Arcom
Le régulateur de la communication audiovisuelle et numérique

Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques

Octobre 2024

© Arcom

Sommaire

Sommaire 3

Introduction 5

La responsabilité des services visés diffusant des contenus à caractère pornographique 5

L'évolution du rôle de l'Arcom dans le cadre de la loi visant à sécuriser et réguler l'espace numérique 6

Les travaux déjà engagés sur la vérification de l'âge 7

Présentation du référentiel 9

Accompagner le secteur dans la mise en place de solutions de vérification de l'âge 9

Actualisations du référentiel et état de l'art 9

Structure du référentiel et calendrier de mise en œuvre 10

Première partie : considérations générales relatives à la fiabilité des systèmes de vérification de l'âge 11

Deuxième partie : protection de la vie privée 14

Principes de protection de la vie privée 14

Mise en œuvre d'un système de vérification de l'âge respectueux de la vie privée par défaut et par conception 14

Exigences minimales applicables à tous les systèmes de vérification de l'âge 15

- 1. Indépendance du prestataire de système de vérification de l'âge vis-à-vis des services visés diffusant des contenus à caractère pornographique 15
- 2. Confidentialité vis-à-vis des services visés diffusant des contenus à caractère pornographique 16
- 3. Confidentialité vis-à-vis des prestataires de génération de preuve d'âge 16
- 4. Confidentialité vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge 16
- 5. Mesures de sauvegarde des droits et libertés des personnes par les vérificateurs de l'âge 16

Exigences spécifiques pour les systèmes protecteurs de la vie privée respectant le principe de « double anonymat » 17

- 6. Confidentialité renforcée vis-à-vis des services visés diffusant des contenus à caractère pornographique 17
- 7. Confidentialité renforcée vis-à-vis des émetteurs d'attributs d'âge 18
- 8. Confidentialité renforcée vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge 18
- 9. Disponibilité et couverture de la population 18

Information des utilisateurs sur le niveau de protection de la vie privée attaché aux dispositifs de vérification de l'âge 19

- 10. Affichage explicite du niveau de protection de la vie privée des utilisateurs 19

Objectifs souhaitables et bonnes pratiques **19**

Troisième partie : solutions de génération de preuve dérogatoires acceptées à titre temporaire 20

Quatrième partie : audit et évaluation des solutions de vérification de l'âge 21

Évaluation en conditions réelles des systèmes mis en place **21**

Taux d'erreur, contournement et risques d'attaque **21**

Indépendance du prestataire d'audit **21**

Introduction

La responsabilité des services visés diffusant des contenus à caractère pornographique

1. Avec la démocratisation des terminaux mobiles permettant d'accéder à internet auprès des enfants, l'exposition des mineurs aux contenus pornographiques sur internet est en forte progression.

Selon une étude réalisée par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) sur la base de données fournies par Médiamétrie, 2,3 millions de mineurs fréquentent chaque mois des sites à caractère pornographique, ce nombre étant en croissance rapide ces dernières années et corrélé à la démocratisation des terminaux mobiles auprès des enfants. La part des mineurs fréquentant des sites « adultes » a progressé de 9 points en 5 ans, de 19 % fin 2017 à 28 % fin 2022. Chaque mois en 2022, plus de la moitié des garçons de 12 ans et plus s'est rendue sur de tels sites, pourcentage qui monte à deux tiers pour les garçons âgés de 16 ans et 17 ans. En moyenne, 12 % de l'audience des sites adultes est réalisée par les mineurs[1].

Depuis le début des années 2000[2], des travaux sur les conséquences de l'exposition précoce à la pornographie montrent qu'une exposition des plus jeunes à des contenus pornographiques peut avoir des **conséquences graves** sur leur épanouissement mental et la représentation qu'ils se font de la sexualité et des rapports entre individus, au détriment de leur développement personnel et d'une plus grande égalité dans les rapports entre les genres[3].

2. Depuis le 1er mars 1994, en application des dispositions de l'article 227-24 du code pénal, introduit par la loi n° 92-684 du 22 juillet 1992, il est interdit d'exposer des mineurs à un contenu pornographique.

La rédaction de cet article a été modifiée afin d'en préciser le champ d'application, mais aussi les modalités d'appréciation lorsqu'il s'agit de constater l'infraction sur internet. Consacrant une jurisprudence constante, l'article 227-24 précise, depuis 2020, qu'une simple déclaration d'âge ne suffit pas à prouver la majorité[4]. La rédaction actuellement en vigueur est ainsi la suivante :

---

[1] Arcom, *La fréquentation des sites « adultes » par les mineurs* (sur la base de données fournies par Médiamétrie) publiée le 25 mai 2023 : https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs

[2] M. Arzano, C. Rozier, *Alice au pays du porno : Ados : leurs nouveaux imaginaires sexuels*, Ramsay, 2005.

