessive or pathological*"[72] gambling behaviors. However, the number of adults recognized as having such behavior or more generally of minors who still manage to have access to online betting sites[73] also raises the question of the effectiveness of such a regime and its resulting illusion of security.

---

[70] France, Decree no. 2010-518, *op. cit.,* art. 4.I, referring to the French Monetary and Financial Code, art. R561-5-1, 1° and 2° (which will be detailed in part II, chap. 1, I, B, 2) and part II, chap 2, I, C of this study).

[71] Documents listed exhaustively in Decree no. 2010-518, *op. cit.,* art. 4.II.

[72] An entire chapter (chap. III) is provided for in this regard in Decree no. 2010-518, *op. cit.* Furthermore, the SREN law, (2024), *op. cit.,* art. 41.XI also mentions self-exclusion mechanisms and self-limiting mechanisms with regard to JONUM.

[73] 34.8% of teenagers aged 15 to 17 have gambled at least once in 2021 in France. Among them, 21.9% can be characterised as excessive gamblers and 12.9% as moderate-risk gamblers. Figures taken from Tovar M.-L. and Costes J.-M. for the Society for mutual aid and psychological action *("Société d'entraide et d'action psychologique"), Practices of betting and gambling by minors in 2021 ("pratique des jeux d'argent et de hasard des mineurs en 2021"), zoom recherches n°4*, February 2022.

2) Broader concerns

In the same way that the banking and financial sector is subject to anti-money laundering and combating the financing of terrorism (AML/CFT) obligations, the implementation of user identity verification on online betting sites allows more effective monitoring of possible misuse of the initial purpose of these services. This link, explained in the law[74], is all the more noticeable as the legislator directly refers to the verification systems provided for in the Monetary and Financial Code, initially designed for remote customer onboarding in the banking and financial field in response to AML/CFT concerns. Beyond these concerns, the legitimate financial gain by players, including that obtained via video games, could be a scenario of interest to the State from a tax perspective. Thus, the recent authorization regime for games with monetizable digital objects could also have been driven by the desire to track and tax players' winnings more efficiently. An age verification scenario may thus constitute only one of the components of a given legal framework, in which case other considerations must then be taken into account.

III - Access to Social Networks

A. Legal Framework

1) Legal provisions calling for a verification

Access to social networks for minors is now regulated by the 2023 "*digital majority*"[75]. This law introduces[76] a new article in the law for confidence in the digital economy (*Loi pour la Confiance dans l'Économie Numérique - LCEN*)[77],

---

[74] France, Decree no. 2010-518, *op. cit.,* art. 9 and 15.

[75] France, LAW no. 2023-566, *op. cit.*, although the use of the term *"digital majority"* for this legal framework is questionable in that it covers a specific situation in the digital universe. See on this point Petelin T.*, The digital majority in question: commentary on the law of 7 July 2023 aimed at establishing a digital majority and combating online hate' ("La majorité numérique en question : commentaire de la loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne"),* Dalloz IP/IT no 12, 2023 p. 667.

[76] France, LAW no. 2023-566, *op. cit.*, art. 4.

[77] France, LAW no. 2004-575 of 21 June 2004 for confidence in the digital economy (*"pour la confiance dans l'économie numérique"*), introduction of an art. 6-7.

and therefore requires social media service providers, to deny the registration of minors for their services. Two clarifications should be made. First, this "digital majority" is set at 15 years old, and not 18 years old as is the case with the age verification in the two preceding scenarios. This legal framework is therefore more in line with the spirit of the majority to consent to the processing of personal data, which will subsequently be studied in the next chapter through the EU framework in this matter[78]. Secondly, the legislator still provides for the possibility for minors under 15 years old to register on social networks, but only with the express authorization of their legal representatives[79]. The legal framework established is, here too, close to principles theoretically established in the field of data protection.

2) Specifications about the age verification system to implement

This legal framework assigns to the ARCOM, after consultation with the French National Commission for Information Technology and Civil Liberties (*Commission nationale de l'informatique et des libertés - CNIL*)[80], the responsibility for developing a technical framework, specifying the methods for verifying users' ages. There is even a sanction mechanism planned against social network service providers that have not implemented this framework[81]. This framework, and more generally the implementing decree[82] for this verification obligation, however, never emerged. Issues of procedure and distribution of prerogatives between the EU and its Member States can explain this situation. As it carried out a 2015 directive providing for an information procedure for technical regulations linked to information society services[83],

---

[78] See part I, chap. 2, I of this study.

[79] The law refers more precisely to the authorization of the "*holders of parental authority over the mino*r" *("titulaires de l'autorité parentale sur le mineur")*, but for the sake of clarity, the notion of *"legal representatives"* will be used generally hereafter for the age verification situations involving this type of concept.

[80] Which is the French supervisory authority with regard to GDPR, art. 51.

[81] France, LAW no. 2004-575, op. cit., art. 6-7 II.

[82] *Ibid.* art. 6-7 IV.

[83] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society service.

France should have obtained the approval of the European Commission[84] before the promulgation of the digital majority law[85]. However, not only was this approval requested after the promulgation of the law, but the European Commission's opinion is unequivocal on the substance[86]. The digital majority law not only constitutes an unjustified restriction on the freedom to provide information society services on French territory, in violation of the *eCommerce* (electronic commerce) *Directive* of 2000[87], but also violates the application of the DSA[88], which will be studied later[89]. The European Commission also suggests in its opinion that French law should further be examined in light of the AVMSD[90], which will also be detailed later in this study[91]. As a result, the French legal framework for age verification to access social networks is, although adopted, not applicable because it encroaches on EU prerogatives and regulations. Online age verification in the context of social networks is currently, however, undergoing other developments through the application of the DSA, but also due to the policies of the dominant industry players in this area[92].

---

[84] By notifying the European Commission of the draft technical rule, which must then give a detailed opinion on the conformity or not of the national rule with regard to EU law. (See *ibid.,* art. 6). The aim of such a procedure is in particular to ensure that Member States do not fragment the EU internal market.

[85] Even though article 7 of this law ensures that the other measures of this law can enter into force only after the publication of a decree (that the French legislator wished to publish after having received a favourable Commission's detailed opinion, which in the end was never obtained).

[86] European Commission's Commissioner for Internal Market, Breton T., *Detailed opinion in response to Notification* 2023/237/FR and 2023/362/FR, (Ares(2023)5596'438), 14 August 2023.

[87] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), and more particularly art. 3.

[88] DSA, (2022), *op cit.*

[89] Part I, chap. 2, III of this study.

[90] AVMSD, (2018), *op. cit.*

[91] As it will be detailed in part I, chap. 2, III of this study.

[92] Meta's Global Head of Safety, Davis A., web page *Europe Can Make Parenting in a Digital World Easier,* 25 November 2024, https://about.fb.com/news/2024/11/europe-can-make-parenting-in-a-digital-world-easier/ , accessed 1 December 2024.

B. Issues and Challenges at Stake

1) Especially for minors

Challenges comparable to those of the first two age verification scenarios in this chapter can be identified. This includes protecting the interests of young people in the short term, particularly in terms of online cyber harassment or more generally regarding exposure to inappropriate content. In the longer term, it is also about partially preventing the risks of addiction, or the undesirable effects recognized in terms of social anxiety or depression[93], once again addressing public health considerations.

As presented above, this scenario of age verification to access social networks does not only involve minors. The parental authorization mechanism is made up of several sub-elements designed to involve the child's legal representatives. For example, one measure allows legal representatives to “suspend” the child’s account instead of deleting it. Yet another requires online social media providers to activate a device, enabling legal representatives to control how long the child uses the networks[94]. Although these measures limiting the harmful effects of social networks are laudable, if they were applicable, they could also limit the potential “beneficial” effects of such networks. In situations of child abuse, or when the sexual orientation of a child is not accepted by their legal representatives, for example, social networks can sometimes represent a space where minors can find support[95]. Conditioning their access to the authorization

[93] Boniel-Nissim M. et *al., International perspectives on social media use among adolescents: Implications for mental and social well-being and substance use,* in: Computers in Human Behavior 129(1), December 2021.

[94] Law no. 2004-575, *op. cit.,* art. 6-7.

[95] See Hubert M.,*Social networks and LGBT concerns* (“Les réseaux sociaux face aux questions LGBT”) blog article on Alliance arc-en-ciel website, 25 mars 2017, https://arcencielquebec.ca/2017/03/25/les-reseaux-sociaux-face-aux-questions-lgbt/ , accessed on 1 December 2024, which also highlights the positive aspects of social networks, and *Government launches national campaign to raise awareness of helplines for child victims of violence (“Le Gouvernement lance une campagne nationale de sensibilisation aux numéros d’aide pour les enfants victimes de violences”)* webpage, 03 october 2022, https://solidarites.gouv.fr/le-gouvernement-lance-une-campagne-nationale-de-sensibilisation-aux-numeros-daide-pour-les-enfants , accessed on 1 December 2024, where the French government used social networks to spread its campaign.

of their legal representatives could then exclude certain children, or even certain categories of children, and more generally infringe upon their privacy[96].

2) Broader concerns

The question of anonymity also has to be explored as it regularly preoccupies French deputies[97]. A verification of minors' age on social networks, and possibly of their identity as well as their legal representatives', implies effectively a verification for all users, even adults who successfully pass the verification. Just as with age verification to access betting sites, a strong link appears here with more general identity verification. Risks then emerge in terms of personal data protection[98]. The possibility of complete anonymity on social networks is already quite relative[99]. But the legal framework established by the SREN law already includes repressive measures, some of which may take the form of suspension of accounts, including those of minors[100]. Thus, wouldn't the establishment of such an infrastructure capable of easily linking an account to an identity be an invitation to adopt, within a few years, a law that would truly put an end to

---

[96] Debates took place in France following the positions taken by certain politicians calling for maximum surveillance by parents over their children. See notably, La Voix Du Nord, *No privacy for teenagers, we have to ''look into their phones'': Sabrina Agresti-Roubache shocks ("La vie privée des ados, c'est « non », il faut « fouiller leurs téléphones » : Sabrina Agresti-Roubache choque"),* 23 April 2024, https://www.lavoixdunord.fr/1455216/article/2024-04-23/la-vie-privee-des-ados-c-est-non-il-faut-fouiller-leurs-telephones-sabrina , accessed on 1 December 2024.

[97] The French parliamentary debates in this regard being recurring, see notably the proposed law n° 1776 (15th legislature) aimed at forcing users of social networks to register under their real identity *("visant à obliger les utilisateurs des réseaux sociaux à s'y inscrire sous leur identité réelle")* of 20 March 2019, but not adopted. Or proposed amendment no. 373 aiming to commission a report from the Government on the feasibility and consequences of lifting anonymity on social networks, of 13 January 2021 but rejected. Also see on this topic, Ancona L., *Should we put an end to anonymity on social* networks?'("*Faut-il mettre fin à l'anonymat sur les réseaux sociaux ?"),* April 2023.

[98] CNIL, *Thematic file - Digital identity ("Dossier thématique - L'identité numérique"),* February 2023, notably p. 10-11.

[99] See the written question no. 1564 (16th Parliament) of the deputy of the French national assembly, Ardouin J.-P., *Social networks: lifting anonymity and cooperation with the authorities (Réseaux sociaux : levée de l'anonymat et coopération avec les autorités,* 27 September 2022. Also see, Lee E. and Huet B., *Paradoxical immunity for anonymous authors of defamatory content ("L'immunité paradoxale offerte aux auteurs anonymes de contenus diffamatoires"),* Légipresse, 26 July 2024.

[100] See in this sense Léger P., *The additional penalty of suspension of access accounts to online services: symbol of measures to secure the digital space and the difficulties of their implementation ("La peine complémentaire de suspension des comptes d'accès à des services en ligne : symbole des mesures de sécurisation de l'espace numérique et des difficultés de leur mise en œuvre"),* Dalloz IP/IT, July 2024, p.395

anonymity on social networks? Whistleblowers, journalists or more generally citizens could then see their freedom of speech drastically reduced. Likewise, will justice and public authorities not be tempted to use this infrastructure? The already existing possibility for the French tax administration to use evidence from social networks during its investigations[101] makes it easy to imagine a possible misuse of the infrastructure, initially designed to protect minors, for repressive purposes.

IV - Access to Online Pornographic Content

A. Legal Framework

1) Legal provisions calling for a verification

The exposure of minors under 18 years old to online pornography is a problem addressed by article 227-24 of the French Penal Code. This provision also covers the exposure of minors to other types of content: such as those displaying a certain degree of violence, inciting terrorism or seriously harming human dignity, or inciting minors to engage in games that would put them physically in danger. The ban on such exhibition, extended since 2007[102] to content accessible online, is punishable by three years' imprisonment and a fine of 75,000 euros. It should be noted that the constitution of the offense is not conditioned to the actual consumption of the disputed content by a minor. The content only has *"to be likely seen or perceived by a minor".*

ARCOM[103] is designated to ensure compliance with this article with regard to pornographic content. This authority can send formal notices to online public communication services that enable minors to have access to such content. Until recently, if these services did not put an end to this access, ARCOM could

[101] France, LAW No 2019-1479 of 28 December 2019 on finance for 2020 art. 154 as amended by LAW No 2023-1322 of 29 December 2023 on finance for 2024 art. 112.

[102] France, LAW no. 2007-297 of 5 March 2007 relating to the prevention of delinquency ("relative à la prévention de la délinquance"), art. 35.

[103] The CSA in the law.

refer the matter to the president of the Paris judicial court[104] to put an end to the access to the concerned services. This mechanism, used by the authority[105], was replaced by the SREN law with a new one that grants greater powers to ARCOM. The authority can now directly initiate a financial penalty, after having consulted the CNIL[106]. This framework, however, suffers from a limitation. As for the accessibility to social networks, France's regulatory activity in terms of access to pornographic content addresses an area also regulated at the EU level. Having learned the lesson of the notification of the digital majority law a year earlier, France notified the SREN law at several points during its negotiation before its vote[107]. In order not to encroach on the prerogatives of the EU, France decided to limit the scope of its legal framework on access to pornographic content to operators established in France or outside the EU, but not to those established in other EU Member States[108].

2) Specifications about the age verification system to implement

In 2020, a paragraph[109] was added to the aforementioned article 227-24 of the French Penal Code. This paragraph is the opposite of the scenario of alcohol sale in France, since it specifies that a simple declaration made by users of their majority cannot constitute an exemption of liability for the author of the offense. This clarification alone, however, does not give more information on the exact verification process that is expected. Initially, a 2021 decree gave

---

[104] France, LAW no. 2020-936 of 30 July 2020 aimed at protecting victims of domestic violence *("visant à protéger les victimes de violences conjugales*"), art. 23.

[105] CSA, Decisions no. 2021-P-02, 2021-P-03, 2021-P-04, 2021-P-05 and 2021-P-06 of 13 December 2021. Also see ARCOM, press release: *Access of minors to pornographic sites: Referral to the president of the Paris judicial court ("Accès des mineurs aux sites pornographiques : Saisine du président du tribunal judiciaire de Paris"),* 8 March 2022.

[106] SREN law (2024), *op. cit.,* art. 1, amending in particular the article 10 of the LCEN (2004), *op. cit*. For more detail of the two regimes see Huttner L., *Controlling access of minors to pornographic sites ("Le contrôle de l'accès des mineurs aux sites pornographiques"),* Dalloz IP/IT, July 2024, p. 400.

[107] European Commission, *Detailed opinion in response to Notification 2023/461/FR, op. cit.* and European Commission's Commissioner for Internal Market, Breton T., *Detailed opinion in response to Notification 2023/632/FR,* (389 final), 17 January 2024.

[108] SREN law (2024), *op. cit.,* art. 1.I. although it is possible to make sites established in other EU Member States subject to the law via a procedure referred to in art. 2 of the same law, thereby creating an art. 10-2 to the LCEN law (2004), *op. cit.*

[109] LAW n°2020-936*, op. cit.,* art. 22.

ARCOM the possibility of adopting guidelines[110] "*concerning the reliability of technical processes making it possible to ensure that users wishing to access pornographic content from an online public communication service are of legal age*". However, these guidelines were not published.

The SREN law has also reorganized the legal framework on this point. Article 23 of Law no. 2020-936 cited earlier, from which the article authorizing ARCOM to publish guidelines arises, is simply repealed[111]. It is replaced by the aforementioned regime giving more power to the authority in its mission of control and sanction. It also requires the authority to publish the *framework on access to pornography*[112] mentioned in the introduction. ARCOM did not wait for the SREN law to be adopted before working on this framework. A version of it, published for public consultation between April and May 2024[113], was simultaneously notified to the European Commission which did not detect any contentious measures under EU law[114]. Public since October 2024[115], the final version of the framework has only undergone slight changes. The framework therefore has four parts, the first of which contains general considerations relating to the reliability of age verification systems[116]. The second part focuses on the protection of privacy by applying GDPR principles to the framework of online age verification. It also requires entities that must implement an age verification system to use independent third-party service providers. It also

[110] France, Decree no. 2021-1306 of 7 October, 2021 relating to the modalities of implementation of measures aimed at protecting minors against access to sites disseminating pornographic content ("relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique"), art. 3, in application of LAW n°2020-936, *op. cit.*, art. 23.

[111] SREN law (2024), *op. cit.,* art. 2.II.

[112] *Ibid.,* art. 1, amending in particular the article 10 of the LCEN (2004), *op. cit.*

[113] ARCOM, *Public consultation on the draft framework setting out the minimum technical requirements for age verification systems set up for access to online pornographic content ("Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à des contenus pornographiques en ligne")*, 11 April 2024.

[114] European Commission's Commissioner for Communications Networks, Content and Technology, Viola R., *Detailed opinion in response to Notification* 2024/0208/FR, C(2024) 5148 final, 15 July 2024.

[115] ARCOM framework on access to pornography (2024), *op.cit.*

[116] With principles of tightness of age control, of effectiveness of the solution, of limiting the possibilities of circumvention, of verification at each service consultation and of non-discrimination.

requires the implementation of at least one *"double anonymity"* system. These architectures will be detailed in the second part of this study[117]. The different entities mentioned in the framework are subject to various measures such as prohibitions on the reuse of data for purposes other than the age verification initially planned. The framework also contains good practices, a third part specifying the "*alternative proof generation solutions accepted on a temporary basis*" and a *fourth part* mentioning the terms of audit and evaluation of age verification systems.

B. Issues and Challenges at Stake

1) Especially for minors

The analysis of the direct challenges for minors is not an exception, as it once again contains concerns relating to addiction. Being exposed to pornographic content at too young an age involves public health challenges such as a distorted understanding of sexuality and possible inappropriate behaviors it may lead to.

Another risk, already mentioned when discussing other age verification scenarios, could be creating a false sense of security by assuming that the current framework will restrict access to all pornographic sites, while it will not regulate actors from other EU Member States by default. It will also be a question of seeing whether and to what extent ARCOM will be able to effectively monitor and sanction international actors established outside the EU. It will also be useful to verify whether and to what extent this new legal framework will be bypassed by minors or not, for example via the use of a VPN[118] or anonymization tools.