[3] Voir : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Quelles-solutions-pour-proteger-votre-enfant-des-images-a-caractere-pornographique-sur-internet ; et B. Smaniotto (chercheuse en psychopathologie et psychologie clinique), « Pornographie : quels impacts sur la sexualité adolescente ? », *The Conversation*, 28 août 2023 : https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142.
À ce sujet également, l'Arcom invite les parents à consulter le site : https://jeprotegemonenfant.gouv.fr/pornographie/

[4] Cour de Cassation, Chambre criminelle, 23 février 2000, 99-83.928, https://www.legifrance.gouv.fr/juri/id/JURITEXT000007070001

« Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique, y compris des images pornographiques impliquant un ou plusieurs animaux, ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

« Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

« Les infractions prévues au présent article sont constituées y compris si l'accès d'un mineur aux messages mentionnés au premier alinéa résulte d'une simple déclaration de celui-ci indiquant qu'il est âgé d'au moins dix-huit ans. »

Le législateur a instauré, par la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, **une procédure spéciale faisant intervenir l'Arcom dans l'objectif d'assurer la pleine effectivité de ces dispositions** sur les services de communication au public en ligne mettant des contenus pornographiques à disposition du public sur internet.

Cette loi a ainsi confié au président de l'Arcom une prérogative de mise en demeure de l'éditeur d'un site de se conformer au code pénal et, si cette mise en demeure n'est pas suivie d'effet, de demander au juge judiciaire d'ordonner aux fournisseurs d'accès à internet (FAI) d'empêcher l'accès à ce site.

3. Sur le fondement de ces dispositions, l'Autorité a prononcé treize mises en demeure. Elle a par ailleurs saisi, le 8 mars 2022, **le président du tribunal judiciaire de Paris** afin **qu'il ordonne aux FAI le blocage de cinq de ces services mis en demeure**. Cette procédure est toujours en cours à la date de publication du présent référentiel.

L'évolution du rôle de l'Arcom dans le cadre de la loi visant à sécuriser et réguler l'espace numérique

La loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) a fait évoluer le dispositif prévu par la loi du 30 juillet 2020.

L'article 10 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) prévoit que **l'Arcom** *« établit et publie* [...], *après avis de la Commission nationale de l'informatique et des libertés, un* ***référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge****. Ces exigences portent sur la fiabilité du contrôle de l'âge des utilisateurs et le respect de leur vie privée. »* Le champ d'application du dispositif concerne *« les contenus pornographiques mis à la disposition du public par un éditeur de service de communication au public en ligne, sous sa responsabilité éditoriale, ou fournis par un service de plateforme de partage de vidéos au sens de l'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication »* (ci-après *« les services visés diffusant des contenus à caractère pornographique »* ou *« les services*

visés »). L'Arcom peut, le cas échéant après avis de la présidente de la CNIL, mettre en demeure un de ces services de se conformer à ce référentiel et, en cas de persistance du manquement, après avis de la CNIL, prononcer une sanction pécuniaire à son égard dans le respect de la procédure prévue à l'article 42-7 de la loi n° 86-1067 du 30 septembre 1986.

Les nouvelles compétences confiées à l'Arcom par la loi SREN complètent les pouvoirs reconnus par ailleurs au juge judiciaire, qui peut être saisi directement aux fins de blocage d'un site ne respectant pas les dispositions de l'article 227-24 du code pénal sur le fondement par exemple de l'article 6-3 de la LCEN.

En outre, la protection des mineurs contre l'accès à des contenus pornographiques s'inscrit dans un cadre plus général qui régit la protection des enfants, notamment la Convention des Nations Unies relative aux droits des enfants du 20 novembre 1989 et son observation générale n° 25 de 2021 sur les droits de l'enfant en relation avec l'environnement numérique[5], ainsi que l'article 24 de la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, qui prévoit que l'*« intérêt supérieur de l'enfant doit être une considération primordiale »*.

Les travaux déjà engagés sur la vérification de l'âge

Le présent document s'inscrit dans le **contexte de travaux engagés** ces dernières années par la CNIL sur les solutions de vérification d'âge permettant de concilier protection des mineurs et respect de la vie privée.

La CNIL a tout d'abord rendu un avis en juin 2021 sur le projet de décret pris pour l'application de la loi de 2020, relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des services de communication au public en ligne diffusant du contenu pornographique[6]. Pour éviter que l'orientation sexuelle – réelle ou supposée – des personne puisse être déduite des contenus visualisés et directement rattachée à leur identité, la CNIL préconisait dès cet avis de passer par des tiers de confiance et formulait plusieurs recommandations[7] qui comprenaient une partie relative à la vérification de l'âge. Ces publications ont été renforcées par une communication publiée en juillet 2022 intitulée *« Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée »*[8] et la mise en ligne d'un démonstrateur d'un mécanisme de vérification de l'âge respectueux de la vie privée des utilisateurs[9], en coopération avec le PEReN et M. Olivier Blazy, professeur à l'École polytechnique.

[5] https://www.ohchr.org/fr/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[6] CNIL, Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique (voir : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781).
[7] Voir : https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne
[8] Voir : https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie
[9] Voir : https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee

La CNIL a déjà eu l'opportunité de rappeler que *« Contrairement à ce qui est parfois dit, le RGPD*[10] *n'est pas incompatible avec un contrôle de l'âge pour l'accès aux sites pornographiques, qui est prévu par la loi. »*[11]

Comme la CNIL, l'Arcom a également rendu un avis sur le projet de décret d'application de l'article 23 de la loi du 30 juillet 2020[12].

C'est dans ce contexte que **l'Arcom et la CNIL, avec le concours du PEReN**, ont engagé début 2023 des échanges techniques conjoints avec les acteurs de la vérification de l'âge. Ces échanges ont été enrichis par les retours d'expérience dont l'Arcom a pu bénéficier de la part de certains de ses homologues étrangers qui sont également confrontés aux enjeux de protection des mineurs et de la vie privée attachés au contrôle de l'accès aux contenus pornographiques. Le présent référentiel a été adopté à la suite d'une consultation publique, ouverte du 11 avril au 13 mai, de sa notification à la Commission européenne, le 15 avril, au titre de la directive 2015/1535 du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information et de la délibération n° 2024-067 du 26 septembre 2024 de la CNIL portant avis sur le projet de référentiel.

[10] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[11] Voir communiqué de la CNIL en date du 21 février 2023 : https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques
[12] CSA, Avis n° 2021-11 du 23 juin 2021 sur le projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044174211

Présentation du référentiel

Accompagner le secteur dans la mise en place de solutions de vérification de l'âge

Conformément aux dispositions de la loi, le référentiel précise les **exigences techniques** attendues.

L'objet de ce référentiel n'est pas de certifier des solutions techniques.

Les services visés diffusant des contenus à caractère pornographique demeureront libres de choisir les solutions de protection des mineurs de leur choix, dès lors qu'elles respectent les exigences techniques du référentiel.

L'absence de système de vérification de l'âge, tout comme les systèmes de vérification de l'âge qui ne seraient pas fiables ou offriraient un degré de protection de la vie privée inférieur au niveau d'exigence établi par le présent référentiel, ne seraient pas admissibles.

Actualisations du référentiel et état de l'art

Le référentiel **pourra être revu et actualisé** afin de tenir compte de l'état de l'art. La loi SREN dispose à cet égard que le *« référentiel est actualisé en tant que de besoin dans les mêmes conditions »*.

Il est en effet souhaitable que le secteur adopte des solutions de vérification d'âge correspondant à l'état de l'art et aux standards européens et internationaux (notamment tout standard européen qui émergerait à court terme), et compatibles avec les pratiques du secteur, s'agissant particulièrement des protocoles techniques existants.

C'est dans cet esprit que les autorités françaises ont indiqué, en réponse à une demande d'information de la Commission européenne, dans le cadre de la procédure de notification prévue par la directive 2015/1535 du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (texte codifié) que :

« S'agissant de l'avenir, elles prennent l'engagement de réviser en tout ou partie leur dispositif juridique interne lorsqu'une base légale suffisamment précise au niveau de l'Union permettra d'imposer à tout ou partie des plateformes concernées par l'accès à des contenus pornographiques un dispositif effectif de vérification de l'âge.

« Dans ces conditions, elles envisagent le [référentiel] *comme une solution transitoire, dans l'attente d'une solution européenne efficace. »*

Structure du référentiel et calendrier de mise en œuvre

La première partie du référentiel énonce des considérations générales sur la fiabilité des systèmes de vérification de l'âge découlant de la loi. Outre la nécessité de garantir une protection des mineurs par défaut, c'est-à-dire avant même l'accès au service, il s'agit de rappeler les **conditions d'efficacité des systèmes de vérification de l'âge en ligne, tout en évitant leur contournement.**

La deuxième partie porte spécifiquement sur la protection de la vie privée par les systèmes de vérification de l'âge déployés pour contrôler l'accès à des contenus à caractère pornographique. Les sites peuvent proposer des **systèmes de vérification de l'âge présentant des niveaux de protection de la vie privée différents, sous réserve d'informer les utilisateurs du niveau attaché à chaque système**.

Dans ce cadre, le référentiel établit des **objectifs minimaux applicables à tous les systèmes de vérification de l'âge**, ainsi que des objectifs spécifiques renforcés pour les systèmes les plus respectueux de la vie privée dits en « double anonymat ». **Les utilisateurs devront se voir proposer au moins un dispositif de vérification de l'âge conforme aux standards de protection de la vie privée en « double anonymat ».**

Cette deuxième partie comprend aussi des **bonnes pratiques** en matière de protection des données, considérées comme souhaitables.

Par ailleurs, les services visés diffusant des contenus à caractère pornographique pourront mettre en œuvre, à titre temporaire, des solutions de génération de preuve d'âge fondées sur la **fourniture d'une carte bancaire, par dérogation aux conditions prévues par les première et deuxième parties, mais sous réserve du strict respect de certaines conditions cumulatives énoncées** dans la troisième partie du présent document.

Enfin, la quatrième et dernière partie fixe les grands principes susceptibles de guider les services visés diffusant des contenus à caractère pornographique amenés à procéder à la réalisation d'un audit de leurs systèmes de vérification de l'âge. Il est notamment question de préciser **l'objet** de tels audits, les **conditions** de leur réalisation et les **exigences** applicables aux tiers auditeurs.

Première partie : considérations générales relatives à la fiabilité des systèmes de vérification de l'âge

Le présent référentiel vise à assurer la protection des mineurs par défaut, dès l'affichage de la première page d'un service de communication au public en ligne permettant la diffusion de contenus à caractère pornographique.

La protection des mineurs implique en effet de **prévenir toute exposition** de ces derniers à des contenus pornographiques dès l'accès aux services de communication au public en ligne mettant ces contenus à disposition.