[117] Part II, chap. 1, II, B of this study.

[118] *Virtual Private Network,* which protects its users by encrypting their data and masking their IP (Internet Protocol) addresses. See Kishk Y. A., *State-Based Online*. *Restrictions*: *Age-Verification* And The *VPN*. *Obstacle* In The *Law*," 2 Int'l J. L. Ethics, Technology, 2024.

2) Broader concerns

The French legal framework regarding age verification for access to pornographic content also poses challenges in terms of market competition. Paradoxically, if foreign market leaders could have the means to be compliant by setting up such reliable age verification systems, the cost of such an infrastructure could be proportionately heavier for actors with a mainly national scope. Beyond the cost, the existence of an age verification process for entities subject to it will likely constitute a competitive disadvantage in terms of user experience, compared to sites not subject to it or not applying it. On the other side of the screen, the exact nature of the verification system could also exclude certain categories of users who may not have access to it.

User experience allows us to discuss a final series of risks, also present in verification scenarios in other sections, but even more pronounced in terms of access to pornography. If challenges relating to freedom of expression seem less present concerning this matter, those relating to the protection of personal data and to privacy are, on the contrary, exacerbated given the nature of the regulated scenario[119].

[119] See the illustration of the risks in terms of cybersécurity in part II, chap. 1, II, A, 2) of this study.

Chapter 1 Summary

Verified scenario	Main legal source	Age verified	Application	Details on verification systems
Remote access to certain regulated products	Public Health Code art. L3342-1 for **alcoholic beverages** and objects encouraging alcohol consumption	**18** (16 before 2009)	*Theoretical* (rarely enforced in practice)	**No** (and art. L3353-5 of the Public Health Code providing for a release of responsibility from the person giving access to the disputed product having been misled about the age of the minor)
	Public Health Code art. L3512-12 for **tobacco products**			**No**
	Public Health Code art. L3513-5 for **vaping products**	**18**		
Access to online gambling and betting	Internal Security Code art. L. 320-8 for access to online **gambling and betting**	**18**	**Yes**	**Yes** (through identity document verification and the physical delivery of a code to the user's home, or the use of a certified electronic identification method, by reference to the monetary and financial code art. R. 561-5-1).
	SREN law art. 40 and 41 for games with **monetizable digital objects**		*Upcoming*	*Upcoming* (as indicated by a forthcoming decree under art. 41.III)
Access to social networks	Digital majority law art. 4, introducing an art.6-7 in the LCEN	**15**	**No** (incompatible with EU law))	**No** (**reference to an** ARCOM framework, but not yet published)
Access to pornographic content online	Penal Code art. 227-24 for **content to pornographic, violent or inciting terrorism or of a nature to seriously harm human dignity or to incite minors to engage in games putting them in physical danger**	**18**	*Theoretical* (rarely enforced in practice for online access)	**No** (with only a clarification that a minor's self-declaration does not constitute verification)
	At the same time, SREN law art. 1, modifying in particular art. 10 of the LCEN for **pornographic content**		*Upcoming*	**Yes** (*ARCOM framework on access to pornography* of October 2024).

Tab. 1: Summary of France's main online age verification scenarios (with main legal sources, status of application and details on age verification system to be implemented)

France has dealt with several online age verification scenarios over the past two decades. More precisely, the last two years have shown a great level of proactivity in the field. However, the state of progress of each scenario depends closely on its own legislative context, leading to varying levels of application from one legal regime to another. This disparity is sometimes explained by the complex issues related to the distribution of responsibilities between France and the EU. It was, until recently, generally accompanied by a lack of specific guidance regarding the technical verification system to set up. The notable efforts undertaken by France make the topic of online age verification an advanced project, but one that is still in progress and requires further development overall.

Chapter 2: Analysis of Age Verification Scenarios in EU Legislation

Other online age verification scenarios are gradually emerging at the EU level. The BIK+ strategy[120] uses the idea of an age verification system several times, mentioning various scenarios[121]. The objectives of these scenarios, and sometimes even more specifically their themes or the actors they regulate, significantly interact with the objectives of the scenarios provided for by the French legal framework. Most of the age verification scenarios in this chapter have also been addressed through regulation over several years. They will also be classified according to their last "*substantial*" or even prospective modification, from the oldest of these scenarios to the most recent developments. We will thus analyze the age verification scenarios that aim: to apply to minors a regime intended to be more protective in terms of data protection (I), to protect them from content which may impair their physical, mental or moral development (II), to apply various protection mechanisms to them in the context of their use of digital services (III) and finally, to protect them from sexual abuse (IV).

I - The Theoretically Enhanced Protection of Minors' Personal Data [GDPR]

A. Legal Framework

1) Legal provisions calling for a verification

The principle of "*lawfulness of processing*" from the GDPR[122] requires data controllers to justify their data processing via one of the six legal bases provided for by the regulation.[123] One of these legal bases is fulfilled when data subjects

[120] BIK+ strategy, (2022), *op. cit.*

[121] *Ibid.,* p. 6, 10 and 11.

[122] GDPR, (2016), *op. cit.,* art. 5.1.a)

[123] *Ibid.,* art. 6.1.

give their consent to the data controller.[124] The regulation not only sets out details on the conditions of validity of this consent[125], but also includes a dedicated article on "*conditions applicable to child's consent in relation to information society services*"[126]. This article specifies that the consent given by a child to an *information society service* can only be lawful if it is *authorized by the holder of parental responsibility over the child.* The GDPR provides a threshold age, which must be verified, set at 16, with the possibility for each Member State to set a lower age, ranging down to 13 years at the lowest. France retained the age of 15[127] for the application of this mechanism, which served as a model for the age chosen in the mechanism restricting access to social networks, as examined in the first chapter[128].

The GDPR, which explicitly recognizes the need for specific protection of children in terms of data protection[129], provides specific provisions in this regard. In terms of the right to information, it is specified that "*any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*"[130]. The *right to erasure ('right to be forgotten') is* also strengthened if the data subject, who was consenting, was a child at the time[131]. The question of the presence of a child may also have to be taken into account in terms of risk analysis[132] and

[124] *Ibid.,* art. 6.1.a).

[125] *Ibid.,* art. 4.11 and 7.

[126] *Ibid.,* art. 8.

[127] France, LAW no 78-17 of 6 January 1978 on data Processing, Data Files and Individual Liberties, *("relative à l'informatique, aux fichiers et aux libertés"),* art. 45.

[128] Part I, chap. 1, III of this study.

[129] GDPR (2016), *op. cit.,* whereas 38.

[130] *Ibid.,* whereas 58. Also see art. 12.1, asking "*to provide any information […] in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*".

[131] *Ibid.,* whereas 65 et art. 17.

[132] *Ibid.,* whereas 75

more precisely when justifying the processing via the legitimate interest[133] legal basis.

2) Specifications about the age verification system to implement

The GDPR, however, remains unclear on the precise age verification system to implement. With regard to consent, the regulation only asks the data controller to "*make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology*"[134]. The European Data Protection Board (EDPB) seems to limit the scope of this obligation by specifying that the measures must be proportionate to the risks of the processing activities[135]. The authority also mentions the possibility to use a verification system that consists only of a simple declaration of the user, following which the data controller *"can"* take *"appropriate checks to verify that this statement is true"*[136], including "*if doubts arise"*[137]. Although the EDPB mentions the possibility for data controllers to resort to *"trusted third party verification services*"[138] to obtain an authorization from the child's legal representatives, the EU data protection framework remains relatively non-prescriptive on the exact methods of verification[139]. The

---

[133] *Ibid.,* art. 6.1.f).

[134] *Ibid.,* art. 8.2.

[135] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* 4 May 2020 , para. 132 (see also para. 135).

[136] *Ibid.,* para. 133 (see also para. 135).

[137] *Ibid.,* para. 135.

[138] *Ibid.,* para. 137.

[139] By comparison, the situation in Great Britain appears to be slightly more detailed. The *Information Commissioner's Office* (the data protection authority in Great Britain), although also using a risk-based approach, provides further details on the subject in its part "*3. Age appropriate application*" from its "*Age appropriate design: a code of practice for online services".* available at : *https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/* , accessed on 1 December 2024.

general result is a non-application of users' age verification before the obtaining of their consent[140].

The situation is not much more precise in terms of the exercise of the right to erasure. When a data subject triggers this right, by specifying that their consent was given when they were a child, the data controller can immediately grant the request or verify the declaration.[141] The most common practice is for the data controller to request a copy of the identity document from the data subject.[142]

B. Issues and Challenges at Stake

1) Especially for minors

The main direct issue lies in the reinforced protection of children against the exploitation or misuse of their personal data. This is therefore a concern relating to the defense of the fundamental right to the protection of one's personal data and respect for one's private and family life. An issue of the level of empowerment of children linked to the active participation of their legal representatives also appears[143], in the same way as for the legal framework for age verification regarding access to social networks in France.

Despite this wish intention to protect, the lack of precision concerning the verification system to set up regarding the validity of consent to the processing of one's data makes this regime an illusory form of protection. Worse still, the possibility[144] for the data controller to request a copy of the data subject's

[140] Goicovici J, *The collecting of consent to the processing of children's personal data, between volatility and disobedience,* SHS Web of Conferences, 2023.

[141] GDPR, (2016), *op. cit.,* art. 12.6 (and whereas 64 for right of access).

[142] This practice is monitored by the EDPB which tends to try to limit it. See notably EDPB, *Guidelines 01/2022 on data subject rights - Right of access*, Version 2.1, 28 March 2023, para. 74-79.

[143] See, for these two challenges of "protection" (by parents) and "*emancipation and participation*" of children to be weighed in balance, Hof S. van der, *I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World.* Wisconsin International Law Journal, 34(2), 2017, p. 125-132.

[144] Although questionable when used systematically even when not relevant. See CNIL, Deliberation no. 2018-284 of 21 June 2018 (referral no. AV 18012134) " *such a systematic requirement could lead the data controller to process excessive amounts of data in relation to the purposes pursued, in breach of the principle of data minimisation" (une telle exigence systématique pourrait conduire le responsable du*

identity card regarding the right to erasure is not only restrictive but also potentially dangerous. The exact terms of transmission of the copy of the identity document, and its storage by the data controller remain at its discretion, which means that the general level of security of the verification processes in this matter exposes the data subject to the risk of identity theft.

2) Broader concerns

Beyond the immediate protection of children, this issue raises broader concerns related to the application of the regulation in different Member States. The mere existence of different age thresholds within the EU makes it more difficult for entities operating in multiple Member States, as it introduces additional complexity into cross-border compliance. Furthermore, the risk-based approach, although it can lead to appropriate protection in certain cases, can accentuate inequalities in the treatment of data subjects depending on the resources and sensitivity of the data controller or national data protection authorities.

II - Protection From Content Potentially Impairing Minors' Physical, Mental or Moral Development [AVMSD]

A. Legal Framework

1) Legal provisions calling for a verification

The first AVMSD[145] was adopted in 2010. The protection of minors was already an important objective[146] . The directive provides for a ban of audiovisual commercial communications[147], television advertisements and teleshopping[148] for alcoholic beverages expressly aimed at minors. These measures are

traitement à traiter des données excessives au regard des finalités poursuivies, en méconnaissance du principe de minimisation des données").

[145] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)

[146] *Ibid.,* whereas 12.

[147] *Ibid.,* art. 9.1.e.

[148] *Ibid*., art. 22.a).

therefore part of a certain continuity with those mentioned within the French legal framework in terms of access to alcoholic beverages. Other measures in the directive can be compared to other verification scenarios. There is indeed an obligation for Member States to take appropriate measures to prevent media services and audiovisual services on demand that could seriously harm the physical, mental or moral development of minors from being accessible to them.[149] Another comparable measure, aimed at television shows and broadcasting organizations, specifies that programs likely to seriously harm the physical development of minors may in particular be those including scenes of pornography or gratuitous violence[150].

The directive was updated in 2018[151]. The aforementioned article 12 was then replaced[152] by another that is almost similar in content, focusing on media service providers.[153] A clarification is nevertheless provided by the legislator. It is specified in the article that the measures that can be taken by each Member State may include the use of tools allowing age verification or other technical measures. Age verification is mentioned a second time. It is indeed one of the measures that can be implemented by the "*video-sharing platform providers*" to protect minors from content likely to harm their development[154]. Among the other measures that can be implemented by platforms for the same purpose are parental control systems[155], such as the one conditioning the access to social networks in France, seen in the first chapter[156].

---

[149] *Ibid.,* art. 12.

[150] Ibid., art. 27.1.

[151] AVMSD (2018), *op. cit.*

[152] *Ibid.,* art. 1.17.

[153] *Ibid.,* art. 1.10), creating an article 6.a).

[154] *Ibid.,* art. 1.23), creating an article 28b.3.f).

[155] *Ibid.,* art. 1.23), creating an article 28b.3.h).

[156] Part I, Chap. 1, III of this study.

2) Specifications about the age verification system to implement

The AVMSD is not very prescriptive regarding the technical methods of age verification. Regarding the first of the two mentions of age verification systems, which concerns media service providers, the legislator specifies that the measures must be "*proportionate to the potential harm of the program*"[157], and that personal data collected during the verification process must not be processed for commercial purposes[158]. This last measure is repeated for the second mention of age verification systems, concerning video-sharing platform providers[159]. Member States are supposed to put in place the necessary mechanisms to evaluate the appropriateness of the measures implemented by by video-sharing platform providers, such as age verification systems[160]. Another measure more directly allows Member States, if they wish, to impose on video-sharing platform providers more detailed or stricter measures in this area. The level of transposition of the directive differs from one Member State to another[161]. In France, in 2020[162], this left the ARCOM the possibility to specify the conditions under which age verification systems in particular can be put in place[163]. These details were not directly provided through this method, but partially via the SREN law[164] and the ARCOM framework on access to pornography[165] studied in the first chapter[166]. This was only partial, because the SREN law and the framework only cover pornographic content and not all content that could harm the development of minors covered by the AVMSD.

---

[157] *Ibid.,* art. 1.10), creating an article 6.bis.1.

[158] I*bid.,* art. 1.10), creating an article 6.bis.2.

[159] *Ibid.,* art. 1.23), creating an article 28b.3 para. 4.

[160] *Ibid.,* art. 1.23), creating an article 28b.5.

[161] See the different stages of application in each Member State in European Audiovisual Observatory, *The protection of minors on VSPs: age verification and parental control,* 2023.

[162] France, ordinance no. 2020-1642 of 21 December 2020.

[163] *Ibid*., art. 22 creating new art. 60 in the LAW no. 86-1067 of 30 September 1986 on freedom of communication *("relative à la liberté de communication") (Loi Léotard)).*

[164] SREN law, (2024), *op. cit.*

[165] ARCOM framework on access to pornography, (2024), *op. cit.*

[166] For access to pornography detailed in part I, chap. 1, IV of this study.

B. Issues and Challenges at Stake

1) Especially for minors

The AVMSD includes issues already mentioned regarding the access to pornography. The protection from content which may impair the physical, mental or moral development of minors can possibly aim to prevent certain addiction phenomena, but more broadly try to ensure that minors are not encouraged to reproduce certain inappropriate behaviors. Beyond public health concerns, issues of public order also arise.

2) Broader concerns

The nature of the regulation, namely a directive, illustrates an issue already discussed differently. Pornographic content is mentioned by the AVMSD as an example of content which may impair the physical, mental or moral development of minors, but this list is not exhaustive. Therefore, the interpretation of this concept may vary from one Member State to another. Two consequences arise from this. The first, comparable to the scenario of age verification in terms of access to pornography, is of a practical nature for regulated entities. A non-harmonized application across the EU of what constitutes unsuitable content for minors would lead to disparities which could lead to inequalities from a competitive point of view. The second consequence affects the population more directly. Preventing minors from accessing certain content, under the guise of protecting their good mental and moral development could, taken to the extreme, amount to a form of questionable censorship. Hungary's choice in 2021[167] assimilating the ban on pornographic content and content promoting change of gender identity, sex change and homosexuality to minors under the same regime illustrates this risk.

[167]See notably European Parliament press release *European Parliament vehemently opposed to Hungarian anti-LGBTIQ law,* 08 July 2021.

III - Protection of Minors in the Context of Digital Services Use [DSA]

A. Legal Framework

1) Legal provisions calling for a verification

The creation of the DSA[168] marks an important step in the EU regulation of digital services. This regulation, which updates some provisions of the eCommerce Directive[169], is part of a framework aimed at protecting the fundamental rights of users while adapting legislation to the growing role of digital services in daily life. The protection of minors figures prominently among the strategic objectives of the DSA[170]. The regulation provides for several regimes in this regard.

The first regime should be compared to two verification scenarios studied in the first chapter, namely access to social networks[171] and pornography[172]. It is applied to "*intermediary services*"[173], which include in particular "h*osting' services*"[174]. This category includes "*online platforms*"[175], which can be *"social networks*"[176] and/or which can be used for the diffusion of pornographic content[177]. When these entities address minors, the DSA requires them to explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand[178]. The DSA seems to create what could be

[168] DSA, (2022), *op. cit.*

[169] eCommerce Directive, (2000), *op. cit.*

[170] DSA, (2022), *op. cit.*, especially whereas 71.

[171] Part I, chap. 1, III of this study.

[172] Part I, chap. 1, IV of this study.

[173] DSA, (2022), *op. cit.,* art.3.g).

[174] *Ibid.*, art. 3.g)iii.

[175] *Ibid.*, art. 3.i).

[176] *Ibid.*, whereas 13.

[177] *Ibid.*, whereas 87 mentions this hypothesis for *"very large online platforms*".

[178] *Ibid.*, art. 14.3.

analyzed as a presumption of minority when the *intermediary service* is *"primarily directed at minors or is predominantly used by them"*[179], taking into account in particular its design or marketing[180]. An online age verification system could still potentially be considered on a case-by-case basis

A second mechanism established to protect minors in the regulation applies only to online platforms, when they are accessible to minors. These platforms are then required to implement "*proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service*"[181]. This regime also includes a measure prohibiting online platforms to present advertising to minors on the basis of profiling of the said minors[182]. A sort of presumption of minority comparable to the first regime emerges with regard to online platforms "*accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes*" [183]. The observation is the same for the more precise ban on the profiling of minors for advertising purposes, which applies when providers of online platforms are "*aware with reasonable certainty*" that the target of the advertising is a minor[184]. The question of an age verification system specifically put in place to respond to this regime may still arise. Certainly, the regulation specifies that it does not require *online platforms* to process additional personal data, in order to determine whether the recipient of the service is a minor or not[185]. It refuses to be interpreted as an incitement for "*online platforms to collect the age of the*

[179] *Ibid.*, art. 14.3.

[180] *Ibid.*, whereas 46.

[181] *Ibid.*, art. 28.1.

[182] *Ibid.*, art. 28.2.

[183] *Ibid.*, whereas 71.

[184] *Ibid.*, whereas 71 and art. 28.2.

[185] *Ibid.*, art. 28.3.

user of the service prior to their use"[186]. But the first steps of the DSA application, which will be mentioned below, suggest future clarifications on the methods of age verification and, therefore, a possible incentive to implement such an age verification system.

The third DSA regime to be mentioned is applied to *online platforms and to online search engines*[187] considered "*very large*"[188]. The regulation requires these entities to establish measures to mitigate risks that might have been identified. The regulation cites among the possible examples of risks "*any actual or foreseeable negative effects in relation to […] the protection of […] minors*"[189]. Here, a possible presumption of minority users can also be interpreted from the wording of the text, when the services "*are aimed at minors or predominantly used by them*"[190]. This third DSA regime nevertheless differs from the first two by explicitly mentioning age verification. Among the possible risk mitigation measures for minors there are "*targeted measures to protect the rights of the child, including age verification and parental control tools*"[191]. More comparable to a recommendation, the establishment of an age verification system therefore does not constitute, *a priori,* a direct obligation for very large online platforms and *very* large online search engines. The future application of the DSA could, however, make this recommendation an obligation in practice.

2) Specifications about the age verification system to implement

Although the DSA mentions different protective regimes for minors, it does not directly specify the methods for verifying whether users are adults or minors. For the third regime, the regulation invites very large online platforms and very

[186] *Ibid.*, whereas 71.

[187] Defined in DSA, (2022), *op. cit.,* art. 3.j).

[188] That is to say having a number of active users equal to or higher than 45 million and designated as such in the conditions of the DSA, (2022), *op. cit.*. See in particular art. 33.1 and 33.4.

[189] DSA, (2022), *op. cit.,* ar. 34.1.d).

[190] *Ibid.*, whereas 89.

[191] *Ibid.*, art. 35.1.j).

large online search engines to consider *"industry best practices, including as established through self-regulatory cooperation, such as codes of conduct"* as well as potential future guidelines from the European Commission[192].

As planned by the DSA[193], guidelines from the European Commission are currently being developed in order to specify the application of the second regime mentioned, namely article 28 applicable to online platforms. Although age verification is not explicitly mentioned in the regulation for this regime, it is mentioned in the European Commission's call for evidence[194] related to the forthcoming guidelines[195]. ARCOM communicated during this consultation phase to encourage the European Commission to publish "*as soon as possible either general guidelines on article 28 or to consider issuing shorter and minimal guidelines related to article 28 but dedicated only, for instance, to the protection of minors on pornographic online platforms or to prevent them from accessing the most serious content*"[196].

Although the European Commission has already started to apply the DSA[197], we will have to wait for this application to become clearer regarding the methods used for age verification in this context. In this regard, the European Commission will particularly rely on the work of the *European Board for Digital Services*[198] and the *Task Force on Age Verification* launched in early 2024[199], in

---

[192] *Ibid.*, whereas 89.

[193] *Ibid.*, art. 28.4.

[194] European Commission, *Call for evidence for an initiative - Digital Services Act - guidelines to enforce the protection of minors online,* Ref. Ares(2024)5538916, 31 July 2024, p. 2-3.

[195] Planned for Q2-2025.

[196] ARCOM, *Arcom's contribution to the Call for evidence for guidelines on the protection of minors under the Digital Services Act*, 26 September 2024.

[197] This is particularly true of measures to protect minors, as illustrated by the formal proceedings opened by the Commission. See the press release *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram,* 16 May 2024.

[198]The European Board for Digital Services is established by the DSA. Its working group n°6 focuses on protection of minors. The Task Force on Age Verification and the ARCOM are participating in this group.

[199] The Commission has set up this task force for the implementation of the DSA in cooperation with national authorities of Member States. This cooperation would build on existing measures at national level,

which the French authorities are also encouraged by the European Commission to "*continue their active participation*"[200]. It should also be noted that the regulation supports the publication of "*voluntary standards set by relevant European and international standardization bodies",* particularly concerning targeted measures to protect minors online[201].

B. Issues and Challenges at Stake

1) Especially for minors

Age verification in the DSA responds to numerous concerns already mentioned in other texts. The most obvious issue is certainly the desire to protect minors from inappropriate content, just like the AVMSD did with respect to access to pornography in France, and more generally the desire to protect them from the broader risks associated with accessing online services, to which the French legal regime also seeks to respond for social networks services.

By requiring intermediary services to make a particular effort to simplify and clarify their conditions of use, the regulation actually applies measures normally already suggested by the GDPR in terms of the right to information as detailed earlier[202]. This concern for the integration of minors and the promotion of meaningful autonomy while seeking, at the same time, to integrate their legal representatives, is also reflected in the mention of parental control tools in the DSA.

Finally, by prohibiting targeted advertising for minors, the regulation also aims to reduce the risks of psychological manipulation or economic exploitation of young audiences, reflecting certain common concerns with the French regime on access to gambling.

---

including those resulting from the transposition of the AVMSD (2018), *op. cit.,* studied in part I, chap. 2, II of this study.

[200] European Commission, *detailed opinion on Notification 2024/0208/FR*, *op. cit.,* p. 3.

[201] DSA, (2022), *op. cit.,* art. 44.j).

[202] See part I, chap. 2, I of this study.

2) Broader concerns

Beyond the protection of minors, age verification raises indirect implications in connection with the practical implementation of the DSA's provisions. The absence of European harmonization specifying the technical arrangements could once again generate significant disparities between Member States: it could create a competitive disadvantage for players subject to stricter requirements in certain countries. Conversely, a future application of the DSA, which would ultimately impose age verification in practice, will have to take into account other obligations to which regulated actors may already be subjected to through other regimes. As a general example, the age threshold of majority is 18 years for the DSA[203], while the application of the AVMSD and the GDPR may result in different age thresholds to be verified depending on each Member State. Without it being necessary to analyze the interaction of more specific measures[204], this difference in age thresholds that has to be verified by one entity could represent a constraint both for regulated players, in terms of compliance and for users of their services, in terms of user experience.

[203] Not directly specified in the regulation but suggested in the *Call for evidence for an initiative - Digital Services Act - guidelines to enforce the protection of minors online* (2024), *op. cit.*, p. 2.

[204] See the case of certain pornographic sites being also considered as very large online platforms within the meaning of the DSA, (2022), *op. cit.*, via the European Commission press release *"Commission designates adult content platform XNXX as Very Large Online Platform under the Digital Services Act",* 10 July 2024. See also the different age thresholds existing in each Member State for different age verification situation on the European Union Agency for Fundamental Rights website https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu , accessed on 1 December 2024.

IV - Protection of Children From Sexual Abuse [CSAR]

A. Legal Framework

1) Legal provisions calling for a verification

In 2021, a provisional regulation[205] introduced a temporary derogation from certain provisions of the *ePrivacy* Directive[206] regarding the confidentiality of communications and the retention of traffic data[207]. This exemption initially applicable until August 3, 2024[208] allows number-independent interpersonal communications services to use the data collected as part of their services to detect sexual abuse committed against minors online and to report it to the competent authorities[209]. The text does not detail the precise nature of the technologies to be used but specifies that "*the technologies used to detect patterns of possible solicitation of children are limited to the use of relevant key indicators and objectively identified risk factors such as age difference*"[210]. In this regard, it is conceptually possible to draw a link with possible age verification systems.

This exemption was put in place, as the preparation and adoption of a long-term legal framework were pending. In this sense, a regulation "*laying down rules to prevent and combat child sexual abuse"* (CSAR) was proposed in 2022[211]. The

[205]Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

[206] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) consolidated text after the adoption of the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[207] *Ibid.,* art. 6.1.

[208] *Ibid.,* art. 10.

[209] Regulation (EU) 2021/1232, *op. cit.* art. 3.1.a.i).

[210] *Ibid.*, art. 3.1.f).

[211]CSAR, (2022), *op. cit.*

text proposes to repeal the aforementioned 2021 provisional regulation[212] to replace it with a framework whose mechanisms and wording in some respects can be compared to those of the DSA. The proposal **provides for o**"*an assessment of the risk of use of the service for the purpose of online child sexual abuse*"[213]. The providers of hosting services and providers of interpersonal communications on the one hand[214] and the providers of software application stores on the other hand[215], having identified such a risk, are then respectively required to "*take the necessary age verification and age assessment measures to reliably identify child users on their services*". A slight difference therefore appears compared to the DSA since the wording used in the proposal seems not to constitute a recommendation but directly an obligation for regulated actors.

2) Specifications about the age verification system to implement

The provisional regulation, like the proposed 2022 regulation, does not detail the technical means to be implemented to verify the users' age. The proposal nevertheless provides that the European Commission may, after conducting a public consultation, publish guidelines on the application of the respective regimes by *providers of hosting services and providers of interpersonal* communications[216] and providers of software application stores on the other hand[217].

The prospect of such guidelines still has a long way to go and will first and foremost require that the text be adopted. The already busy legislative calendar under *Ursula von der Leyen's* first mandate did not allow the co-legislator to

[212] *Ibid.,* art. 88.

[213] *Ibid.,* art. 3.

[214] *Ibid.,* art. 4.3.

[215] *Ibid.,* art. 6.1c).

[216] *Ibid.,* art. 4.5.

[217] *Ibid.,* art. 6.4.

reach an agreement before the end of the period initially covered by the provisional regulation of 2021, i.e. before August 3, 2024. A second temporary regulation of three pages was therefore voted in 2024[218] in order to extend this date until April 3, 2026[219] to allow sufficient time to resume negotiations on the CSAR proposal.

B. Issues and Challenges at Stake

1) Especially for minors

The legal framework for combating sexual abuse of minors naturally aims to protect "minors"[220] against serious risks to their physical and moral integrity. A parallel can be drawn between the objective of protecting physical integrity and the French framework of age verification in terms of access to alcoholic beverages and tobacco products. The objective of protecting moral integrity could be compared to the frameworks set by the AVMSD and the framework of age verification governing access to pornographic content in France. But here too, and perhaps even more so, data protection concerns then also emerge[221].

2) Broader concerns

As for the DSA, the risk of fragmented approaches across the EU could arise depending on whether the European Commission publishes guidelines and their exact content. Unlike the DSA, however, age verification systems will

[218] Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

[219] *Ibid.*, art. 1.4 amending article 10 of regulation (EU) 2021/1232, *op. cit.*

[220] Although the age of Consent for sexual activity with an adult varies from one Member State to another. See the different age thresholds about it on the European Union Agency for Fundamental Rights website, https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/consent-sexual-activity-adult , accessed on 1 December 2024.

[221] CSAR's proposal received strong criticism after it was published, due to its mechanism involving large-scale scanning of communications. See on this point *EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse,* 28 July 2022, para. 91 (European Data Protection Supervisor - EDPS) and EDPS, *Briefing note on the CSAM proposal: "The Point of No Return",* 23 October 2023, p. 1-2. A parallel can be drawn with the terms of the Online Safety Act 2023 Government Bill of the United Kingdom of 26 October 2023, which has generated the same kind of criticism.

directly constitute an obligation here, if the proposed text is voted on. Therefore, the European Commission will have to ensure that the systems in question are compatible with other obligations to which regulated entities may already be subject, and that these systems are also realistic in terms of the financial resources to be deployed by the latter.

Chapter 2 Summary

Verified scenario	Main legal source	Age verified	Application	Details on verification systems
Protection of minors in terms of personal data	GDPR art. 8 for the age to **consent to the processing of personal data**	**15** in France (**16** by default, but each Member State may lower it to **13**[222]).	*Theoretical* (rarely applied in practice)	**No**
	GDPR whereas 58 and art.12.1 for the **right to information**			
	GDPR whereas 75 and art. 6.1.f In terms of **risk analysis** and use of **legitimate interest**			
	GDPR whereas 65 and art. 17 for the **right to erasure**			**No** (in practice, often a request to send a copy of the identity card)
Protection from content that may impair the physical, mental or moral development of minors	AVMSD (2010, as amended in 2018) art 6.a and 28b.3.f	**18** in France (but may vary by Member State)	*Partially* (Depends on Member State)	**No**
Protection of minors when using digital services	DSA art.14. obligation for intermediary services to **adapt the information in their terms and conditions** to minors	**18** (not directly specified in the text but inferred from its application)	*Upcoming*	**No**
	DSA art. 28, obligation for online platforms to put in place **appropriate measures to protect minors**, and **ban advertising based on profiling** of minors			*Guidelines of the European Commission to come for Q2 2025* in application of art 28.4 of the DSA
	DSA art. 35.1.j mentions age verification as a **risk mitigation measure** that very large online platforms and the very large online search engines may implement.			**No** (recommendation to draw from industry best practices and possible future Commission guidelines, thus the guidelines of art 28.4 could possibly also constitute a source of inspiration)
Protection of children from sexual abuse	Regulation (EU) 2021/1232, art.3.1.a.i) and 3.1.f indirectly **permits** number-independent interpersonal communications services to implement an age verification system	**18** (in line with the directive 2011/92/U, art 2.a. Although subtleties may appear between Member States depending on the age of sexual consent also mentioned in the directive in art 2.b. i.e. 15 years in France.	*Rarely used*	**No**
	CSAR proposal art. 3, 4 and 6 mentions age verification as a **risk mitigation measure** that providers of hosting services and providers of interpersonal communications, and providers of software application stores must set up		*Not yet voted*	*Possible guidelines of the European Commission* when the text will be voted (provided for in art. 4.5 and 6.4)

Tab. 2: Summary of EU's main online age verification scenarios (with main legal sources, status of application and details on age verification system to be implemented))

[222] See the different age thresholds regarding consent on the European Union Agency for Fundamental Rights website, https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children , accessed on 1 December 2024.

In recent years, the EU has also taken up several age verification scenarios. As seen in the previous chapter and confirmed in this one, the scenarios regulated by the EU sometimes interact significantly with those regulated by France. Unlike in France, where verification scenarios generally aim to grant access or refuse it, in the EU these scenarios generally aim to apply a more protective regime to minors identified as such. However, EU verification scenarios rarely impose age verification as a direct obligation, but rather as one of the possible measures for regulated entities to be compliant with more general requirements. Specifications on online age verification systems to set up are then not specified by the European legislator. However, things could change with the recent adoption and current phase of application of the DSA, which could perhaps bring about the *"European technical solution"* regarding age verification, *"for the benefit of the whole new generation of Europeans"*[223] in the future.

[223] European Commission, *Detailed opinion in response to Notification 2023/461/FR, op. cit.,* p. 5.

Part I Summary and Conclusion

Today, verifying various age thresholds online is a question addressed in many legislations, both in France and at the EU level, with largely overlapping regulatory concerns.

The first category of considerations concerns the initial objectives of the legislator, who seeks to impose or encourage age verification to protect minors. This protection may target their physical and psychological integrity, in the short or long term. Public health thus appears to be a recurring concern, particularly linked to issues of addiction. The economic interests of minors can sometimes also be targeted. However, certain regulations pursue complementary or predominant purposes, such as the preservation of public order, the fight against tax fraud and AML/CFT as illustrated by the regulations on access to online gambling and betting in France.

A second series of concerns arises from the undesirable effects that age verification systems could entail[224]. These effects primarily concern minors themselves, exposed to the risk of a false illusion of security in the case of an imperfect age verification system or a deficient legal framework. The question of their degrees of empowerment and the eventual involvement of their legal representatives in the regimes also remains central in several scenarios. The implications extend beyond just minors. Age verification scenarios often involve not only age checking, but also other elements of the user's identity. This raises concerns for all users regarding the fluidity of the user experience and, more significantly, in terms of fundamental rights to the protection of personal data and, more generally, the right to privacy. Systems could also be misused for purposes of surveillance or repression by public bodies, representing a threat to freedom of speech.

[224] EDRi, *Joint Statement on the Dangers of Age Verification Proposals to Fundamental Rights Online,* 16 September 2024.

The regulated entities may also be exposed to risks, due to the cost of implementing age verification systems, and sometimes also with respect to competitive imbalances. The overlap of certain legislative frameworks can lead to challenges in legal certainty for entities subjected to several of them. This interaction between legal frameworks is also a challenge for national and European legislators, who are in fact interdependent[225]. France's attempt to regulate minors' access to social networks, ultimately inapplicable, is an example since it would normally fall at the EU level. On the contrary, Europe's desire to protect minors from certain content through the AVMSD is conditional on the national transposition of each Member State, which may remain incomplete, as in France, despite the progress that the SREN law represents for pornographic content.

Source of challenge /risk **Concerned by the challenge /risk**	Initial situation motivating the adoption of a regulation	Potential adverse effects of a regulation (or of the resulting age verification system)
Minors	Physical integrity Mental or moral integrity Economic interest (*e.g. addiction and public health, fight against harassment, etc.*)	Degree of empowerment of the minor (and integration or exclusion of their legal representatives) Exclusion of specific categories of children Ineffectiveness (false sense of security)
Broader concerns	Adult addiction too AML/CFT Tax fraud Public order	Privacy and data protection Freedom of speech Use of age verification systems by public bodies for repressive purposes *(all these elements can also be applied to minors to a certain extent depending on the situation)* User experience, or even exclusion of certain categories of users Difficulties in the interplay between different legislations due to imprecisions, prerogatives or fragmentation (implementation difficulties for regulated entities, and potential inequalities in competition) Implementation costs of age verification systems and potential loss of customers

Tab. 3: Summary and classification of key challenges and risks identified in Part I concerning online age verification scenarios under French and EU legislation

The SREN law and its current application through the ARCOM framework on access to pornography call, just like the DSA and its current application through forthcoming guidelines from the European Commission, for one final lesson.

[225] The same synergies can be observed for other Member States, leading to other possible risks of interaction between the various national measures among them and with those of the EU. See in this respect the various technical standards notified to the European Commission by various Member States in 2024 alone, such as Spain (Notification Number: 2024/0531/ES), Italy (Notification Number 2024/0578/IT), Ireland (Notification Number 2024/0283/IE), Germany (Notification Number 2024/0283/IE 2024/0188/DE) and Denmark (Notification Numbers 2024/0483/DK, 2024/0226/DK, 2024/0225/DK and 2024/0064/DK).

Legal frameworks that fail to specify concrete methods for age verification generally remain inapplicable or not very effective. This lack of details may result from an unfinished legislative ambition or from political choices that leave regulated entities without clear indication about the age verification system to set up. Remote sales of alcohol, tobacco and vaping products in France, as well as the protection of minors under the GDPR, are examples of such imperfect regimes. Contemporary French and European legislators seem aware of the importance of combining legal obligations with details of the verification system to set up, going so far as to directly reference specific age verification systems. The second part of this study proposes to study these thoughts on the online age verification system to set up, and on a possible common age verification system for the EU.

PART II: IDENTIFICATION OF RELEVANT KEY COMPONENTS OF AGE VERIFICATION SYSTEMS TO ENSURE CONSISTENCY

The multiple issues identified in the first part highlight the crucial importance of designing an effective online age verification system. The question then becomes what would constitute the future of age verification systems? To try to answer this question, this second part proposes to take different approaches, integrating as many considerations as possible raised in the first part. We will first analyze theoretical classifications of systems. Elements will then emerge suggesting the effectiveness of a given system, as well as the potential level of risk it entails (chap. 1). Once these theoretical bases have been established, we will be able to focus on concrete age verification ecosystems, exploring the legal and technical frameworks developed by the EU and France in the field of digital identity. These developments, which involve both public and private stakeholders, are gradually tending to apply precisely to certain age verification scenarios studied in the first part of this study (chap. 2).