À cet égard, l'article 1er de la loi SREN prévoit explicitement que les services visés diffusant des contenus à caractère pornographique sont tenus d'afficher un écran ne comportant aucun contenu à caractère pornographique **« tant que l'âge de l'utilisateur n'a pas été vérifié »**.

Par ailleurs, il découle de la loi SREN que les services visés diffusant des contenus à caractère pornographique doivent garantir **qu'aucun utilisateur n'accède à un contenu à caractère pornographique tant qu'il n'a pas prouvé sa majorité**.

Cette protection des mineurs par défaut peut être assurée, par exemple, par le biais d'un floutage complet de la page d'accueil du service. Les éditeurs peuvent aussi signaler le caractère pornographique de leur service. Pour ce faire, ils peuvent s'appuyer sur un mécanisme d'auto-déclaration tel que le label RTA[13] à mettre en place au niveau de chaque page de leurs sites, permettant aux systèmes de contrôle parental d'avoir connaissance de l'âge minimum requis pour accéder aux contenus présents sur le site, par l'intermédiaire d'en-têtes de réponse (ou « headers »[14]).

Pour satisfaire la loi, les systèmes de vérification de l'âge (en l'occurrence de la majorité) mis en place par les services visés diffusant des contenus à caractère pornographique **doivent permettre de distinguer les utilisateurs mineurs des utilisateurs majeurs**. Il est attendu que les solutions évoluent avec l'amélioration des techniques et la mise sur le marché de nouveaux systèmes de vérification de l'âge, notamment tout standard européen qui émergerait à court terme.

Lorsque la solution technique mise en place par les services visés diffusant des contenus à caractère pornographique repose sur une estimation de l'âge de l'utilisateur, le respect de la loi implique qu'elle doit être paramétrée de sorte à exclure le risque qu'un utilisateur mineur soit considéré comme majeur (« faux positifs »).

Pour respecter la loi, les services visés diffusant des contenus à caractère pornographique doivent fournir leurs meilleurs efforts, conformément aux normes élevées du secteur en matière de diligence professionnelle, **pour limiter les possibilités de contournement des solutions techniques qu'ils mettent en place**. Les systèmes de vérification de l'âge ne doivent pas permettre le partage de preuves d'âge avec d'autres personnes afin de limiter les risques de fraude. Ainsi, le système doit être robuste face aux risques d'attaques, tels que l'hypertrucage (*deepfakes*), l'usurpation d'adresses internet (*spoofing*), etc.

---

[13] « *Restricted to adults* ».

[14] Les *headers* sont des informations renvoyées par le serveur du site internet à destination du navigateur de l'utilisateur au moment d'une requête.

Par exemple, s'agissant des solutions reposant sur une **estimation de l'âge par analyse des traits du visage**, les services visés diffusant des contenus à caractère pornographique devront s'assurer que les solutions comportent un **mécanisme de reconnaissance du vivant**, dont il est attendu que l'efficacité soit conforme à l'état de l'art. La détection doit être effectuée au moyen d'une qualité d'image suffisante et permettre d'exclure tout procédé de détournement susceptible d'être utilisé par des mineurs afin d'apparaître artificiellement comme majeur, notamment par le recours à des photos, vidéos enregistrées ou encore des masques. Enfin, s'agissant des solutions techniques de génération de preuve d'âge fondées sur la présentation d'une pièce d'identité physique, il est attendu que les services visés diffusant des contenus à caractère pornographique s'assurent que les solutions techniques qu'ils mettent en place permettent de vérifier : (i) que le document est réel, et qu'il ne s'agit pas d'une simple copie ; (ii) que l'utilisateur est bien le détenteur du document d'identité renseigné. Cette vérification peut notamment s'effectuer par le biais d'une reconnaissance des traits du visage impliquant un mécanisme de détection du vivant, dans les conditions énoncées *supra*.

Afin d'empêcher l'exposition des mineurs aux contenus à caractère pornographique en ligne, il est attendu que la vérification de l'âge **ait lieu à chaque consultation d'un service**. Ainsi, l'interruption de cette consultation doit déclencher une nouvelle vérification de l'âge en cas de souhait d'un nouvel accès à un contenu pornographique. Ceci est sans préjudice de la possibilité, pour l'utilisateur, de recourir à une preuve d'âge réutilisable ou regénérée par lui-même, sous réserve de la présence d'un second facteur d'authentification. Celle-ci peut être effectuée en liant l'usage de la preuve réutilisable au terminal de la personne concernée, comme cela est le cas s'agissant des portefeuilles numériques (dits « *wallets* »).

Par ailleurs, **le système de vérification ne doit pas permettre le partage de cette preuve avec une autre personne ou un autre service**. Dans l'hypothèse d'un terminal de consultation partagé entre une personne majeure et une personne mineure, il convient d'empêcher que la durée de validité de la vérification de l'âge permette de consulter des contenus pornographiques sans nouvelle vérification. Il peut être considéré que la validité d'une vérification d'âge doit donc s'interrompre lorsque l'utilisateur quitte le service, c'est-à-dire lorsque la session prend fin, lorsque l'utilisateur quitte son navigateur ou lorsque le système d'exploitation entre en veille et, en tout état de cause, après une période d'une heure d'inactivité.