Chapter 1: Analysis of Two Typologies to Hierarchize Age Verification Systems

Many technologies and configurations can be considered in order to verify that an online service's user exceeds a given age threshold. A framework for analysis therefore appears necessary to assess the relevance of a verification system in relation to the main issues arising from the first part. A first method of classifying age verification systems, according to the nature of the proof of age, will thus be proposed (I). In order to better respond to the challenges of online age verification, this first classification will then be supplemented by a second one, focusing more on the stakeholders in the verification process and their organization, that is to say the architecture of the verification system (II). These two classifications combined will allow us to estimate, throughout this chapter,

the direction in which the future of the online age verification system seems to be heading.

I - Typology Based on the Nature of Age Proof

A first way frequently used to classify the different online age verification systems is to take the nature of the age proof as a point of distinction. This classification method studies how age information is initially generated. Three categories of systems are then distinguished: those based on a user declaration (A), those based on the verification of certified information (B) and those based on an age estimation (C). Each category will be explained and illustrated before listing any potential limitations.

A. Self-Declared

1) General concept

"Declarative"[226], or *"self-declaration"*[227,228], of *"age declaration"*[229,230], such various yet similar formulations cover the same idea of a system based on a simple declaration made by users about their age or their belonging to an authorized age group.

This method relies on the presumption of good faith and the assumption that users will provide accurate information without seeking to circumvent restrictions. The operation of these systems is generally not very intrusive, as it is most of the time limited to a check box or the simple indication of a date of

[226] Center of expertise in digital régulation ("*Pôle d'expertise de la régulation numérique" - PEReN*), *Online underage users detection: can we reconcile efficiency, convenience and anonymity?*, Shedding light on", #04, May 2022, p. 8.

[227] ARCOM framework on access to pornography, (2024), *op. cit.,* p. 11.

[228] Renaissance Numérique, *Age assurance online: working towards a proportionate and European approach,* September 2022, p. 26.

[229] EDRi*, Position paper Online age verification and children's rights,* 4 october 2023, p. 15 and CNIL on its website, page *Recommendation 7: verify the child's age and parental consent while respecting their privacy ("Recommandation 7 : vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée"),* 1 June 2021, https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee , accessed on 1 December 2024.

[230] Forbrukerrådet, *COMMERCIAL EXPLOITATION OF CHILDREN…*, (2024), *op. cit.,* p. 37.

birth. They offer a simple and quick solution, promoting the smoothness of the user experience.

2) Examples

"*Are you over 18? [Yes] / [No]*": Self-declaration systems are widely used in the context of the online sale of regulated products, such as alcohol in particular. To this day, they are also widely used when it comes to accessing pornographic sites. As mentioned in the first part of this study, the widespread use of this easy solution led the French legislator to clarify in 2020[231] that the mere establishment of such a system cannot constitute a release of liability for the person responsible for the offense of exposing minors to inappropriate content[232].

3) Limits

Despite their practicality, self-declaration systems have easily conceivable limits. Especially when they are used to authorize or deny access to regulated products or inappropriate content, minors can freely make a false declaration and immediately access the desired services. It is therefore not surprising to see a consensus emerging between public authorities regarding the lack of relevance of using age "verification" systems for this category.

B. Certified

1) General concept

"*Certification*"[233], "*age check, using a document with the person's identity and date of birth*" [234], "*ID-based age verification*"[235] *"techniques for generating proof*

[231] LAW n°2020-936*, op. cit.,* art. 22.

[232] French Penal Code, art. 227-24 regarding content of a pornographic, violent or inciting terrorism nature or likely to seriously harm human dignity or to incite minors to engage in games putting them in physical danger. As studied in the part I, chap I, IV of this study.

[233] CNIL on its website, page *Recommendation 7…,* (2021), *op. cit.*

[234] PEReN, *Online underage users detection…*, (2022), *op. cit.,* p. 6.

[235] Forbrukerrådet, *COMMERCIAL EXPLOITATION OF CHILDREN…*, (2024), *op. cit.,* p. 30.

of age based on the presentation of a physical identity document" [236], "*verification* "[237], "*document-based age verification"*[238], *etc. ;* the second category of online age verification systems is also covered by many terms. Here, users have to provide proof via an element certified by a trusted source, most of the time involving directly or indirectly the State at the end of the chain. Depending on the age verification system studied, the entity that has to verify an age proof can use several methods to ensure the authenticity of the proof provided.

2) Examples

The most classic example is the transmission of a copy of an identity document; which is one of the systems authorized by the French framework regarding the access to online gambling. More generally, depending on the scenario studied, the verification can be minimal, involving only the transmission of a photo analyzed visually. On the contrary, it can represent a greater degree of certainty via video recording of the identity document from several angles then analyzed by software, as is the case in some customer identity verification systems for establishing remote banking relationships in France[239]. In any case, the mere transmission of an identity document and the verification of its authenticity is not sufficient to prove that the user who transmitted it is its rightful owner. Another verification process must therefore be added to the first: receiving a code at home for example, as is the case in the aforementioned example of the access to online gambling or using facial recognition technology.

Another common example of a verification system in this category is the use of credit cards. Although they are not explicitly identity documents, their use is based on the principle that they are held by adults whose age and identity have necessarily been verified by a banking establishment beforehand. But here too,

[236] ARCOM framework on access to pornography, (2024), *op. cit.,* p. 12.

[237] Renaissance Numérique, *Age assurance online…,* (2022), *op. cit.,* p. 26.

[238] EDRi, *Position paper Online age verification…,* (2023), *op. cit.,* p. 16.

[239] In application of the article R561-5-1 of the French Monetary and Financial Code.

it is appropriate for the entity that would like to use an age verification system based on the possession of a credit card to ensure that the card really belongs to the user who claims it. The user can thus be asked to trigger a payment, for a zero sum or reimbursed subsequently, which should normally be validated by a SCA (*strong customer authentication*) process provided for in the Revised Payment Services Directive (PSD2)[240]. This process can normally only be validated by actual card holders, since it requires them to verify with their bank two elements from two distinct categories among the following: something that they ”*know”* (such as a personal secret code), something that they “*possess*” (such as validating the operation from their smartphone, which they have certified to be their own beforehand) or a proof they *“are*” (such as the verification of a biometric element such as one's fingerprint, iris or face)[241].

3) Limits

Despite their theoretical reliability, these systems can raise major problems. First, sending copies of official documents online can represent security and data privacy risks. In certain situations, relating to online age verification, the CNIL has thus considered “*as contrary to the rules relating to data protection the collection of official identity documents, taking into account the specific issues attached to these documents and the risk of identity theft linked to their disclosure and misappropriation*”[242]. Even if these documents are processed securely and proportionately[243], the quality of the user journey can be compromised, in particular due to the delays required for manual verification or automatic analysis of the needed documents. In addition, even when supplemented by the receipt of a home code, these systems do not always

[240] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, art. 4.30.

[241] *I.e.* the categories *“knowledge”, “possession”* and “*inherence*” in the sense of PSD2 art. 4.30.

[242] “*comme contraire aux règles relatives à la protection des données la collecte de justificatifs d’identité officiels, compte tenu des enjeux spécifiques attachés à ces documents et du risque d’usurpation d’identité lié à leur divulgation et détournement”,* CNIL, deliberation 2021-069 of 3 June 2021.

[243] The French government has notably proposed a service for providing “single-use” proof of identity in order to limit the risks of identity theft. See the service *Single-use proof of identity (“ Le justificatif d’identité à usage unique*“) on its web site https://france-identite.gouv.fr/justificatif/ , accessed on 1 December 2024.

make it possible to fully ensure that the document presented really belongs to the person making the request. The situation is worse when it comes to presenting a credit card. Certain banks have, for a time, limited the SCA system to the simple receipt of a code by SMS[244]. But it can be viewed without unlocking the smartphone. Moreover, this method is based on a questionable premise since it is legally possible for a minor to possess and use a credit card in their name[245]. Although aware of this limit but considering that systems based on the use of a credit card can constitute "*an initial method of filtering out some of the minors*", ARCOM authorizes this type of system for a transitional period of three months in its framework on access to pornography[246].

Even this second category can have limitations depending on the exact system studied, it remains more relevant than declarative verification systems. The final chapter of this study will analyze the potential of verification systems aimed primarily at sharing information falling into this category.

C. Estimated

1) General concept

"Solution based on age estimation"[247], "*estimation*"[248], "*age estimation*"[249], *"age estimation techniques"*[250]; the terms used to mention systems falling into the third category generally use almost identical vocabulary but sometimes mention the technology used via other formulations such as "*algorithmic estimation*"[251] or

[244] Short Message Service.

[245] see the different ages from which it is possible to hold a credit card in the different EU Member States on the European Union Agency for Fundamental Rights website https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/issuance-credit-card , accessed on 1 December 2024.

[246] ARCOM framework on access to pornography, (2024), *op. cit.,* p. 20.

[247] ARCOM framework on access to pornography, (2024), *op. cit.,* p.18.

[248] Renaissance Numérique, *Age assurance online…,* (2022), *op. cit.,* p. 26.

[249] EDRi, *Position paper Online age verification…,* (2023), *op. cit.,* p. 15.

[250] Forbrukerrådet, *COMMERCIAL EXPLOITATION OF CHILDREN…*, (2024), *op. cit.,* p. 35.

[251] PEReN, *Online underage users detection…*, (2022), *op. cit.,* p. 6.

more directly "*artificial intelligence*"[252]. Except for this detail, all these terms cover systems capable of determining the probability that a user is an adult or not by using certain of their data. These data may or may not be actively provided by the user, but they are in any case not certified by a state entity at the end of the chain as is the case in the previous category.

2) Examples

These systems are generally based on artificial intelligence (AI) technology. A first example is the use of facial analysis of an individual in order to determine their age based on facial features, from a photo or a video recording. An emblematic example in this regard in France is that of the terminals tested by the French betting company *La Française des Jeux (FDJ)* at certain tobacconists in order to estimate the age of customers[253]. This technology, however, is to this day not used alone for remote age verification. A second example, theoretical but also not used alone in practice in terms of remote age verification, is an age estimation established from behavioral data such as browsing history, as is particularly the case in terms of profiling on social networks or via a conversational agent[254]. Another example is that of *Instagram*, testing various methods of age verification around the world, combining both certified proofs, in association with other proofs, of an estimated nature, via the use of AI on biometric or behavioral data[255].

---

[252] CNIL on its website, page *Recommendation 7…,* (2021), *op. cit.*

[253] Le Parisien news website, *An AI capable of estimating your age? FDJ tests the device in tobacconists to keep out minors ("Une IA capable d'estimer votre âge ? La FDJ teste le dispositif chez des buralistes pour écarter les mineurs")*, 6 april 2023, https://www.leparisien.fr/high-tech/une-ia-capable-destimer-votre-age-la-fdj-teste-le-dispositif-chez-des-buralistes-pour-ecarter-les-mineurs-06-04-2023-VALETOLKFFA7XIK5IUPJE4LUIY.php , accessed on 1 December 2024.

[254] McConvey J. R. on Biometric Update.com news website, *ChatGPT can recognize 'facial identities,' perform age estimation: research, 8 October 2024,* https://www.biometricupdate.com/202410/chatgpt-can-recognize-facial-identities-perform-age-estimation-research , accessed on 1 December 2024.

[255] Meta's news, *Introducing New Ways to Verify Age on Instagram,* 23 June 2022, https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/ , accessed on 1 December 2024, via the service provider "Yoti", also used by the FDJ.

3) Limits

Despite their potential, these systems raise significant legal, ethical and technical issues[256]. Their reliability remains variable depending on the exact technology used, as expressed by the CNIL regarding the use of navigation data for accessing pornographic sites[257]. They can also involve significant risks of discrimination and racial bias[258]. Furthermore, from a legal point of view, if an entity, which conditions access to its services on age verification, wishes to offer a verification system based on the processing of biometric data, it then has to offer at least one other system that is not based on such data[259]. Taking these elements into account, the ARCOM standard does not strictly oppose the use of an age estimation system but first requires it to be "*configured in such a way as to exclude the risk of a minor user being considered as being an adult ('false positives')*"[260] and to include a "*mechanism for recognizing living persons*"[261], so as to avoid circumvention by pre-recorded videos. Furthermore, the authority requires that at least two different methods of generating age proof are offered to users for one specific system it prescribes[262].

II - Typology Based on Proof Transmission Architecture

Another classification of online age verification systems is relevant with respect to the issues raised in the first part of this study. In this second classification, the aim is to study age verification from the angle of the data sharing it involves,

---

[256] Eynard J., *Online Age verification: AI as a solution?*, in: Artificial Intelligence Law : between sectoral rules and comprehensive regime comparative law, Castets-Renard C. and Eynard J. (eds.), Bruylant, 2023.

[257] CNIL, Deliberation no. 2021-069, *op. cit.*

[258] Stardust Z. et al., *Mandatory age verification for pornography access: Why it can't and won't 'save the children', B*ig Data & Society, 11(2), June 2024.

[259] See in particular the case law of the French *Conseil d'Etat* about identity verification, Decision no 432656 ECLI:FR:CECHR:2020:432656.20201104, 4 November 2020, indirectly reaffirmed by the CNIL regarding access to pornography in its delibération n° 2021-069, *op. cit.*

[260] ARCOM framework on access to pornography, (2024), *op. cit.,* p. 11.

[261] *Ibid.,* p. 12.

[262] *Ibid.,* p. 18, explicitly mentioning as an example, systems based on identity documents in addition to systems based on age estimation. However, this specification only applies to double anonymity systems, which will be described in more detail in the next section.

and incidentally from the angle of the stakeholders involved in the verification process. In theory, the three types of proof detailed earlier can circulate in the different sharing architectures detailed below. But in practice, the general lack of relevance of using self-declaration systems further encourages us to consider these architectures in order to share certified and possibly estimated proofs of age. The three types of architectures detailed below are distinguished according to: the absence of a third-party verifier (A), the presence of a third-party verifier (B), and the presence of a third-party verifier as well as an intermediary (C) in the age verification system.

A. Bilateral Verification Architecture

1) General concept

The first architecture involves the *"user"*[263], *i.e.* the person who wishes to access a service and for whom the age will need to be verified, and only one[264] entity in front, the *"entity requesting the verification"* that provides the desired service[265]. The entity requesting the verification may be legally obliged to verify age, as is the case with access to online betting games in France, or do so on a more voluntary basis, as part of risk mitigation measures for example, as it is the case for certain DSA measures. In all these cases, when the user requests access to the desired services, the entity requesting the verification then asks the user to provide an age proof. The proof is transmitted directly from the user to the entity requesting the verification, which then takes care of checking it itself. If the verification phase confirms that the user exceeds a certain age threshold, the entity requesting the verification provides access to the service initially requested by the user.

[263] Who is therefore also considered to be a data subject within the meaning of the GDPR, (2016), *op. cit.*

[264] Apart from the data subject, each entity mentioned in this section II may, as a data controller within the meaning of the GDPR, (2016), *op. cit.*, use the services of data processors to carry out all or part of their processing. Although a data processor is normally legally distinct from the data controller, distinguishing them in the context of this study of age verification architectures would only complicate the discussion without providing any useful elements for distinguishing the three architectures. Thus, for the sake of intelligibility, only entities having the quality of data controller, therefore fixing the purposes and means of processing will be distinguished subsequently.

[265] Or sells the desired products.

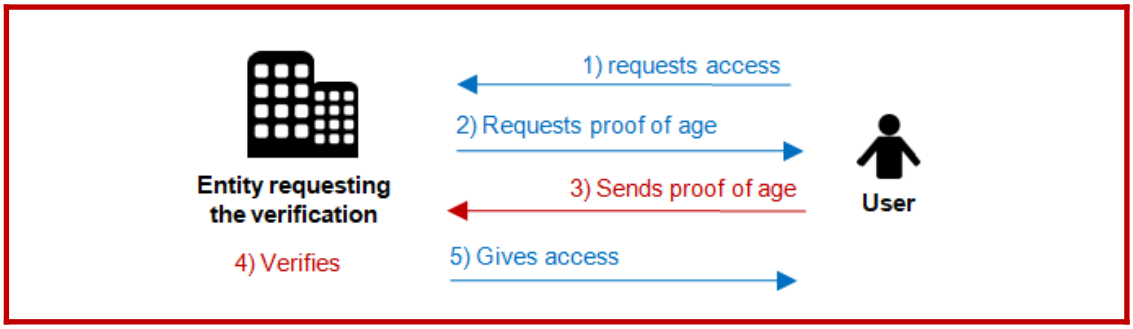

Fig. 1: Diagram representing a bilateral verification architecture (with general actions in blue and actions on age proof in red)

2) Details: opportunities, limits and future

This first architecture has the advantage of potentially being the simplest to implement for the entity requesting the verification, in that it does not require relying on other entities and thus allows the entity to stay in control of the entire verification process. However, it has three major limitations.

The first one is linked to the notion of "*further processing*". The GDPR strictly regulates the reuse of data for different purposes than those for which they were initially collected. It normally requires the data controller to ensure that both purposes, the initial one and a later one, are compatible[266]. If the two purposes are not compatible, the data controller cannot freely reuse the data, and must, for example, obtain the data subject's consent, for the second processing operation it intends to carry out with the data already in its possession. This legal rule, which relies on a subjective evaluation of compatibility, is not always perfectly respected. It remains that, on a technical level, a system built on a bilateral architecture theoretically allows the entity requesting the verification to reuse the data, initially collected for age verification, for another purpose as part of its service, and whose compatibility could be questionable or completely non-existent. Information on the user's age or identity could thus be illegally reused for profiling purposes, and in particular for commercial purposes.

Beyond such a hypothesis of possible abusive behavior by certain entities requesting verification, a second limitation results from the sole fact that the

[266] GDPR, (2016), *op. cit.,* art. 6.4.

data is centralized within a single entity, therefore accentuating the seriousness of the risks in terms of cybersecurity. If obligations for the data controller in matters of security also exist through the GDPR[267], the recent wave of hacking of telecommunications operators in France[268] shows that no company is safe from cyberattacks. The hacking incident resulted in the public disclosure of customer information on the internet, including international bank account numbers (IBAN) and e-mail addresses, thereby indirectly revealing the individuals' status as customers of specific telecommunications operators. Beyond the associated phishing risks, the implications would be even more serious if websites requiring age verification, such as pornographic platforms, were to be similarly compromised, given the private and potentially stigmatizing nature of the information that could be exposed.

A final risk applies even when the entity requesting the verification manifests its good faith, and when the hypothesis of any unauthorized access is not at stake. As part of its obligations under the GDPR, the entity requesting the verification has to select a legal basis and determine the means of its processing[269]. In the case of a verification obligation that specifies the verification system to be put in place, as is the case for online gaming sites in France, the data controller can in principle justify its processing on the legal basis of compliance with a legal obligation[270]. But when the legal framework requiring age verification does not precisely specify the modalities, or when the age verification is not explicitly required but only strongly recommended, as in the context of certain DSA measures, the choice of a legal basis is more complicated for the data controller. It is then still possible to justify the processing via the legal basis of the legitimate interests[271]. But it requires the data controller to conduct a

[267] *Ibid.*, art. 5.1.f) and 32.

[268] See Mediavilla L. for Le Figaro, *Free, SFR... Telecoms operators caught in the wave of cyber attacks* ("*Free, SFR… Les opérateurs télécoms pris dans la vague des cyberattaques*"), 26 October 2024, https://www.lefigaro.fr/secteur/high-tech/free-cible-par-une-cyberattaque-impliquant-un-vol-de-donnees-personnelles-de-clients-20241026 , accessed 1 December 2024.

[269] Even if it is also applicable for the other architectures, it is more sensitive in the case of a bilateral verification architecture due to the existence of the two aforementioned risks.

[270] GDPR, (2016), *op. cit.,* art. 6.1.c).

[271] *Ibid.,* art. 6.1.f).

balancing exercise between fundamental rights, freedoms and interests at stake, to ensure that the means of its processing are appropriate in relation to the purpose of processing, even though this purpose of processing was not decided by the data controller. If the means of processing are considered too intrusive, they will be objectionable under the data protection framework. Conversely, insufficient means of processing limiting the effectiveness of the age verification system, may also be criticized under the regulations mentioning the verification. This results in potential legal uncertainty for the entity requesting the verification[272].

This first architecture is used for certain older verification scenarios such as access to online gambling in France[273]. However, it is likely that it does not represent the future of online age verification systems. Public authorities currently seem to be encouraging the use of other verification architectures, or even sometimes directly requiring them, as illustrated by the ARCOM framework on access to pornography[274], thus indirectly prohibiting the use of bilateral architectures.

B. Third-Party Verification Architecture

1) General concept

The second architecture involves two independent entities[275] interacting with the user. When the users request access to the service of an entity who wishes to ensure that he or she exceeds a certain age threshold (still the entity "*requesting the verification"),* this entity will ask another entity, a "*third-party verifier*", to verify that this threshold has been exceeded. The third-party

[272] See the EDPB, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR),* 2 August 2023, and its analysis by Radtke T., *Mandatory Age Verification for Online Services under GDPR — The protection of children according to data protection law in the light of EDPB's Binding Decision regarding TikTok,* Computer Law Review International, vol. 24, no. 6, 2023, p. 161-168.

[273] When the use of a remote verification system is not possible, see part I, chap. 1, II of this study.

[274] ARCOM framework on access to pornography, (2024), *op. cit.*

[275] In this subsection, the third-party verifier is independent from the entity requesting the verification: it is not its data processor within the meaning of the GDPR, (2016), *op. cit.*. If this were not the case, the resulting architecture would not be the one currently studied, but rather the bilateral architecture of the previous sub-section.

verifier will ask the user to send proof of his or her age which it will verify[276]. Once the verification has been carried out, the third-party verifier will inform the entity requesting the verification whether access can be given to the user or not.

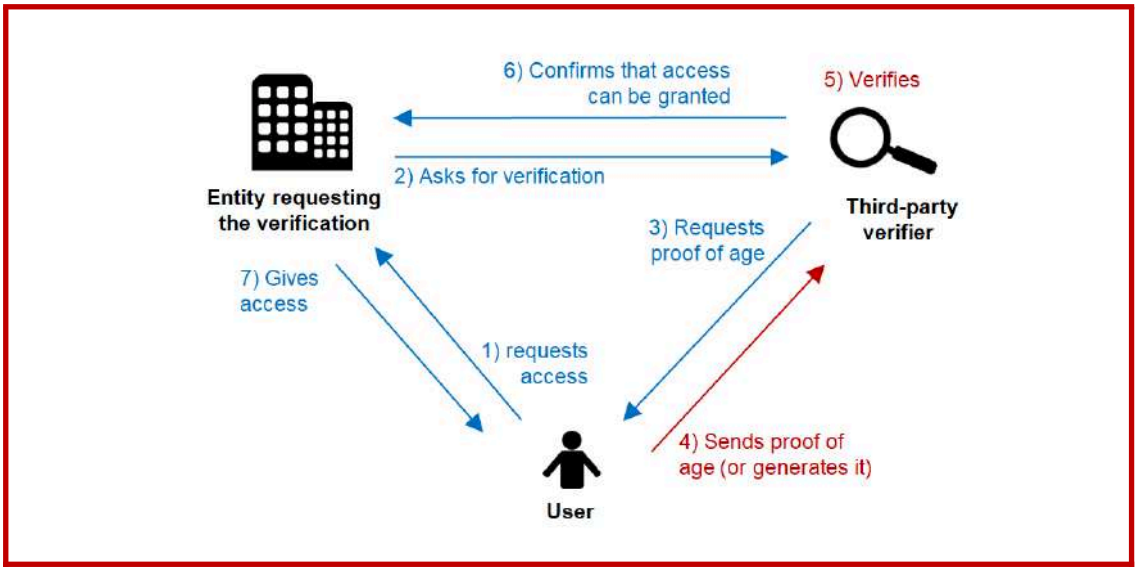

Fig. 2: Diagram representing a third-party verification architecture (with general actions in blue and actions on age proof in red if ZKP compliant)

2) Details: opportunities, limits and future

After verifying the age of the user, the third-party verifier could transmit the age information to the entity requesting the verification. It is, however, also possible that the third-party verifier just informs the entity requesting the verification whether or not the user exceeds the age limit, but without providing the exact age. In this second case, the age verification system follows a protocol called *"zero-knowledge proof*" (ZKP), where zero information is shared apart from confirmation of whether or not the age is exceeded. The aforementioned risk of the abusive reuse of the user's age by the entity requesting the verification thus disappears, since the latter does not have access to this information. The risks of legal uncertainty in determining the means of processing is also reduced for the entity requesting the verification since this architecture poses fewer risks to it.

[276] Or to generate it, depending in particular on whether the third-party verifier bases his system on a nature of proof such as certification (studied in part II, chap. 1, I, B) or estimation (studied in part II, chap. 1, I, C).

This situation should not, however, lead one to believe that the predominant risks detailed for the bilateral architecture disappear in this architecture with a third-party verifier. They are actually shifted away from the entity requesting the verification, to the third-party verifier. Indeed, the third-party verifier concentrates information on the user's age and on the service requested. The risks of further processing from the *third-party verifier* seem less likely, especially when the latter does not offer other services to users other than verifying their age. However, this risk is not entirely absent, as in the case of bilateral architecture, cybersecurity risks are also concentrated on a single entity here.

This second architecture reduces some limitations of the first but does not completely eliminate them. It could constitute the minimum basis for online age verification in the future. Already used, theoretically as a general rule, for age verification in terms of access to online gambling in France, this architecture constitutes the "*minimum requirements for all age verification systems*"[277] of the ARCOM framework on access to pornography. A final type of architecture, however, makes it possible to further reduce the aforementioned risks.

C. *"Double Anonymity"* Verification Architecture

1) General concept

The third architecture involves three independent entities in addition to the user. The entity requesting the verification and the third-party verifier are always present, but only communicate through another third party, which then constitutes an *"intermediary"*. This way, the entity requesting the verification does not know from whom the information initially originates regarding exceeding the necessary age threshold. The third-party verifier, on its side, does not know which service will be consulted by the user. This results in a form of anonymity between these two entities, thus giving its name to this architecture[278]. The verification process begins with the user requesting access

[277] ARCOM framework on access to pornography, (2024), *op. cit.,* p. 15-17.

[278] "Double anonymity*" (*"double anonymat"*)* sometimes also called "Double confidentiality" *("double confidentialité")*, see ARCOM framework on access to pornography, (2024), *op. cit.*, p. 14.

to a service that requests a verification. This entity sends a verification request to the intermediary, which then transmits the request to the third-party verifier. The latter asks the user to generate or provide an age proof. Once the verification has been carried out by the third-party verifier, this entity sends the response to the intermediary, possibly via a ZKP compliant method. The intermediary then informs the entity requesting the verification that access can be granted or not, and the access is finally granted or not, by the entity requesting the verification, to the user.

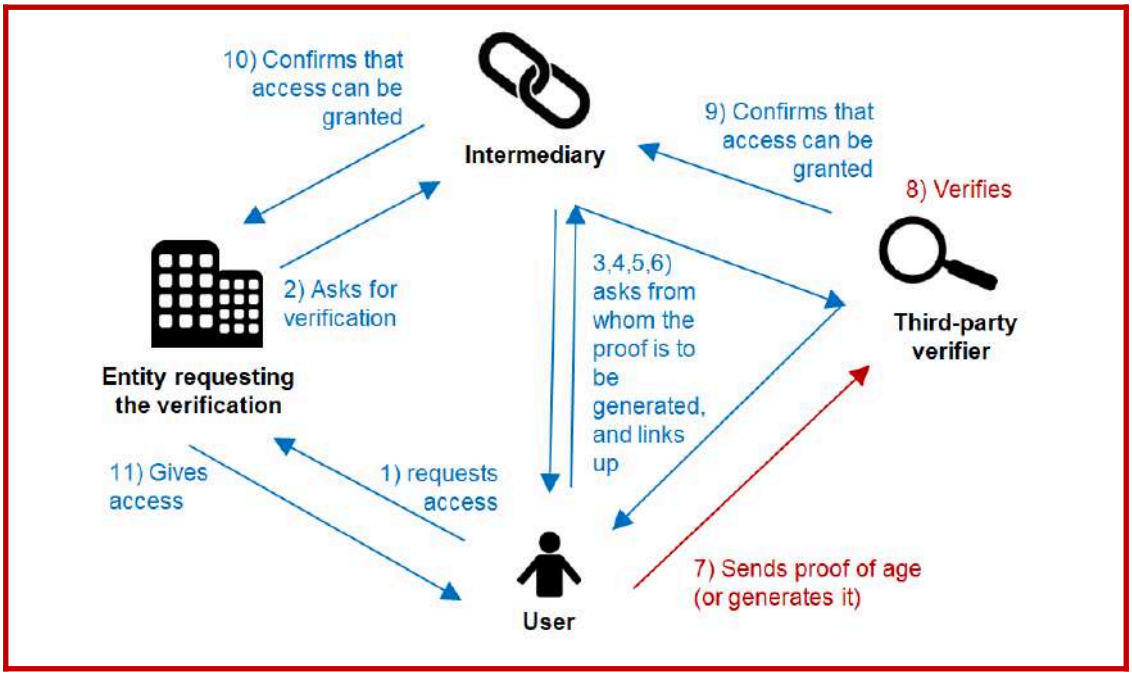

Fig. 3: Diagram representing a double anonymity verification architecture (with general actions in blue and actions on age proof in red if ZKP compliant)

2) Details: opportunities, limits and future

The double anonymity architecture limits the aforementioned risks in terms of data protection and cybersecurity. In fact, the entity requesting the verification is in the same situation as third-party verifier architecture, since the architecture in double anonymity can also respect the ZKP protocol. While the risks were associated with the third-party verifier in the second architecture, in the double anonymity architecture this entity is not aware of the service consulted, and therefore cannot use this information, or reveal it unintentionally if it were hacked. Only residual risks are then shifted on the intermediary's side. They are only residual because the intermediary has, of course, knowledge of the service

consulted; but it only knows whether or not the user exceeds an age threshold, and not their exact age or their identity if the system respects a ZKP protocol. The risk of data reuse or hacking of this data therefore seems less serious than in the hypotheses formulated in the first two architectures.

This architecture has been the subject of in-depth reflection on the part of public authorities in France, in particular through the LINC (the CNIL Digital Innovation Laboratory)[279]. Optional specificities can be added to the broad outlines of this architecture, such as cryptographic measures, by making the user the direct intermediary of the system[280], or even by basing the system on blockchain technology. This presence of an intermediary could also be conceptually compared to other notions also calling for a form of intermediation. This is the case of "*data intermediation services providers*", dedicated at the EU level through the 2022 *Data Governance Act (DGA)*[281], which are subject to neutrality obligations[282] and may include storage services for user data such as age[283] or even anonymization and pseudonymization of data[284]. This idea of independent and neutral third parties in the digital ecosystem is reminiscent of the Anglo-Saxon concept of "*data trusts*" or "*data fiduciaries"* aimed at strengthening the protection of user privacy[285]. In this sense, the architecture with double anonymity could represent, despite its organizational complexity and its potential implementation cost, the future of online age verification. In its framework on access to pornography, the ARCOM requires the equivalent of

---

[279] Gorin J., Biéri M. and Brocas C., *Demonstration of a privacy-preserving age verification process* webpage, 22 June 2022, https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process , accessed 1 December 2024, popularizing the work of the Digital Innovation Laboratory of the CNIL (Laboratoire de l'innovation numérique de la CNIL - LINC), Blazy O. and the PEReN.

[280] Included in the desirable objectives and good practices of the ARCOM framework on access to pornography, (2024), *op. cit.*, p. 19.

[281] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), chap. III.

[282] *Ibid.,* art. 12.

[283] *Ibid.,* whereas 30.

[284] *Ibid.,* art. 12.e).

[285] See more generally the concept of *fiduciary mode*l applied to the digital environment via Balkin J. M., *The fiduciary model of privacy,* Harvard Law Review Forum, Vol. 134, no. 1, november 2020.

our entity requesting the verification, to offer its users at least one verification system respecting the architecture in double anonymity, for which the authority then provides specific measures[286].

Chapter 1 Summary

Two typologies allow us to assess the relevance of an online age verification system with regard to some of the challenges mentioned in the first part of this study. The first typology distinguishes age verification systems into three different types based on the nature of the age proof. Age proofs generated on a declarative basis by the user appear to be of little relevance to efficiently protect minors. Age proofs generated from certified information that are then verified seem more appropriate, although they may involve risks and constraints for the user in terms of user experience depending on the exact detail of the verification system studied. Finally, age proofs generated on an estimated basis seem intrusive in terms of data protection and privacy. This distinction according to the nature of the proof is therefore not sufficient on its own because the risks and the effectiveness of the system actually depend on the details of the age verification system[287], especially considering the fact that a given verification system may in reality include several proofs of different nature.

It is therefore useful to combine it with a second typology of online age verification systems. The second typology focuses on the "*architecture*" of the verification, *i.e.* how the proof of age is shared, and which stakeholders are involved in the process. The first architecture, the bilateral one, only includes the user and the entity requesting the verification, which itself takes care of the verification. In this configuration, the risks are all the greater because they are concentrated on the entity requesting the verification. A third-party verifier is added to the verification process in the second architecture. This architecture

[286] ARCOM framework on access to pornography, (2024), *op. cit.,* requirements 6 to 10.

[287] For more details and deep analysis of different systems, see the assessment made by Sas M. and Mühlberg J. T., *TRUSTWORTHY AGE ASSURANCE? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective*, 2024.

makes it possible to respect a ZKP protocol, *i.e.* not to directly disclose the age or identity of the user to the entity requesting the verification. Although reduced, the risks are nevertheless shifted to the third-party verifier's side. Finally, an intermediary is added in the third architecture between the entity requesting the verification and the third-party verifier, creating a *"double anonymity"* of one with respect to the other. The risks are once again shifted, to the intermediary's side this time, but may only be residual if the system respects a ZKP protocol.

Certain old age verification scenarios still call for verification systems of a declarative nature or bilateral architecture to this day. The positioning of public authorities, and more explicitly of the ARCOM framework on access to pornography, nevertheless allow us to estimate that the future of identification verification systems will rather turn towards age proofs of a certified nature, while leaving, however, the door open to proofs of an estimated nature despite the greatest limits they entail to this day. They will also be oriented towards architecture including at least a third-party verifier and ideally relying on a double anonymity since they both allow respect for a ZKP protocol, and despite the organizational constraints they could imply.

Although some of the challenges identified in the first part of this study have been addressed in this chapter, some of them cannot be directly assessed through our two typologies. In order to address these last major challenges, but also to illustrate this first chapter, we will examine, in the last chapter of this study, systems initiated by public authorities which could constitute relevant solutions for online age verification.

Chapter 2: Analysis of the Digital Identity Framework as a Potential Future EU Age Verification System

The first part of this study made it possible to identify a strong link between age verification and the broader verification of a person's identity. In this regard, a European framework exists on the notion of "*digital identity*" (eID). This framework is currently experiencing a significant legal update. This final chapter therefore first proposes to examine the current situation, resulting largely from the framework established by the 2014 eIDAS regulation[288] (I), before detailing the current developments aimed at implementing the 2024 revision of the eIDAS regulation (eIDAS 2.0)[289] (II), explaining for each their link with age verification.

I - The eIDAS Electronic Identification Scheme for Age Verification

A. eIDAS' Legal Framework

The ambition of the 2014 eIDAS regulation is to strengthen trust in digital transactions and promote the digital single market. To this end, it establishes a legal framework on "*trust services*"[290] such as "*electronic signatures*" or "*electronic time stamps*" on the one hand, and on "*electronic identification scheme*"[291] on the other hand. This section focuses only on the latter. The regulation considers these electronic identification schemes as systems within which electronic identification means[292] are issued. These electronic identification means allow users to identify and authenticate themselves to

[288] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[289] eIDAS 2.0, (2024), *op. cit.*

[290] eIDAS, (2014), *op. cit.,* art. 3.16.

[291] *Ibid.,* art. 3.4.

[292] The term "*electronic identification scheme"* from eIDAS, (2014), *op. cit.,* art. 3.4, therefore covers the "*electronic identification means",* but also the suppliers of this identification means, the technical protocols, governance rules, *etc*. The electronic identification means alone represent the concrete solution that a user uses to prove its identity within the framework of a scheme.

access online services[293]. These infrastructures were established in order to offer an alternative to bilateral verification architectures[294], as the electronic identification schemes and means rely on third-party or double anonymity architecture. In addition to limiting the risks mentioned in the previous chapter, such a system makes it possible to optimize user experience by allowing users to identify themselves on many different services with the same identification data and thus spares users from having to remember all the passwords for all the services they want to access. The aim of the regulation was to enable these systems to be used across borders in the EU. It provides the framework for any Member State that wishes to do so to be able to notify its own electronic identification scheme at the EU level. When such a notification occurs it is then recognized by the other Member States and citizens of the Member State that notified the system can theoretically use their national identifiers to access online services from the other Member States[295].

In order to be eligible for such notification and recognition across the EU, national electronic identification schemes must respect certain elements. eIDAS notably provides for security requirements, by setting three "assurances levels": "*low*", "*substantial*" *and* "*high*"[296]. Without diving into the technical details of each level[297], only the electronic identification scheme at substantial or high assurance levels can be notified. It should be pointed out that the security requirements of these two levels indirectly enable compliance with the

[293] eIDAS, (2014), *op. cit.,* distinguishing the "electronic identification" in art. 3.1 (when the user uses a "*person identification data*") of the "authentication" phase in art. 3.5 (during which the identification is *"confirmed"*). For the sake of intelligibility, the distinction will not be strictly made hereafter.