Pour éviter que la réutilisation de compte utilisateur ne conduise des mineurs à accéder à des contenus pornographiques, il est attendu que, la preuve d'âge ne puisse pas être conservée dans un compte utilisateur sur le service visé. En toute hypothèse, il résulte de la loi que l'obligation de vérification de l'âge s'applique à chaque accès, avec ou sans compte utilisateur.

Pour assurer la protection des mineurs et le respect de la loi, il est attendu que les solutions déployées par les services visés diffusant des contenus à caractère pornographique soient **efficaces pour tous les groupes de population et n'aient donc pas pour effet d'en discriminer certains**, notamment selon les motifs énoncés à l'article 21 de la Charte des droits fondamentaux de l'Union européenne. Ainsi, l'efficacité de la solution technique de vérification d'âge sera la même quelles que soient les caractéristiques physiques de l'utilisateur. S'agissant des systèmes de génération de preuve d'âge basés sur l'apprentissage machine (dit aussi « *machine learning* ») ou des modèles statistiques, les

prestataires peuvent, par exemple, tester leur solution sur des bases de données diversifiées afin de s'assurer du respect de cette exigence. En effet, il est essentiel que les systèmes de contrôle de l'âge **limitent les biais discriminatoires, qui génèrent en outre des erreurs susceptibles de remettre en cause tant leur fiabilité que leur acceptabilité**. Les services visés diffusant des contenus à caractère pornographique sont invités à intégrer les éventuels biais discriminatoires, déclinés en fonction des motifs de discrimination pertinents, dans l'évaluation de la performance de leur système de vérification de l'âge, mais aussi au titre des audits auxquels ils procéderaient (v. *infra*).

Deuxième partie : protection de la vie privée

Le présent référentiel vise également à assurer la **protection de la vie privée des utilisateurs** des systèmes de vérification de l'âge. En effet, ces systèmes peuvent présenter des risques élevés en matière de sécurité des données à caractère personnel, la vérification de l'âge s'apparentant à une vérification d'identité, et pouvant à ce titre nécessiter la collecte de données sensibles ou de documents d'identité.

Les acteurs impliqués dans les systèmes de vérification de l'âge doivent donc être particulièrement attentifs à la protection de la vie privée de leurs utilisateurs et à la sécurité des systèmes d'information concernés, principes au respect desquels la CNIL est chargée de veiller en application notamment du règlement général sur la protection des données (RGPD).

Principes de protection de la vie privée

En pratique, les systèmes de vérification de l'âge dans leur ensemble doivent être respectueux de la législation en vigueur concernant la protection des données à caractère personnel et la vie privée, dont les **principes de minimisation et de protection des données dès la conception et par défaut** (articles 5 et 25 du RGPD).

Les prestataires de tels systèmes doivent prêter notamment attention aux principes suivants :

- exactitude, proportionnalité et minimisation des données collectées ;
- information des utilisateurs concise, transparente, compréhensible et facilement accessible ;
- durées de conservation des données appropriées ;
- possibilité pour les personnes d'exercer leurs droits, à savoir le droit d'accès, le droit d'opposition, le droit de rectification, le droit à la limitation du traitement, le droit à l'effacement, le droit à la portabilité ;
- sécurité à l'état de l'art pour les systèmes d'information utilisés dans le cadre de traitements de données à caractère personnel.

Mise en œuvre d'un système de vérification de l'âge respectueux de la vie privée par défaut et par conception

En 2022, la CNIL a publié un démonstrateur de mécanisme de vérification de l'âge respectueux de la vie privée pour la transmission d'un attribut d'identité (en l'occurrence une preuve d'âge)[15, 16]. Le mécanisme proposé permet notamment de garantir l'étanchéité entre les services visés diffusant des contenus à caractère pornographique ayant l'obligation de vérifier l'âge de leurs utilisateurs et les tiers émetteurs d'attributs d'âge.

Ce mécanisme, connu depuis sous l'appellation de « double anonymat » ou « double confidentialité », a fait l'objet de développements et d'expérimentations par différents acteurs publics et privés, permettant de confirmer sa faisabilité technique et sa capacité à

[15] https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee
[16] https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie

répondre au besoin de protection de la vie privée inhérent aux mécanismes de vérification de l'âge en ligne. Il correspond par ailleurs aux objectifs fixés en général aux systèmes d'identité numérique incluant une gestion des attributs. Toutefois, ce mécanisme, bien qu'il soit désigné par « double anonymat » dans le présent document, n'est pas « anonyme » au sens du RGPD, mais garantit cependant une grande confidentialité.

Les services de communication au public en ligne qui mettent à disposition des contenus pornographiques devront proposer à leurs utilisateurs au moins un dispositif de vérification de l'âge conforme aux standards de protection de la vie privée en « double anonymat », en s'assurant que ce système puisse être utilisé par une large majorité de ses utilisateurs.

Cette exigence entrera en vigueur à la fin de la période transitoire prévue dans la troisième partie du présent référentiel, fixée à six mois après sa publication, sans préjudice des exigences minimales énoncées *infra*. Ainsi, jusqu'à cette date, les systèmes de vérification de l'âge devront respecter le socle minimum d'exigences prévues ci-dessous afin de garantir un niveau acceptable de protection des données à caractère personnel de leurs utilisateurs.