[294] Part II, chap. 1, II, A of this study.

[295] eIDAS, (2014), *op. cit.,* notably art. 6, 7 and 9.

[296] *Ibid.,* notably art. 8.

[297] Laid down in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

requirements under PSD2 for SCA mentioned in the previous chapter for the use of bank cards[298].

B. French Implementation

Because eIDAS relies on voluntary notification of *electronic identification schemes*, not all Member States have adopted such a system, or have done so recently[299]. France has started to develop an eIDAS-compliant system through the launch of *"FranceConnect"*[300] in 2016. This system alone does not constitute an electronic identification scheme in itself. It is an "*identity federation"* (comparable to our intermediary under the prism of the verification architectures studied in the previous chapter) allowing the user to select an "*eID provider"* of his or her choice (comparable to our third-party verifier) to authenticate to a given "service provider" (comparable to our entity requesting the verification). The architecture is therefore highly comparable to an architecture featuring double anonymity studied in the previous chapter, since neither the service provider, nor eID provider are aware of each other. However, the system does not rely on a ZKP protocol as the eID provider provides FranceConnect numerous pieces of information about the user's identity which is then verified by FranceConnect before a public body, the French national directory for the identification of natural persons *("Répertoire national d'identification des personnes physiques" - RNIPP)*[301]. After this verification, FranceConnect

[298] See in part II, chap. 1, I, B of this study, the example of age verification using a bank card, requiring such SCA. Both procedures require two elements from different categories among the following three, knowledge, possession, inherence. But beware, the inverse is not always true. The only respect for a SCA within the meaning of PSD2, (2015), *op. cit.* does not necessarily ensure compliance with all the requirements requested for the assurances levels substantial high in the sense of eIDAS (2014), *op. cit.*

[299] See the progress record for each Member State on the European Commission website, https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS , accessed on 1 December 2024.

[300] See the presentation of FranceConnect on its official website https://franceconnect.gouv.fr/ , accessed on 1 December 2024. To be precise, the solution is now split between " *FranceConnect*" for systems with an assurances level low and " *FranceConnect+* " for systems with assurances levels substantial or high . This distinction will not be made later as it is not useful for the discussion.

[301] The national directory for the identification of natural persons includes the civil status of 113 million people who were born or have lived in France. Each person is assigned an identification number ALSO known as the *'social security number'.*

transfers the data to the service provider, with a unique user identifier specially created for this service provider.

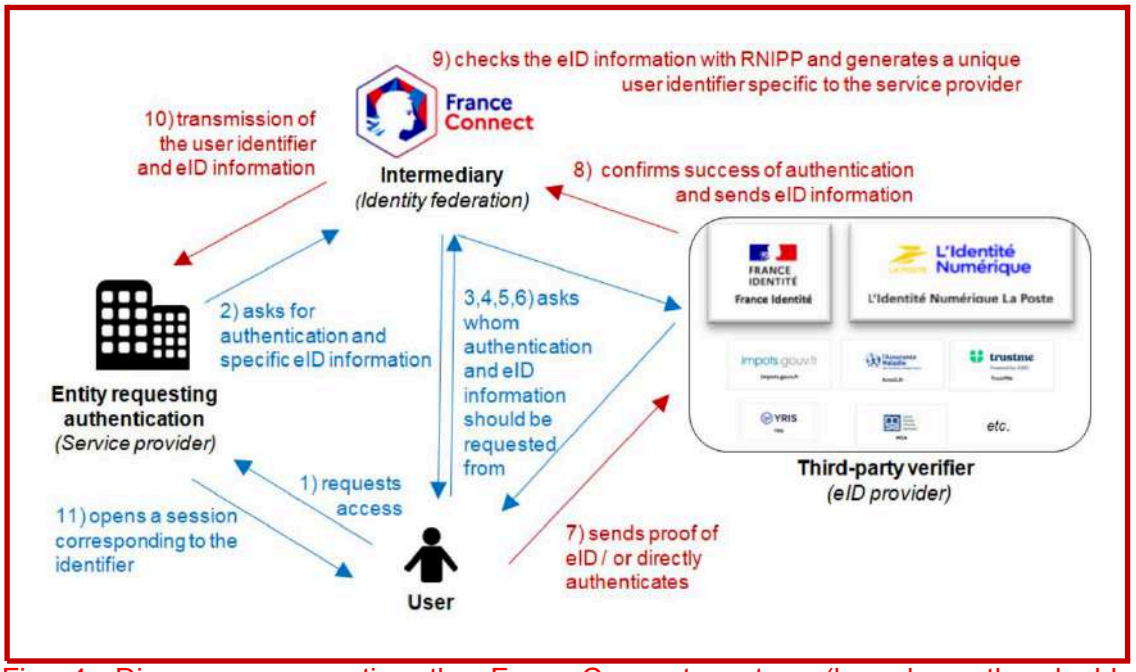

Fig. 4: Diagram representing the FranceConnect system (based on the double anonymity architecture model from fig.3 with general actions in blue and actions on eID information/age proof in red, as non-ZKP compliant)

Two of the eID providers proposed by FranceConnect have been notified at the EU level in order to be recognized by the other Member States: "*The Digital Identity La Poste"* in 2021[302], and more recently *"France Identité"* in 2024[303].

C. Use as an Age Verification System

The date of birth, and more generally the age, is recognized as one of the essential attributes of an individual's identity[304]. It is therefore legitimate to consider the use of such electronic identification schemes to respond to age verification scenarios. In this regard, although principally aimed at accessing public services, the application of the eIDAS framework in France has gradually

[302] Notified at the EU level under the name *"French eID scheme "FranceConnect+ / The Digital Identity La Poste"* on 2 February 2021, and validated on 27 September 2021.

[303] Notified at the EU level on 24 April 2024, and validated on 9 September 2024.

[304] CNIL, *Thematic file - Digital identity,* (2023), *op. cit.*, p.11.

opened up to private services. The French Monetary and Financial Code has notably recognized the possibility for banks to use an electronic identification scheme notified at the EU level[305] for remote customer onboarding. Since no system was notified at the EU level before 2021, the French legislator left other options for remote customer onboarding by commissioning the French national agency for information systems security ("*agence nationale de la sécurité des systèmes d'information"* - ANSSI)[306] to certify *"remote identity verification services providers*" ("*prestataires de vérification d'identité à distance"* - PVID)[307] on the basis of a national standard[308] which explicitly refers to the eIDAS substantial and high assurance levels[309]. As mentioned in the first part of this study[310], the same two options, of an electronic identification scheme notified at the EU level or a PVID, are provided by the French legislator in terms of age verification for access to online gambling, by referring to the same article of the French Monetary and Financial Code[311].

Going beyond the French framework, it is also possible to mention the "*euCONSENT*"[312] initiative, a non-governmental organization aiming to offer online age verification systems based on the infrastructures adopted under eIDAS. Still in the pilot stage, the project aims simultaneously to offer parental control solutions.

---

[305] French Monetary and Financial Code, art. R. 561-5-1.1°.a).

[306] France, Decree n°2021-387 of 2 April 2021, art. 1, modifying article R561-5-1 of the Monetary and Financial Code.

[307]The certified PVID are listed on the ANSSI website, https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid , accessed on 1 December 2024.

[308] ANSSI, *Remote identity verification service providers - Requirements rule set,* version 1.1 of 1 March 2021.

[309] *Ibid.*, I.1.1. and I.3.2.

[310] Part I, chap. 1, II of this study.

[311] Decree no. 2010-518, *op cit.,* art. 4.I, referring to 1° and 2° of article art. R. 561-5-1 of the Monetary and Financial Code.

[312] See their official website https://euconsent.eu/ , accessed on 1 December 2024 and the research they funded Hof S. van der *"We Take Your Word For It' — A Review of Methods of Age Verification and Parental Consent in Digital Services",* European Data Protection Law Review Volume 8, 2022, Issue 1 p. 61-72.

It is therefore not surprising to see the French government considering the establishment of *"public initiative solutions"* in terms of access to social networks for example[313]. However, it would be risky to claim that electronic identification schemes notified under eIDAS could constitute a system that perfectly meets all the challenges of age verification scenarios mentioned in the first part of this study. First, the use of such a system by public authorities, although supervised in their own use of the former, raises the question of the risks of abuse and diversion of its initial purposes for repressive purposes[314]. Furthermore, although such systems are used today in France by more than 40 million users[315], their establishment must take into account the risks of exclusion they entail, both in terms of general coverage of the population and more specific groups, such as foreign nationals in particular. Finally, these systems are not necessarily designed to respect a ZKP protocol. The service provider can then access numerous pieces of information about the user identity[316], which implies the same problems as in a bilateral verification architecture. The recent update of the eIDAS regulation could nevertheless reduce some of these risks.

---

[313]Meeting of 29 april 2024 of the French Secretary of State for Digital with stakeholders in age verification and representatives of large platform*s, NAR - Marina Ferrari will meet with age verification stakeholders and representatives of the major platforms at Bercy (NAR - Marina Ferrari recevra à Bercy les acteurs de la vérification d'âge et les représentants des grandes plateformes"*), press release no. 1808, 28 April 2024, as reported by Hue B. for RTL in the press article *Digital majority at 15: why the implementation of the measure defended by Macron promises to be difficult in Europe ("Majorité numérique à 15 ans : pourquoi la mise en place de la mesure défendue par Macron s'annonce difficile en Europe"),* 29 April 2024, https://www.rtl.fr/actu/sciences-tech/majorite-numerique-a-15-ans-pourquoi-la-mise-en-place-de-la-mesure-defendue-par-macron-s-annonce-difficile-en-europe-7900379346 , accessed on 1 December 2024. Even if the legal age verification regime for access to social networks is in reality not applicable, as explained in part I, chap. 1, III of this study.

[314] See EDRi (via By epicenter.works) webpage, *Orwell's Wallet: European electronic identity system leads us straight into surveillance capitalism,* 2 February 2022, https://edri.org/our-work/orwells-wallet-european-electronic-identity-system-leads-us-straight-into-surveillance-capitalism/ , accessed 1 December 2024.

[315] In June 2024, number drawn from official bodies on https://www.numerique.gouv.fr/actualites/franceconnect-franchit-le-cap-des-40-millions-de-citoyens-connectes-en-juin-2024/ , accessed on 1 December 2024.

[316] Far from the ZKP protocol or the precept of selective disclosure of information (allowing the user to only disclose the necessary information) recommended by the CNIL in its *Thematic file - Digital identity,* (2023), op. cit., p.11, and regarding ZKP, also in the best practices mentioned in the ARCOM framework on access to pornography, (2024), *op. cit.,* p. 19.

II - eIDAS 2.0's EDIW for Age Verification

A. eIDAS 2.0's Legal Framework

Several aspects of the eIDAS regulation have limited its effectiveness. The most important of them is the voluntary nature of the notification of electronic identification schemes by each Member State. The second is the orientation of the regulation, whose application has benefited public service access more, and not necessarily private services. The parallel development of private third-party identification systems by internet giants[317] to access other private services has pushed the European Commission to propose in 2021 a revision of the eIDAS regulation.

Finally adopted in 2024, eIDAS 2.0[318] retains the notification mechanism for electronic identification schemes. The great novelty it brings is the obligation for each Member State to set up one specific electronic identification means, in the form of a "*European Digital Identity Wallet*" (EDIW)[319]. The regulation only sets out the broad outlines of this system, which should notably allow users "*to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties*"[320]. These relying parties, i.e. the services to which the user wishes to access and requesting the latter to authenticate, may be public or private services. In order to ensure the democratization of EDIWs, eIDAS 2.0 even requires certain private entities to offer EDIW among the identification solutions offered to their users. The two scenarios targeted are, on the one hand, the very large online platforms defined by the DSA[321]. And on the other hand, the situations implying

---

[317] Such as *"Facebook Connect", "Google Sign-In",* or *"Sign in with Apple"* where these operators behave like private eID providers. As the eID verification systems are of a bilateral architecture (with regard to our analysis grid of part II, chap. 1, II, A), these operators are technically able to reuse connection information for other processing. This situation then raises questions of data protection, but also in terms of sovereignty. See CNIL, *Thematic file - Digital identity,* (2023), op. cit., p. 17.

[318] eIDAS 2.0, (2024), *op. cit.*

[319] Sometimes only referred to as EUDIW or DIW. *Ibid.,* art. 1.3.j.42 and 1.5.

[320] *Ibid.,* art. 1.3.j.42.

[321] *Ibid.,* whereas 57 and art.1.5.(art. 5f.3).

a "*strong user authentication*"[322], during which the EDIW will therefore constitute one of the solutions offered to the customer to validate the operation.

B. Current Implementation

eIDAS 2.0 is based on numerous implementing regulations to specify the architecture and technical modalities of the EDIW. Five of them[323] were adopted in December 2024 on the basis of the implementation preparation work that was done in parallel with the negotiation of the regulation[324]. Through a simplified description[325] of the functioning of the future EDIW, it is possible to distinguish several types of stakeholders. A first entity (the *"EDIW provider"*) will be mandated by each Member State to provide the software used by the user, such as a smartphone application. Another entity (the *"provider of person identification data*" - "*PID provider*") will also be mandated by each Member State to provide the user's person identification data, that is to say the essential

---

[322] *Ibid.,* art. 1.5.(art. 5f.2) and whereas 56. Although eIDAS 2.0, (2014), *op. cit.,* mentions the term of strong "*user"* authentication, it defines it in art. 1.3.j.51 in the same way as the strong "*customer*" authentication provided for in PSD2, (2015), *op. cit.,* art. 4.30 mentioned upstream as requiring at least two elements respectively from distinct categories between *"knowledge", "possession"* and "*inherence".*

[323] Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallet, Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem, Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets, and Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework.

[324] Since the publication of the initial proposal for the eIDAS 2.0 regulation, initiated by the European Commission with the publication on the same day of Commission *Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework,* C/2021/3968. Having taken shape in particular through the work of the eIDAS Expert Group (E03032).

[325] The details of the exact functioning of the EDIW are provided by both the eIDAS 2.0 regulation, (2014), *op. cit.*, and several implementing regulations. Many of the subtleties will not be mentioned in this description for the sake of clarity. For a more technical explanation, see the work on the *"European Digital Identity Wallet Architecture and Reference Framework" (ARF)* at the following webpage https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/ , accessed on 1 December 2024, and particularly "*Figure 1: Overview of the EUDI Wallet roles*" of which fig. 5 of this study was inspired.

data that constitute its identity[326]. Other entities of different natures (the *"providers of electronic attestations of attributes*") will be able to certify at different levels of trust other types of additional information relating to the user, such as diplomas, pay slips, *IBANs* or other bank account information, *etc.* All these pieces of information could then be transmitted if needed to the service the user wishes to access (the "*relying party"*). Other trusted bodies, not shown in the diagram below, will be integrated at different steps of the process to provide more security.

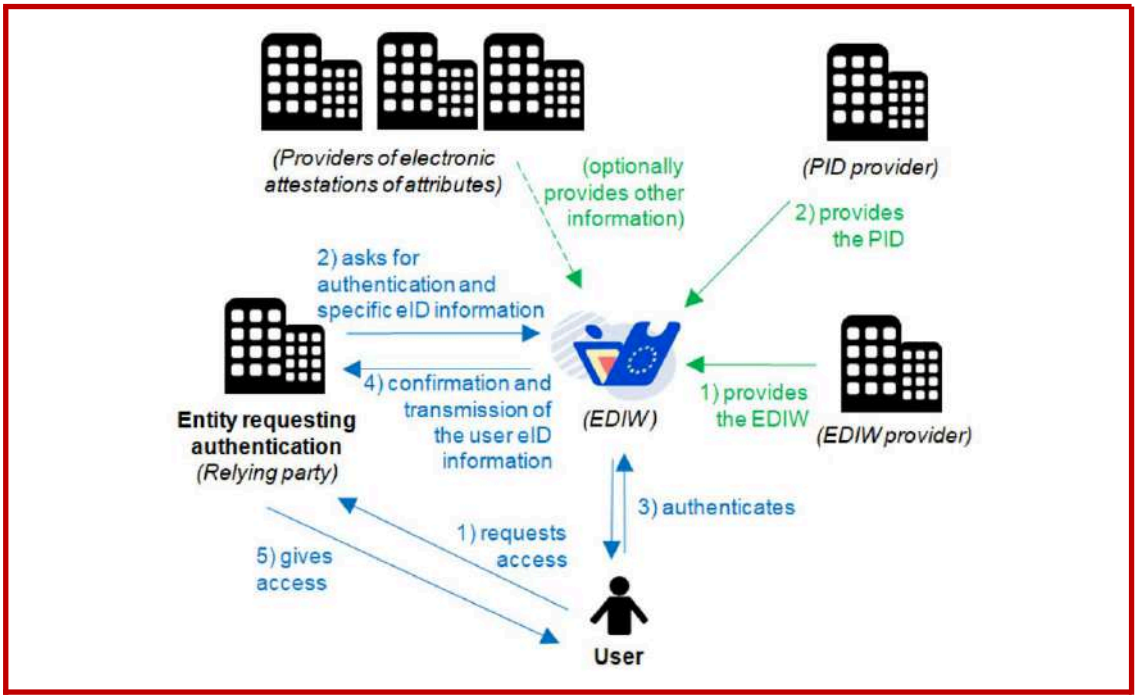

Fig. 5: Diagram representing the EDIW system (based on the double anonymity architecture model from fig.3, with the provision of the EDIW in green, and then the use of the EDIW to access an online service in blue)

C. Prospective Use as an Age Verification System

The eIDAS 2.0 regulation lists age as one of the user identity attributes[327]. But the link between the EDIW and age is also apparent in other layers of work that have been put in place by the European Commission to support the

[326] Listed in Commission Implementing Regulation (EU) 2024/2977, *op. cit.,* annex, 1, dividing them between mandatory data (such as first name, last name, date of birth, nationality) and optional data (such as address, gender, email, telephone number).

[327] eIDAS 2.0, (2024), *op. cit.,* annex VI, 2.

implementation of eIDAS 2.0. Indeed, the European Commission has encouraged the launch of several projects aimed at helping public and private organizations work together across the EU, including on potential uses that could be made freely with EDIW. The stakes are high for Member States who may wish to reuse parts of the infrastructures deployed under eIDAS for their future EDIW, as may be the case for France Identité in France. The stakes are also high for the private sector, which could find new business models[328] by positioning themselves as possible EDIW providers mandated by a State, as providers of electronic attestations of attributes, or more simply by wanting to optimize their customer journey as relying parties. As part of a first call for proposals[329], the European Commission has thus selected four "*large scale pilots*"[330]. Three of these pilots involve French entities, on various use cases for the EDIW such as opening a bank account, transmitting medical prescriptions, presenting a driving license, etc. Age verification was already one of the examples given by the European Commission for the use of the EDIW in its communication elements[331] when it proposed eIDAS 2.0. But another call for proposals, from 2024, explicitly mentions the use of EDIW for age verification, in various *"scenarios including the issuance of pseudonymous attestation containing only age verification*"[332].