Les sections suivantes précisent :

- les exigences applicables à tous les systèmes de vérification de l'âge visés par le présent référentiel ;
- les objectifs spécifiques pour les systèmes les plus respectueux de la vie privée, dits en « double anonymat » ;
- les obligations de transparence visant à informer les utilisateurs du niveau de protection de la vie privée attachées aux dispositifs proposés sur les services ;
- ainsi que des bonnes pratiques énoncées comme souhaitables mais non exigées à ce jour.

Exigences minimales applicables à tous les systèmes de vérification de l'âge

Un **socle minimum d'exigences est applicable à tous les systèmes de vérification de l'âge visés par le présent référentiel :**

1. Indépendance du prestataire de système de vérification de l'âge vis-à-vis des services visés diffusant des contenus à caractère pornographique

Le prestataire de systèmes de vérification de l'âge doit être indépendant juridiquement et techniquement de tout service de communication au public en ligne visé par le présent référentiel et garantir que les services visés diffusant des contenus à caractère pornographique n'aient en aucune circonstance accès aux données servant à vérifier l'âge de l'utilisateur.

- **2. Confidentialité vis-à-vis des services visés diffusant des contenus à caractère pornographique**

Les **données à caractère personnel** permettant à l'utilisateur de vérifier son âge auprès d'un service de communication visé par le présent référentiel **ne doivent pas être traitées par ce service de communication.**

En particulier, la mise en œuvre de solutions de vérification de l'âge **ne doit pas permettre aux services de communication visés par le présent référentiel de collecter l'identité, l'âge, la date de naissance ou d'autres informations à caractère personnel de ces utilisateurs**.

- **3. Confidentialité vis-à-vis des prestataires de génération de preuve d'âge**

Lorsque le système de vérification de l'âge ne permet pas à l'utilisateur d'obtenir une identité numérique ou une preuve d'âge réutilisable, **les données à caractère personnel fournies par l'utilisateur en vue d'obtenir cet attribut ne doivent pas être conservées par le prestataire de génération de preuve d'âge.**

De plus, ce type de système ne doit pas requérir la collecte de documents officiels d'identité, s'il ne permet pas de générer une preuve d'âge réutilisable.

Cette exigence est sans préjudice du respect des obligations légales et règlementaires qui s'appliquent à certains prestataires de génération de preuve d'âge par ailleurs.

- **4. Confidentialité vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge**

Lorsque des tiers autres que les prestataires de génération de preuve d'âge sont impliqués dans le processus de vérification de l'âge, par exemple pour la gestion des preuves ou de la facturation du service, **ces tiers ne doivent pas conserver de données à caractère personnel des utilisateurs du système,** sauf pour le stockage d'une preuve à la demande de l'utilisateur.

- **5. Mesures de sauvegarde des droits et libertés des personnes par les vérificateurs de l'âge**

Lorsqu'il détermine si un utilisateur peut accéder ou non à un service de communication au public en ligne sur la base de la preuve qui lui est soumise, le service visé diffusant des contenus à caractère pornographique prend une décision automatisée au sens de l'article 22 du RGPD. En effet, en refusant l'accès à un service, cette décision est susceptible de produire des effets juridiques sur les personnes concernées, ou au minimum, produit des effets significatifs affectant les personnes de façon similaire.

La CNIL considère qu'une telle décision peut être fondée sur l'exception prévue au paragraphe 2.b. de l'article 22 du RGPD, dans la mesure où le service visé diffusant des

contenus à caractère pornographique est soumis à une obligation de vérification de l'âge prévue à l'article 227-24 du code pénal et les dispositions de la loi SREN. L'article 22.2.b du RGPD impose que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée soient prévues par les dispositions autorisant cette décision automatisée.

Afin de préserver les exigences en matière de protection de la vie privée qui visent à limiter la capacité des services à identifier les personnes, de telles mesures doivent être mises en place non par le service visé diffusant des contenus à caractère pornographique, mais par le prestataire de solution technique de vérification de l'âge, qu'il soit le fournisseur d'attribut ou l'émetteur de preuve. De telles mesures doivent permettre aux utilisateurs, en cas d'erreur, de contester le résultat de l'analyse de leur attribut afin d'obtenir une preuve d'âge. Pour l'exercice de ces voies de recours, ces prestataires de solution de vérification de l'âge devraient proposer aux utilisateurs de recourir à différents fournisseurs d'attributs ou, selon les solutions, à différents émetteurs de preuve.

Le service visé diffusant des contenus à caractère pornographique est tout de même tenu, comme les prestataires de solution technique de vérification de l'âge, de se conformer aux obligations en matière d'information imposées par le RGPD et doit prévenir les utilisateurs de la possibilité d'exercer un recours auprès du fournisseur de la solution de vérification de l'âge.

En tout état de cause, les fournisseurs d'attributs doivent également permettre aux personnes de rectifier leurs données en vertu de l'article 16 du RGPD.

Exigences spécifiques pour les systèmes protecteurs de la vie privée respectant le principe de « double anonymat »

Les objectifs suivants complètent les objectifs du socle minimal pour définir un standard respectueux de la vie privée en matière de vérification de l'âge en ligne.

- **6. Confidentialité renforcée vis-à-vis des services visés diffusant des contenus à caractère pornographique**

Les exigences prévues au n° 2 sont complétées des suivantes.

Un système de vérification de l'âge utilisant le « double anonymat » ne doit pas permettre aux services de communication visés par le présent référentiel de reconnaître un utilisateur ayant déjà utilisé le système sur la base des données générées par le processus de vérification de l'âge.

L'utilisation de systèmes de vérification de l'âge utilisant le « double anonymat » ne doit pas permettre à ces services de connaître ou de déduire la source ou la méthode d'obtention des preuves d'âge impliquées dans le processus de vérification de l'âge d'un utilisateur.

Un système de vérification de l'âge respectueux de « double anonymat » ne doit pas permettre à ces services de pouvoir reconnaître que deux preuves de majorité proviennent d'une même source de preuves d'âge.

- **7. Confidentialité renforcée vis-à-vis des émetteurs d'attributs d'âge**

Les exigences prévues au n° 3 sont complétées de sorte qu'un système de vérification de l'âge utilisant le « double anonymat » ne doit pas permettre aux prestataires de génération de preuve d'âge de savoir pour quel service la vérification d'âge est effectuée.

- **8. Confidentialité renforcée vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge**

Les exigences prévues au n° 4 sont complétées des exigences suivantes :

Un système de vérification de l'âge utilisant le « double anonymat » **ne doit pas permettre aux éventuels autres tiers impliqués dans le processus de reconnaître un utilisateur ayant déjà utilisé le système.** Par exemple, un tiers assurant la transmission d'une preuve d'âge ou certifiant sa validité ne doit pas être en mesure de savoir s'il a déjà traité une preuve du même utilisateur.

- **9. Disponibilité et couverture de la population**

Les services de communication visés par le présent référentiel doivent s'assurer que leurs utilisateurs disposent **d'au moins deux méthodes de génération de preuve d'âge différentes permettant l'obtention d'une preuve d'âge par le biais d'un système de vérification d'âge en « double anonymat »**. En pratique, un prestataire proposant une solution en double anonymat doit y associer au moins deux modalités d'obtention d'une preuve d'âge (par exemple, une solution basée sur les documents d'identité et une solution basée sur l'estimation d'âge).

Les services de communication visés par le présent référentiel doivent s'assurer qu'un dispositif de vérification de l'âge en « double anonymat » est disponible pour au moins 80 % de la population majeure résidant en France.

Exemples et application

Concrètement, les solutions en « double anonymat » doivent proposer **plusieurs prestataires de génération de preuve d'âge** (par exemple, différents fournisseurs d'accès à internet et/ou banques) et pour les autres solutions, **différentes modalités de génération de preuve âge** (analyse des traits du visage et fourniture de document d'identité par exemple).

Information des utilisateurs sur le niveau de protection de la vie privée attaché aux dispositifs de vérification de l'âge

- **10. Affichage explicite du niveau de protection de la vie privée des utilisateurs**

Chaque solution de vérification de l'âge doit être explicitement associée à son niveau de protection de la vie privée, de sorte que les solutions respectant les standards de « double anonymat » soient affichées de manière claire et lisible. En tout état de cause, les autres solutions ne doivent pas être confondues ou mises en valeur afin de tromper l'utilisateur en faveur de solutions moins protectrices de la vie privée.

Lorsqu'un tiers participant au processus de vérification d'âge peut connaître le service pour lequel la vérification de l'âge est faite, l'utilisateur doit en être clairement informé.

S'agissant des systèmes de vérification d'âge conformes au principe de « double anonymat », l'utilisateur doit être clairement informé que cette solution garantit que le fournisseur de la vérification d'âge ne peut pas connaître le service pour lequel cette vérification est faite.

Objectifs souhaitables et bonnes pratiques

Les objectifs ci-après ne sont à ce jour pas exigibles des systèmes de vérification de l'âge pour la conformité au présent référentiel, mais constituent **un ensemble de bonnes pratiques vers lequel les solutions de vérification de l'âge devraient tendre**.

Capacité pour l'utilisateur de générer lui-même des preuves d'âge de façon confidentielle :

- l'utilisateur peut générer une preuve d'âge localement, sans informer l'émetteur initial de ses attributs d'âge, ni un autre tiers ;
- l'utilisateur peut générer une preuve d'âge via un service en ligne et utilisable sans disposer d'aucun accès à ses données à caractère personnel.

Confidentialité des systèmes de vérification de l'âge dans leur ensemble :

- le système repose sur des preuves à divulgation nulle de connaissance (*« zero knowledge proof »*) ;
- le système repose sur des techniques de chiffrement possédant des propriétés de résistance aux attaques les plus complexes, y compris dans le futur.