[328] See the estimations of on the AVPA web page, Estimating the size of the global online age verification market, 3 June 2021, https://avpassociation.com/thought-leadership/estimating-the-size-of-the-global-age-verification-market/ , accessed on 1 December 2024, and also Biéri M. for the LINC, Age verification: the economic argument, 19 July 2023, https://linc.cnil.fr/follow-age-verification-economic-argument , accessed on 1 December 2024.

[329] European Commission, *Digital Europe Programme (DIGITAL), Call for proposals, Accelerating best use of technologies (DIGITAL-2022-DEPLOY-02),* 2 February 2022, p. 16-19.

[330] See their respective presentation on the oficial website of the European Commission about the EDIW, *PILOT PROJECTS What are the Large Scale Pilots,* https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects , accessed on 1 December 2024.

[331] See the presentation made by the European Commission on its official website about the EDIW, *European Digital Identity,* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr , accessed on 1 December 2024.

[332] European Commission, *Digital Europe Programme (DIGITAL), Call for proposals, Accelerating best use of technologies (DIGITAL-2024-BESTUSE-TECH-06),* 14 May 2024, p. 9.

It is possible to identify other links between the legislation relating to online age verification scenarios studied in the first part of this study and the EDIW. The BIK+ strategy[333] explicitly mentions the potential that the EDIW could represent in the verification of the age of minors in the context of access to sensitive content. Another example is the *Task Force on Age Verification* commissioned within the framework of the application of the DSA, which is involved in the work relating to the development of the EDIW[334]. This participation is all the more interesting given the fact that the very large online platforms are therefore both encouraged via the DSA to implement risk mitigation measures such as online age verification and parental control tools and obliged to accept the EDIW via eIDAS 2.0. It will then be important, during the respective applications of these regulations, to ensure their good interaction with each other. The European Commission seems fully aware of this interaction, as evidenced by its call for tenders "*Development, Consultancy and Support for an Age Verification Solution*"[335] aimed at financing research on a generic online age verification system usable within the framework of the DSA, but respecting the technical requirements of the EDIW, and which could potentially rely on a ZKP protocol.

Chapter 2 Summary

The eIDAS Regulation represents the first major step of the EU framework for digital identification. The latter allows each Member State to notify an electronic identification scheme for the purpose of mutual recognition with other Member States. In France, this framework has been useful for online age verification regarding access to online gambling. At the EU level, initiatives such as *euCONSENT* demonstrate an ambition to leverage infrastructures adopted

[333] BIK+ strategy, (2022), *op. cit.,* p. 9 and 12.

[334] European Commission, ANNEX to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2024, Brussels, COM(2024) 260 final, 2 July 2024, p.39 and 48. Also mentioned in the press release *Second Meeting of the Task Force on Age Verification, 20 March 2024,* https://digital-strategy.ec.europa.eu/en/news/second-meeting-task-force-age-verification , accessed on 1 December 2024.

[335] European Commission, *Call for tenders Development, Consultancy and Support for an Age Verification Solution,* EC-CNECT/2024/OP/0073, 15 October 2024.

under eIDAS to develop European solutions for age verification and parental control.

Persistent disparities between Member States have nevertheless led to a revision of eIDAS through the adoption of eIDAS 2.0. The update of the framework requires each Member State to make an EDIW available to its citizens, thus allowing them to authenticate themselves for access to public and private services across the EU. The use of EDIW for age verification purposes is explicitly considered by the European Commission, not only due to the involvement of the Task Force on Age Verification in the work on the EDIW, but also through calls for funding, one of which explicitly mentions both age verification under the DSA and the architecture of the EDIW. The deliverables of these projects, and more generally the exact implementation of the EDIW, will make it possible to confirm or not the merits of using such public/private identity verification systems for online age verification scenarios.

Part II Summary and Conclusion

The second part of this study, dedicated to analyzing the direction age verification systems could take in the future, made it possible to identify several essential elements. The classification of systems into different typologies highlighted the limits of bilateral verification architectures and systems based on self-declared proof of age. Architectures including a third-party verifier or estimated proofs of age appear better suited to the challenges of age verification, while involving significant risks. Age verification systems based on an architecture of double anonymity architecture or on certified proofs of age are even more relevant. However, even for these latter types of system, the exact details of the age verification system studied considerably influence their effectiveness and the risks they present, in particular depending on whether or not the system is based on a ZKP protocol.

The second chapter therefore undertook to examine more concrete systems, focusing once again on an area involving both the EU and France, that of digital identity. Numerous links with online age verification emanate from the eIDAS

regulation, its application in France, and its recent revision via eIDAS 2.0. The scenario of access to online gambling in France is an example, as it is based, in particular, on the eIDAS framework. The revision of eIDAS and the planned EDIW could be an important milestone regarding online age verification. The potential use of the EDIW as an age verification system is considered frequently, notably in European Commission funding calls, one of which explicitly aims to develop an age verification system for the application of the DSA**.** Therefore, these efforts could perhaps lead to the creation of a unified European technical solution for age verification as the European Commission has aspired to during its written exchanges with France[336].

[336] European Commission, *Detailed opinion in response to Notification 2023/461/FR, op. cit.,* p. 5.

OVERALL SUMMARY AND CONCLUSION

Online age verification has been a subject gradually addressed by France for the past two decades, with a notable acceleration of regulatory initiatives in the last two years. *Remote access to alcoholic beverages and tobacco products* (part I, chap. 1, I), *access to online gambling and betting* (part I, chap. 1, II), *access to social networks* (part I , chap. 1, III) or *access to pornographic content online* (part I, chap. 1, IV); online age verification scenarios in France have been empirically legislated, leading to varied regimes, whose application and effectiveness remain heterogeneous (tab. 1).

This heterogeneity is sometimes explained by the division of prerogatives between France and the EU. For example, the French regime regarding access to social networks is ultimately inapplicable, while the one relating to access to pornographic content online is limited in its scope of application, so as not to encroach on EU regulations regarding digital services. There is also a lot of regulatory activity around online age verification at the EU level. *Protection of minors in terms of personal data* (part I, chap. 2, I), *protection from content which may impair the physical, mental or moral development of minors* (part I, chap. 2 ,II), *protection of minors in the context of the use of digital services* (part I, chap. 2, III), *protection of children from sexual abuse* (part I, chap. 2, IV); EU systems often favor the identification of minors to apply protective regimes to them, rather than denying them access as is more the case with French systems. The progress and effectiveness of these measures remain, here too, uneven (tab. 2).

Comparable objectives can be identified in all these regulations, starting obviously with the protection of the physical or moral integrity of minors. However, other specific issues must also be taken into account. Thus, age verification systems themselves can generate various types of undesirable risks (tab. 3), regarding the autonomy of minors, the participation of their legal representatives, and, more generally, the protection of personal data and privacy. For the entities deploying these systems, risks in terms of legal

certainty also take shape in the light of the numerous interactions between the different legal regimes on age verification. This risk is all the greater given that most French and EU laws on online age verification do not define the precise age verification systems to set up (tab. 1 and 2), at least

With the recent ARCOM framework on access to pornography and the current DSA application, things seem to be progressively changing on this point. We therefore tried to study the direction in which the future of age verification systems is heading. To do so, we first identified and detailed two classifications of age verification systems. The first, based on the nature of the proof of age (part II, chap. 1, I), makes it possible to identify the limits of self-declared proofs, the risks of estimated proofs and the reasonableness of using certified proofs, even though the latter may also have limits. The second classification focuses on the organization of the stakeholders involved in an age verification system, and how they share data (part II, chap. 1, II). A simple bilateral architecture between a user and a service provider concentrates the risks on the latter's side (fig. 1). Adding a third-party verifying entity in the architecture (fig. 2), or even an intermediary to guarantee a double anonymity (fig. 3), helps to better distribute and reduce these risks. However, the exact details of the age verification systems studied, including whether or not they are based on a ZKP protocol, significantly influence risk limitation.

To apply these two analysis grids more concretely, we then studied the legal framework for digital identity, a field involving once again both the EU and France. The 2014 eIDAS regulation, and its update through the 2024 eIDAS 2.0 regulation, offer promising prospects in terms of identity and age verification. The eIDAS framework (part II, chap. 2, I) proposes that each Member State notify electronic identification schemes at the EU level. France has thus notified two systems, including *France Identité*, usable through the identity federation *France Connect* (fig. 4), and recognizes certain age verification systems, for the access to online gambling, based directly or indirectly on the eIDAS framework. At the EU level, the *euCONSENT* initiative, also based on the eIDAS infrastructures, demonstrates the desire to find a European system for age

verification and parental control. The revision of eIDAS through eIDAS 2 (part II, chap. 2, II) and its EDIW (fig. 5), which each Member State will have to put in place, could constitute this common age verification system at the EU level. The current implementation and the technical developments of the EDIW allow us to identify a very clear objective of using the latter for the purposes of online age verification, particularly within the framework of the DSA.

The future of online age verification in France and within the EU therefore raises two major challenges. On the one hand, it will be necessary to improve the regulatory frameworks and ensure their compatibility and interaction, which are currently sometimes ambiguous. On the other hand, the relevance of emerging European solutions, such as those that could be based on the EDIW, will have to be assessed according to their ability to respond to the various specific issues of each verification scenario. While the EDIW is notably intended for access to very large online platforms under the DSA, it is quite unlikely that users will feel comfortable using a public identification system such as *France Connect* or *France Identité* to access a pornographic website.

It is less likely that users will feel comfortable using a public identification system such as *France connect* or *France Identité* or their possible future evolution through a French EDIW, to access pornographic sites[337]. The coexistence of several verification systems for the same verification scenario, as indirectly suggested by the ARCOM framework for access to pornography in France and more generally by the CNIL[338] therefore seems desirable. The threat of misuse of such systems by public authorities for repressive purposes or the risk of exclusion of certain populations groups could then be limited.

[337] Although the situation is conceivable as evidenced by the legislative development in Spain of the "Age Verification System for Online Content Access, Age Verification Ecosystem", see the details of the technical specifications on the official webpage of the Spanish *Ministerio para la Transformación Digital y de la Función Pública,* , Especificaciones Técnicas, 30 June 2024, https://digital.gob.es/especificaciones_tecnicas.html , accessed on 1 December 2024, and possible interconnections with eIDAS 2.0, (2024), op. cit., Volpicelli G. for Politico, *Spain introduces porn passport to stop kids from watching smut, 3 July 2024,* https://www.politico.eu/article/spain-builds-porn-passport-to-stop-kids-watching-smut/ , accessed on 1 December 2024.

[338] CNIL, *Thematic file - Digital identity,* (2023), *op. cit.,* p. 11.

Finally, if the interactions between French and European measures already reflect sovereignty issues within the EU[339], this dynamic could extend beyond the old continent. Just like the *Brussels effect*[340] experienced by the GDPR, could the EDIW and its compulsory adoption by very large platforms produce a similar effect in the coming years? Future codes of conduct and international standards on online age verification[341] could thus be inspired by, or compete with, emerging European standards. The coming years of application of eIDAS 2.0 and the DSA regarding mitigation measures will therefore be decisive in confirming or refuting this scenario.

[339] President of the French Republic Macron E., *Speech on Europe*, (2024), *op. cit.*

[340] *I.e.* the indirect export of its standards on a global scale, see on this notion Bradford A., *The Brussels Effect : How the European Union Rules the World*, Oxford University Press, 2020, 424 p.

[341] Such as the PAS 1296:2018, *i.e. Code of Practice for Online Age Verification service providers developed by the British Standards Institute and the Digital Policy Alliance*, adopted on **3**1 March 2018, or even the current developments about the ISO/IEC DIS 27566-1 and ISO/IEC WD 27566-3.2 about *Information technology, cybersecurity and privacy protection — Age assurance systems.*

BIBLIOGRAPHY

BIBLIOGRAPHY PLAN

1. LEGISLATION AND NORMS

1.1 UNITED NATIONS

- Convention on the Rights of the Child, New York, 20 November 1989.
- Optional protocol on a communications procedure, 19 December 2011.
- Optional protocol on the sale of children, child prostitution and child pornography, 25 May 2000.
- General comment No. 25 (2021) on children's rights in relation to the digital environment, 2 March 2021.

1.2 OECD

- Declaration on a Trusted, Sustainable and Inclusive Digital Future, OECD/LEGAL/0488, 15 December 2022.

1.3 COUNCIL OF EUROPE

- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, (CETS No. 201), Lanzarote, 25 october 2007.
- Guidelines to respect, protect and fulfil the rights of the child in the digital environment Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States, 4 July 2018.

1.4 EU

1.4.1 General

- Charter of Fundamental Rights of the European Union, (2000/C 364/01).
- European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, 26 January 2022.

1.4.2 Regulations

1.4.2.1 Regulations (adopted)

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- 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).
- Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
- 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 Act).
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. eIDAS means "electronic identification, authentication, and trust services".
- Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

1.4.2.2 Regulations (proposed)

- Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final, 11 May 2022.

1.4.3 Directives

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) consolidated text after the adoption of the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy

in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
- Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)
- Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society service.
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

1.4.4 Implementing Regulations
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallet.
- Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets.
- Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem.
- Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets.
- Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework.

1.4.5 Recommendation
- Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, C/2021/3968.

1.4.6 Guidelines
- EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020.
- EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, 28 March 2023.

1.5 FRANCE
1.5.1 Codes
- Internal Security Code.
- Penal Code.
- Public Health Code.

1.5.2 Laws
1.5.2.1 Laws (adopted)
- LAW no. 78-17 of 6 January 1978 on data Processing, Data Files and Individual Liberties*, ("relative à l'informatique, aux fichiers et aux libertés").*
- LAW no. 86-1067 of 30 september 1986 on freedom of communication *("relative à la liberté de communication") (Loi Léotard)).*
- LAW no. 91-32 of 10 January 1991 on the fight against smoking and alcoholism *("relative à la lutte contre le tabagisme et l'alcoolisme").*
- LAW no. 2004-575 of 21 June 2004 for confidence in the digital economy *("pour la confiance dans l'économie numérique").*
- LAW no. 2007-297 of 5 March 2007 relating to the prevention of delinquency *("relative à la prévention de la délinquance").*

- LAW no. 2009-879 of July 21, 2009 relating to hospital reform and relating to patients, health and territories *("portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires").*
- LAW no. 2014-344 of 17 March 2014 relating to consumption *("relative à la consommation").*
- LAW no. 2016-41 of 26 January 2016 on the modernization of our health system *("de modernisation de notre système de santé").*
- LAW no. 2019-1479 of 28 December 2019 on finance for 2020
- LAW no. 2020-936 of 30 July 2020 aimed at protecting victims of domestic violence *("visant à protéger les victimes de violences conjugales").*
- LAW no. 2023-566 of July 7, 2023 aimed at establishing a digital majority and fighting against online hate *("visant à instaurer une majorité numérique et à lutter contre la haine en ligne").*
- LAW no. 2023-1322 of 29 December 2023 on finance for 2024
- LAW no. 2024-449 of May 21, 2024 aimed at securing and regulating the digital space *("visant à sécuriser et à réguler l'espace numérique").*

1.5.2.2 Laws (proposed and rejected)

- Proposed law n° 1776 (15th legislature) aimed at forcing users of social networks to register under their real identity *("visant à obliger les utilisateurs des réseaux sociaux à s'y inscrire sous leur identité réelle")* of 20 March 2019.
- Proposed amendment no. 373 aiming to commission a report from the Government on the feasibility and consequences of lifting anonymity on social networks, on 13 January 2021.

1.5.3 Decrees

- Decree no. 2010-518 of 19 May 2010 relating to the offer of games and bets from gaming operators and the provision of gaming data to the National Gaming Authority *("relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux").*
- Decree no. 2021-1306 of 7 October, 2021 relating to the modalities of implementation of measures aimed at protecting minors against access to sites disseminating pornographic content *("relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique")*

1.5.4 Ordinance

- Ordinance no. 2016-623 of 19 May 2016.
- Ordinance no. 2020-1642 of 21 December 2020.

1.5.5 Delegated acts from public authorities

- ANSSI, Remote identity verification service providers - Requirements rule set, version 1.1 of 1 March 2021.
- ARCOM, Framework setting out the minimum technical requirements for age verification systems set up for access to certain online public communication services and video-sharing platforms that make pornographic content available to the public, October 2024.

1.6 OTHERS

1.6.1 General

- ISO/IEC DIS 27566-1 and ISO/IEC WD 27566-3.2 about Information technology, cybersecurity and privacy protection — Age assurance systems (in progress).

1.6.2 Spain

- *Ministerio para la Transformación Digital y de la Función Pública, Especificaciones Técnicas,* 30 June 2024, https://digital.gob.es/especificaciones_tecnicas.html , accessed on 1 December 2024,

1.6.3 United Kingdom

- PAS 1296:2018 (Code of Practice for Online Age Verification service providers developed by the British Standards Institute and the Digital Policy Alliance) adopted on 31 March 2018,
- Online Safety Act 2023 Government Bill of 26 October 2023
- Information Commissioner's Office, Age appropriate design: a code of practice for online services". available at : https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ , accessed on 1 December 2024.

2. CASE LAW

2.1 EU

- EDPB, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), 2 August 2023.

2.2 FRANCE

- CNIL, Deliberation No. 2018-284 of 21 June 2018.
- *Conseil d'Etat*, décision N° 432656 ECLI:FR:CECHR:2020:432656.20201104, 4 November 2020.
- CNIL, Deliberation 2021-069 of 3 June 2021.
- CSA, Decision no. 2021-P-02 of 13 December 2021.
- CSA, Decision no. 2021-P-03 of 13 December 2021.
- CSA, Decision no. 2021-P-04 of 13 December 2021.
- CSA, Decision no. 2021-P-05 of 13 December 2021.
- CSA, Decision no. 2021-P-06 of 13 December 2021.

3. PUBLIC OPINIONS, COMMUNICATIONS, CONSULTATIONS AND PROCEDURES

3.1 EU

3.1.1 European Commission

3.1.1.1 Communications and strategies

- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - European Strategy for a Better Internet for Children, COM(2012) 196 final, 2 May 2012.
- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU strategy on the rights of the child, COM/2021/142 final, 24 March 2021.
- European Commission, 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 youth: the new European strategy for a better internet for kids (BIK+), COM/2022/212 final, 11 May 2022.
- European Commission, ANNEX to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2024, Brussels, COM(2024) 260 final, 2 July 2024

3.1.1.2 Call for evidence, tenders and proposals

- Digital Europe Programme (DIGITAL), Call for proposals, Accelerating best use of technologies (DIGITAL-2022-DEPLOY-02), 2 February 2022.
- Digital Europe Programme (DIGITAL), Call for proposals, Accelerating best use of technologies (DIGITAL-2024-BESTUSE-TECH-06), 14 May 2024
- Call for evidence for an initiative - Digital Services Act - guidelines to enforce the protection of minors online, Ref. Ares(2024)5538916, 31 July 2024
- Call for tenders Development, Consultancy and Support for an Age Verification Solution, EC-CNECT/2024/OP/0073, 15 october 2024.