<u>Troisième partie :</u> solutions de génération de preuve dérogatoires acceptées à titre temporaire

En application de l'article 10 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, les services assujettis mettent en œuvre un système de vérification de l'âge conforme aux caractéristiques techniques du présent référentiel dans un délai de trois mois à compter de sa publication. Néanmoins, à l'issue de ces trois mois, les services assujettis peuvent, pendant une **période transitoire de trois mois**, destinée à leur permettre d'identifier et de mettre en place une solution de vérification de l'âge satisfaisant l'ensemble des première et deuxième parties, mettre en œuvre des solutions **utilisant la carte bancaire, qui seront réputées conformes aux caractéristiques techniques du référentiel, sous réserve de respecter les conditions suivantes.**

Une solution utilisant la carte bancaire constituerait une première modalité de filtrage d'une partie des mineurs. Cette solution temporaire repose en effet sur une infrastructure déjà déployée et mobilisable.

Sous réserve du respect des exigences ci-dessous, cette solution permettrait dans un premier temps de **protéger les mineurs les plus jeunes**. Le filtrage doit s'opérer par une authentification forte (c'est-à-dire à double facteur). À titre d'exemple, il peut ainsi s'opérer soit *via* une authentification forte seule (sans paiement), soit *via* un paiement (y compris d'un montant de zéro euro) couplé à une authentification forte.

<u>Ces systèmes de vérification</u> :

- ne doivent pas être mis en œuvre directement par les services visés diffusant des contenus à caractère pornographique, mais par un **tiers indépendant du service** ;

- devront **veiller à la sécurité de la vérification**, afin de prévenir les risques d'hameçonnage qui y seront associés. Il convient donc de s'assurer que les informations de paiement sont bien saisies sur des sites de confiance. Il serait souhaitable à cet égard que les services visés diffusant des contenus à caractère pornographique et les fournisseurs de solutions lancent de manière coordonnée une campagne de sensibilisation aux risques d'hameçonnage, tenant notamment compte de cette nouvelle pratique ;

- devront permettre au minimum de **s'assurer de l'existence et de la validité de la carte**, ce qui exclut une simple vérification de la cohérence du numéro de la carte ;

- mettent en œuvre l'authentification forte prévue par la directive européenne (UE) 2015/2366 relative aux services de paiement (dite « DSP2 »), par exemple en s'appuyant sur le **protocole 3-D Secure**, dans sa deuxième version en vigueur, pour s'assurer que l'utilisateur du service est le titulaire de la carte au moyen d'une authentification à double facteur.

<u>Quatrième partie :</u> audit et évaluation des solutions de vérification de l'âge

La loi SREN prévoit que *« L'Autorité de régulation de la communication audiovisuelle et numérique peut exiger des éditeurs et fournisseurs de services* […] *qu'ils* ***conduisent un audit des systèmes de vérification de l'âge qu'ils mettent en œuvre afin d'attester de la conformité de ces systèmes avec les exigences techniques définies par le référentiel****. Le référentiel précise les modalités de réalisation et de publicité de cet audit, confié à un organisme indépendant disposant d'une expérience avérée. »*

Les sections suivantes visent à préciser les grands principes susceptibles de guider les services visés diffusant des contenus à caractère pornographique qui seraient amenés à procéder à la réalisation d'un tel audit.

Évaluation en conditions réelles des systèmes mis en place

Afin de garantir une protection des mineurs élevée, l'Arcom évaluera les solutions techniques de vérification de l'âge au cas par cas, une fois mise en place par les éditeurs, c'est-à-dire *in concreto*. En effet, certaines solutions étant paramétrables par les services visés diffusant des contenus à caractère pornographique eux-mêmes, il convient d'effectuer une évaluation dans les conditions d'exercice réel.

Les services visés diffusant des contenus à caractère pornographique sont tenus de s'assurer que les solutions mises en place sont systématiquement en mesure de répondre aux exigences du référentiel en adaptant, le cas échéant, leurs principes et leurs paramètres de fonctionnement.

Taux d'erreur, contournement et risques d'attaque

L'audit technique s'attache à évaluer, d'une façon générale, le respect par la solution de vérification de l'âge de la loi et de **l'ensemble du présent référentiel**.

À cet égard, il évalue tout particulièrement :

- la capacité de la solution technique à distinguer les utilisateurs mineurs ;
- l'absence de biais discriminatoires ;
- la résistance aux pratiques de contournement potentielles (*deepfakes*, par exemple) et aux risques d'attaque[17].

Indépendance du prestataire d'audit

Afin de ne pas entacher la crédibilité de l'audit, il convient que l'auditeur dispose d'une expertise et d'une expérience avérée et qu'il soit **indépendant** tant des sociétés proposant les solutions de vérification de l'âge que des services visés diffusant des contenus à caractère pornographique qui emploient ladite ou lesdites solutions techniques.

[17] L'évaluation des risques d'attaques d'une solution de vérification d'âge consiste à déterminer si le système est susceptible d'être détourné à des fins de fraude.

L'Arcom pourra, dans une version ultérieure du présent référentiel, préciser les conditions dans lesquelles les audits doivent être réalisés et mis à la disposition du public.

En l'état, et dans l'attente des précisions qui pourront être apportées ultérieurement par l'Arcom, les entreprises sont encouragées à réaliser des audits techniques de leurs systèmes de vérification d'âge, d'abord sous six mois à compter de la publication du présent référentiel puis au moins **chaque année**.

Les services visés diffusant des contenus à caractère pornographique sont incités également à **publier leur rapport d'audit au sein d'une page facilement accessible de leur interface en ligne, et dans un format aisément compréhensible**, par souci de transparence notamment envers les utilisateurs.