3.1.1.3 Detailed opinions

- Commissioner for Internal Market, Breton T., Detailed opinion in response to Notification 2023/237/FR and 2023/362/FR, (Ares(2023)5596'438), 14 August 2023.
- Commissioner for Internal Market, Breton T., Detailed opinion in response to Notification 2023/461/FR, (7417 final), 25 October 2023.
- Commissioner for Internal Market, Breton T., Detailed opinion in response to Notification 2023/632/FR, (389 final), 17 January 2024.
- Commissioner for Communications Networks, Content and Technology, Viola R., Detailed opinion in response to Notification 2024/0208/FR, C(2024) 5148 final, 15 July 2024.

3.1.2 EDPB-EDPS

- EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 28 July 2022µ

3.2 EU Member States in EU processes

3.2.1 France

- ARCOM, Arcom's contribution to the Call for evidence for guidelines on the protection of minors under the Digital Services Act, 26 September 2024.

3.2.2 Other

- Technical standards notified to the European Commission by Spain (Notification Number: 2024/0531/ES), Italy (Notification Number 2024/0578/IT), Ireland (Notification Number 2024/0283/IE), Germany (Notification Number 2024/0283/IE 2024/0188/DE) and Denmark (Notification Numbers 2024/0483/DK, 2024/0226/DK, 2024/0225/DK and 2024/0064/DK), 2024.

3.3 FRANCE

- Written question no. 1564 (16th Parliament) of the deputy of the French national assembly, Ardouin J.-P., Social networks: lifting anonymity and cooperation with the authorities *(Réseaux sociaux : levée de l'anonymat et coopération avec les autorités"),* 27 September 2022.
- ARCOM, Public consultation on the draft framework setting out the minimum technical requirements for age verification systems set up for access to online pornographic content *("Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à des contenus pornographiques en ligne"),* 11 April 2024.

4. RESEARCH AND STUDIES

4.1 Academic research (alphabetic order)

- Bousquet-Bérard C. and Pascal A. for the presidency of the French Republic, *Children and screens In search of lost time* ("*Enfants et écrans À la recherche du temps perdu"),* April 2024,
- Balkin J. M., *The fiduciary model of privacy,* Harvard Law Review Forum, Vol. 134, No. 1, november 2020.
- Boniel-Nissim M. et *al., International perspectives on social media use among adolescents: Implications for mental and social well-being and substance use,* in: Computers in Human Behavior 129(1), December 2021.
- Bradford A., *The Brussels Effect : How the European Union Rules the World*, Oxford University Press, 2020, 424 p.
- De Cicco D., Downes J., Helleputte C., *No Children in the Metaverse? The Privacy and Safety Risks of Virtual Worlds (and How to Deal with Them)*, in: Rannenberg K., Drogkaris P., Lauradoux C. (eds) Privacy Technologies and Policy. APF 2023. Lecture Notes in Computer Science, vol 13888. Springer, Cham, 2024.
- Dos Santos Lemos Fernandes S., *Protecting Children from Cybercrime: Legislative Responses in Latin America to Fight Child Pornography*, Online *Grooming, and Cyberbullying through Information and Communication Technologies,* World Bank, Washington, DC, 2015.
- Eynard J., *Online Age verification: AI as a solution?*, in: Artificial Intelligence Law : between sectoral rules and comprehensive regime comparative law, Castets-Renard C. and Eynard J. (eds.), Bruylant, 2023.
- Goicovici J*, The collecting of consent to the processing of children's personal data, between volatility and disobedience,* SHS Web of Conferences, 2023.
- Hof S. van der, *I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World.* Wisconsin International Law Journal, 34(2), 2017.
- Hof S. van der "We Take Your Word For It' — A Review of Methods of Age Verification and Parental Consent in Digital Services", European Data Protection Law Review Volume 8, 2022, Issue 1 p. 61-72.
- Huttner L., *Controlling access of minors to pornographic sites ("Le contrôle de l'accès des mineurs aux sites pornographiques"),* Dalloz IP/IT, July 2024.
- Jolicoeur M.-P., *Checking the age of Internet users on pornographic sites to limit access to minors: an innovative and necessary measure for Canadian law ("Vérifier l'âge des internautes sur les sites pornographiques pour en limiter l'accès aux personnes mineures : une mesure novatrice et nécessaire pour le droit canadien"), in:* Zannou L. R., Gaumond E. and et Lang M. (dir.), Meetings. Crossed views on justice (Rencontres. Regards croisés sur la justice), Lex Electronica, 28-2, p. 79-121, 2023.
- Kishk Y. A., *State-Based Online*. *Restrictions*: *Age-Verification* And The *VPN*. *Obstacle* In The *Law*," 2 Int'l J. L. Ethics, Technology, 2024.
- Lee E. and Huet B., *Paradoxical immunity for anonymous authors of defamatory content ("L'immunité paradoxale offerte aux auteurs anonymes de contenus diffamatoires"),* Légipresse, 26 July 2024
- Léger P., *The additional penalty of suspension of access accounts to online services: symbol of measures to secure the digital space and the difficulties of their implementation ("La peine complémentaire de suspension des comptes d'accès à des services en ligne : symbole des mesures de sécurisation de l'espace numérique et des difficultés de leur mise en œuvre"),* Dalloz IP/IT, July 2024, p.395
- Livingstone S. and Stoilova M., *The 4Cs: Classifying Online Risk to Children*, (CO:RE Short Report Series on Key Topics), Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence, 2021).

- Livingstone S. *et al.*,*The best interests of the child in the digital environment,* Digital Futures for Children centre, LSE and 5Rights Foundation, 2024.
- Niestadt M. for the European Parliamentary Research Service, *Protecting children in virtual worlds (the metaverse), PE 762.294,* April 2024.
- Petelin T.*, The digital majority in question: commentary on the law of 7 July 2023 aimed at establishing a digital majority and combating online hate' ("La majorité numérique en question : commentaire de la loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne"),* Dalloz IP/IT no 12, 2023.
- Radtke T., *Mandatory Age Verification for Online Services under GDPR — The protection of children according to data protection law in the light of EDPB's Binding Decision regarding TikTok,* Computer Law Review International, vol. 24, no. 6, 2023.
- Rahamathulla M., *Cyber Safety of Children in the Association of Southeast Asian Nations Region: a Critical Review of Legal Frameworks and Policy Implications*, in: Journal on Child Malt. 4, p 375-400, 2021.
- Sas M. and Mühlberg J. T., *TRUSTWORTHY AGE ASSURANCE? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective*, 2024.
- Stardust Z. *et al., Mandatory age verification for pornography access: Why it can't and won't 'save the children', B*ig Data & Society, 11(2), June 2024.

4.2 Public bodies research and reports

- PEReN, Online underage users detection: can we reconcile efficiency, convenience and anonymity?, Shedding light on", #04, May 2022
- CNIL, Thematic file - Digital identity *("Dossier thématique - L'identité numérique*"), February 2023.
- EDRi, Position Paper: Age verification can't 'childproof' the internet, 4 October 2023.
European Audiovisual Observatory, The protection of minors on VSPs: age verification and parental control, 2023.
- O'Reilly J. for the Council of Europe, The protection of children against online violence, Rapport | Doc. 15954 | 27 March 2024.
- "European Digital Identity Wallet Architecture and Reference Framework" (ARF) at the following webpage https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/ , accessed on 1 December 2024,
- European Commission: Directorate-General for Communications Networks, Content and Technology, New Better Internet for Kids Strategy (BIK+) - Compendium of EU formal texts concerning children in the digital world - 2024 edition, Publications Office of the European Union, 2024.

4.3 Private or associative entities research and reports

- Renaissance Numérique, Age assurance online: working towards a proportionate and European approach, September 2022.
- Forbrukerrådet, COMMERCIAL EXPLOITATION OF CHILDREN AND ADOLESCENTS ONLINE - How to ensure a rights-respecting digital childhood, November 2024.

4.4 Figures and statistics

- Tovar M.-L. and Costes J.-M. for the Society for mutual aid and psychological action ("Société d'entraide et d'action psychologique"), *Practices of betting and gambling by minors in 2021 ("pratique des jeux d'argent et de hasard des mineurs en 2021"),* zoom recherches n°4, February 2022.
- ARCOM, *Visitation of "adult" sites by minors ("La fréquentation des sites adultes par les mineurs"),* Mai 2023.
- Toluna - Harris Interactive for the Association e-Enfance/3018, with the support of Google, Quantitative survey carried out online from February 6 to 14, 2023.
- Génération Numérique, Survey *on the digital practices of 11- to 18-year-olds ("Enquête sur les pratiques numériques des 11 à 18 ans"),* January 2024.
- Génération Numérique*, Survey on shocking content accessible to minors ("Enquête sur les contenus choquants accessibles aux mineurs"),* January 2024.
- Numerique.gouv.fr, *FranceConnect reaches 40 million connected citizens by June 2024* ("*FranceConnect franchit le cap des 40 millions de citoyens connectés en juin 2024 number drawn from official bodies on June 2024"),*
https://www.numerique.gouv.fr/actualites/franceconnect-franchit-le-cap-des-40-millions-de-citoyens-connectes-en-juin-2024/ , accessed on 1 December 2024.
- European Commission, Special *Eurobarometer 551 on 'the digital decade' 2024 Summary Fieldwork: March-April 2024,* July 2024.

5. ONLINE RESOURCES, PRESS RELEASES AND NEWS

5.1 EU institutions

5.1.1 European Commission

- Press release *Second Meeting of the Task Force on Age Verification*, 20 March 2024, https://digital-strategy.ec.europa.eu/en/news/second-meeting-task-force-age-verification , accessed on 1 December 2024.
- Press release *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram*, 16 May 2024.
- Press release *Commission designates adult content platform XNXX as Very Large Online Platform under the Digital Services Act,* 10 July 2024
- *Overview of pre-notified and notified eID schemes under eIDAS*, https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS , accessed on 1 December 2024.
- European Commission about the EDIW, European Digital Identity, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr , accessed on 1 December 2024.
- *PILOT PROJECTS What are the Large Scale Pilots,* https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects , accessed on 1 December 2024.

5.1.2 European Union Agency for Fundamental Rights

-https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu , accessed 1 December 2024.
-https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/purchasing-and-consuming-alcohol , accessed 1 December 2024.
-https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/purchasing-and-consuming-tobacco , accessed 1 December 2024.
https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/consent-sexual-activity-adult , accessed 1 December 2024.
-https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children , accessed on 1 December 2024.
https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/issuance-credit-card , accessed on 1 December 2024.

5.1.3 European Parliament

- Press release *European Parliament vehemently opposed to Hungarian anti-LGBTIQ law*, 08 July 2021.

5.1.4 EDPS

- *Briefing note on the CSAM proposal: "The Point of No Return",* 23 October 2023

5.2 FRENCH INSTITUTIONS

5.2.1 Government (or affiliated entities)

- *Government launches national campaign to raise awareness of helplines for child victims of violence ("Le Gouvernement lance une campagne nationale de sensibilisation aux numéros d'aide pour les enfants victimes de violences")* webpage, 03 october 2022, https://solidarites.gouv.fr/le-gouvernement-lance-une-campagne-nationale-de-sensibilisation-aux-numeros-daide-pour-les-enfants , accessed on 1 December 2024
- President of the French Republic Macron E., *Speech on Europe,* Sorbonne University, 25 April 2024.
- *NAR - Marina Ferrari will meet with age verification stakeholders and representatives of the major platforms at Bercy (NAR - Marina Ferrari recevra à Bercy les acteurs de la vérification d'âge et les représentants des grandes plateformes"),* press release no. 1808, 28 April 2024.
- *FranceConnect simplifies procedures for more than 40 million people "FranceConnect simplifie les démarches de plus de 40 millions de personnes")* https://franceconnect.gouv.fr/ , accessed on 1 December 2024.
- *Single-use proof of identity (" Le justificatif d'identité à usage unique")*, https://france-identite.gouv.fr/justificatif/ , accessed on 1 December 2024.

5.2.2 ANSSI

- *Remote identity verification services providers ("prestataires de vérification d'identité à distance - PVID"),* https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid , accessed on 1 December 2024.

5.2.3 ARCOM

- Press release: *Access of minors to pornographic sites: Referral to the president of the Paris judicial court ("Accès des mineurs aux sites pornographiques : Saisine du président du tribunal judiciaire de Paris"),* 8 March 2022.

5.2.4 CNIL

- *Online age verification: balancing privacy and the protection of minors*, 22 September 2022, https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors , accessed 1 December 2024.
- *Recommendation 7: verify the child's age and parental consent while respecting their privacy ("Recommandation 7 : vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée"),* 1 June 2021, https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee , accessed on 1 December 2024.

5.2.5 LINC

- Gorin J., Biéri M. and Brocas C., *Demonstration of a privacy-preserving age verification process,* 22 June 2022, https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process , accessed 1 December 2024, (popularizing the work of the Digital Innovation Laboratory of the CNIL (Laboratoire de l'innovation numérique de la CNIL - LINC), Blazy O. and the PEReN).
- Biéri M. for the LINC, Age verification: the economic argument, 19 July 2023, https://linc.cnil.fr/follow-age-verification-economic-argument , accessed on 1 December 2024.

5.3 PRESS

- Hue B. for RTL in the press article Digital majority at 15: why the implementation of the measure defended by Macron promises to be difficult in Europe ("Majorité numérique à 15 ans : pourquoi la mise en place de la mesure défendue par Macron s'annonce difficile en Europe"), 29 April 2024, https://www.rtl.fr/actu/sciences-tech/majorite-numerique-a-15-ans-pourquoi-la-mise-en-place-de-la-mesure-defendue-par-macron-s-annonce-difficile-en-europe-7900379346 , accessed on 1 December 2024.
- Volpicelli G. for Politico, Spain introduces porn passport to stop kids from watching smut, 3 July 2024, https://www.politico.eu/article/spain-builds-porn-passport-to-stop-kids-watching-smut/ , accessed on 1 December 2024.
- McConvey J. R. on Biometric Update.com news website, ChatGPT can recognize 'facial identities,' perform age estimation: research, 8 October 2024, https://www.biometricupdate.com/202410/chatgpt-can-recognize-facial-identities-perform-age-estimation-research , accessed on 1 December 2024.
- Mediavilla L. for Le Figaro, Free, SFR... Telecoms operators caught in the wave of cyber attacks ("Free, SFR… Les opérateurs télécoms pris dans la vague des cyberattaques"), 26 October 2024, https://www.lefigaro.fr/secteur/high-tech/free-cible-par-une-cyberattaque-impliquant-un-vol-de-donnees-personnelles-de-clients-20241026 , accessed 2 December 2024.
- Le Parisien news website, *An AI capable of estimating your age? FDJ tests the device in tobacconists to keep out minors ("Une IA capable d'estimer votre âge ? La FDJ teste le dispositif chez des buralistes pour écarter les mineurs"),* 6 april 2023, https://www.leparisien.fr/high-tech/une-ia-capable-destimer-votre-age-la-fdj-teste-le-dispositif-chez-des-buralistes-pour-ecarter-les-mineurs-06-04-2023-VALETOLKFFA7XIK5IUPJE4LUIY.php , accessed on 1 December 2024.
- La Voix Du Nord, No privacy for teenagers*, we have to ''look into their phones'': Sabrina Agresti-Roubache shocks ("La vie privée des ados, c'est « non », il faut « fouiller leurs téléphones » : Sabrina Agresti-Roubache choque"),* 23 April 2024, https://www.lavoixdunord.fr/1455216/article/2024-04-23/la-vie-privee-des-ados-c-est-non-il-faut-fouiller-leurs-telephones-sabrina , accessed on 1 December 2024.

5.4 OTHER PRIVATE OR ASSOCIATIVE RESOURCES

- Hubert M.,*Social networks and LGBT concerns ("Les réseaux sociaux face aux questions LGBT")* blog article on Alliance arc-en-ciel website, 25 mars 2017, https://arcencielquebec.ca/2017/03/25/les-reseaux-sociaux-face-aux-questions-lgbt/ , accessed on 1 December 2024
- UFC que Choisir, *"Paid content in video games - Winning games, naughty games ("Contenus payants dans les jeux vidéo - Jeux de gains, jeux de vilains")* webpage, 22 November 2017, https://www.quechoisir.org/action-ufc-que-choisir-contenus-payants-dans-les-jeux-video-jeux-de-gains-jeux-de-vilains-n48636/ , accessed 1 December 2024.
- AVPA web page*, Estimating the size of the global online age verification market,* 3 June 2021, https://avpassociation.com/thought-leadership/estimating-the-size-of-the-global-age-verification-market/ , accessed on 1 December 2024.
- EDRi (via By epicenter.works) webpage*, Orwell's Wallet: European electronic identity system leads us straight into surveillance capitalism*, 2 February 2022, https://edri.org/our-work/orwells-wallet-european-electronic-identity-system-leads-us-straight-into-surveillance-capitalism/ , accessed 1 December 2024
- Meta's news, *Introducing New Ways to Verify Age on Instagram*, 23 June 2022, https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/ , accessed on 1 December 2024, via the service provider "Yoti"

- EDRi, Joint Statement on the Dangers of Age Verification Proposals to Fundamental Rights Online, 16 September 2024.
- Tsebee D, Boshe P. and Oloyede R, *Child online protection in Africa : Safeguarding youth in the digital age,* blog article on the Privacy Lens Africa website, 20 November 2024, https://privacylens.africa/2024/11/20/child-online-protection-in-africa-safeguarding-youth-in-the-digital-age/ , accessed 1 December 2024.
- Meta's Global Head of Safety, Davis A., web page Europe Can Make Parenting in a Digital World Easier, 25 November 2024, https://about.fb.com/news/2024/11/europe-can-make-parenting-in-a-digital-world-easier/ , accessed 1 December 2024.
- euCONSENT official website https://euconsent.eu/ , accessed on 1 December 2024
- AVPA website https://avpassociation.com/us-state-age-assurance-laws-for-social-media/ , accessed 1 December 2024.

TABLE OF CONTENTS

ABOUT THE AUTHOR

Alexandre Humain-Lescop (a.humain.research@gmail.com) is a PhD researcher specialized in digital law and data protection law at the *Institut Polytechnique de Paris (IP Paris - France)*. His research explores data-sharing regulatory frameworks and ecosystems, focusing on models, tools, and interfaces that empower data subjects to exercise meaningful control over their information, with particular emphasis on applications in the banking and financial sector as well as regarding online age verification.

ABOUT THE DIGITAL, GOVERNANCE AND SOVEREIGNTY CHAIR

Sciences Po's Digital, Governance and Sovereignty Chair's mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts.

Hosted by the **School of Public Affairs**, the Chair adopts a multidisciplinary and holistic approach to researching and analyzing the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty Chair is chaired by **Florence G'sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs, and visiting professor at the Cyber Policy Center of Stanford University.

The Chair's activities are supported by: