ADAN

Document de travail
Confidentiel

Consultation de l'ARCOM sur le référentiel de vérification d'âge

Réponse de l'Adan

Introduction

Le 11 avril 2024, l'Autorité française de régulation de la communication audiovisuelle et numérique (ARCOM) a publié une consultation publique concernant le projet de référentiel visant à établir les exigences techniques minimales pour les systèmes de vérification de l'âge, destinés à restreindre l'accès des mineurs à des contenus pornographiques en ligne. S'inscrivant dans le cadre de l'interdiction du 1er mars 1994 de l'article 227-24 du Code pénal, cette interdiction vise à protéger les jeunes publics contre les risques associés à l'exposition précoce à des contenus sensibles. Elle a été renforcée au fil des années par diverses législations et mesures réglementaires. L'initiative de ce référentiel représente donc une étape supplémentaire dans l'effort de régulation, en veillant à ce que les plateformes diffusant ce type de contenu respectent effectivement leurs obligations tout en utilisant des systèmes respectueux de la vie privée des utilisateurs.

En synthèse, l'Adan soutient fermement les principes de protection de la vie privée et de confidentialité intégrés au projet de référentiel de l'ARCOM. L'association promeut activement des solutions Web 3 innovantes, qui répondent non seulement aux exigences réglementaires mais vont au-delà en minimisant la collecte et la conservation de données personnelles, conformément au Règlement européen 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, dit "RGPD".

L'Adan salue l'initiative prise par l'Autorité française de régulation de la communication audiovisuelle et numérique d'ouvrir cette consultation publique. Il apparaît en effet opportun que les acteurs déployant des solutions de vérification d'âge puissent, grâce à leur expertise, enrichir les réflexions sur les standards qui seront définis pour ces systèmes. Les objectifs de l'association sont de promouvoir l'existence de solutions qui répondent adéquatement aux objectifs du régulateur, à savoir protéger les mineurs tout en ayant une gestion strictement respectueuse des données personnelles.

La réponse de l'Adan à la consultation se décline donc en trois axes principaux :

1. Recommande que le référentiel établi puisse permettre l'intégration par les sites en ligne de solutions technologiques Web 3 de pointe tels que les preuves de connaissance zéro (ou *Zero Knowledge Proofs* - ZKP).

2. Soutenir l'ouverture du référentiel à d'autres dispositifs techniques sous réserve qu'elles offrent des garanties similaires ou supérieures que celles proposées par les solutions Web 3 en matière de confidentialité et de sécurité, à savoir qu'elles permettent de garantir l'anonymat des utilisateurs et la fiabilité des informations transmises, sans divulgation de données personnelles superflues et sensibles.

3. Encourager l'édiction de directives claires concernant la qualité et l'indépendance des auditeurs de solutions techniques et la fréquence des audits, assurant que les solutions soient à la fois conformes et économiquement viables pour tous les acteurs, y compris les nouvelles entreprises technologiques. L'association recommande que les audits ne soient pas excessivement fréquents ou coûteux, pour éviter de pénaliser les petites et moyennes entreprises innovantes.

L'Adan fédère et représente 200 professionnels – nouveaux acteurs et entreprises établies – qui développent l'innovation et des cas d'utilisation pour le Web 3 dans tous les secteurs de l'économie.

I. Fiabilité des systèmes de vérification de l'âge

Protection des mineurs par défaut

⇒ *Critère n°1 : étanchéité du contrôle de l'âge*

Concernant le critère n°1 d'étanchéité du contrôle de l'âge, lequel implique 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"*, l'Adan soutient pleinement la démarche. Une précision semble toutefois nécessaire quant à l'application proposée pour le floutage de la page tant que l'âge n'a pas été vérifié. Une attention particulière devrait être portée à la mise en œuvre du floutage afin de garantir qu'il ne soit pas facilement contournable. En effet, il faut savoir qu'un floutage réalisé uniquement *via* un filtre CSS par-dessus le contenu réel peut être aisément supprimé en éditant la page *via* la console du navigateur.

- **Par conséquent, l'Adan recommande l'adoption d'une approche qui renforce davantage la sécurité pour empêcher tout contournement. Par exemple, une solution viable pourrait être l'intégration de la protection directement au niveau du code source de la page, ce qui rendrait plus difficile son contournement. Néanmoins, la faisabilité technique de cette approche devrait faire l'objet d'une analyse afin de s'assurer qu'elle puisse être mise en place de manière efficace et sans compromettre les performances du service.**

Critères de fiabilité

⇒ *Critère n°2 : efficacité de la solution*

Le critère n°2 d'efficacité de la solution vise à évaluer la capacité des dispositifs à différencier de manière précise les utilisateurs mineurs des utilisateurs majeurs, tout en minimisant le risque de faux positifs. Il s'agit donc de déterminer dans quelle mesure les mécanismes de vérification d'âge sont fiables et précis.

Dans cette optique, l'Adan a relevé que les solutions Web3, reposant sur des mécanismes cryptographiques, présentent une particularité intéressante par rapport à d'autres solutions, notamment celles basées sur l'intelligence artificielle (IA). Dans le contexte des solutions Web 3, les utilisateurs sont associés à des portefeuilles numériques (ou *wallets*) qui n'appartiennent qu'à eux et peuvent être associés à des identités numériques préalablement vérifiées et encryptées. Cette attestation de majorité est donc fiable, mais aussi infalsifiable, elle permet donc de réduire significativement le risque de faux positifs.

Si le risque de partage d'un portefeuille avec des personnes mineurs n'est pas nul, la sensibilité des informations qu'il contient peut être un frein naturel pour la majorité des utilisateurs. En effet, il ne semble peu probable qu'un utilisateur partage l'adresse d'un portefeuille donnant accès à l'ensemble de ses données personnelles de la même manière qu'une personne aurait peu de raisons de partager largement ses coordonnées bancaires.

- **Les solutions Web3 offrent une approche extrêmement fiable pour authentifier les utilisateurs et différencier les utilisateurs mineurs des utilisateurs majeurs.**

⇒ *Critère n°3 : limitation des possibilités de contournement*

L'Adan reconnaît pleinement l'importance du critère n°3 relatif à la limitation des possibilités de contournement tel que défini par l'ARCOM dans la consultation. Ce critère implique que la solution soit conçue de manière à prévenir les tentatives et possibilités de contournement.

L'Association estime que plusieurs mesures sont envisageables pour atteindre cet objectif.

Sur l'intégration d'un mécanisme de détection des vivants

L'idée première évoquée par l'ARCOM est l'intégration, au sein de la solution, de mécanismes de détection des "vivants" basés sur les traits du visage de la personne.

L'Adan soutient l'intégration de mécanismes de détection des vivants dans les systèmes de vérification de l'âge et reconnaît les avantages qu'ils apportent en termes de sécurité et de fiabilité. La détection des vivants permet de contrer les tentatives d'usurpation d'identité par l'utilisation de photos ou de vidéos permettant d'identifier des caractéristiques vivantes comme, par exemple, les clignements des yeux, les mouvements de la bouche, et d'autres signes de vie. Il est donc vrai que cette intégration garantit **(i)** que la personne est réellement et actuellement présente devant la caméra et **(ii)** réduit encore le risque de faux positifs ou de faux négatifs.

- **Néanmoins, l'Adan recommande à l'ARCOM de considérer l'automatisation de cette intégration dans le but de trouver un juste équilibre entre la limitation du risque de contournement et la préservation de la vie privée.**

Ainsi :

1. L'application de la technologie de reconnaissance faciale avancée (*via* l'utilisation de l'Intelligence Artificielle, ou "IA") analyse en temps réel les traits du visage et les mouvements biométriques de la personne afin de détecter une présence réelle d'une personne majeure.

2. Après la détection réussie d'une présence vivante, le système peut automatiquement initier une vérification de l'identité *via* des documents sécurisés (passeports ou cartes d'identité équipés de puces RFID) ; en utilisant les données encryptées et sécurisées contenues dans les puces pour authentifier l'identité. L'automatisation dispose de plusieurs avantages : **(i)** application cohérente des critères de vérification ; **(ii)** réduction des erreurs humaines et **(iii)** accélération du processus global.

Au résultat, le couplage de ces deux technologies réduit considérablement le risque de contournement, en ce qu'il confirme non seulement que l'utilisateur est présent et majeur, mais valide aussi son identité par des moyens sécurisés.

- Une telle approche nécessiterait néanmoins de pouvoir garantir que toutes les informations personnelles sont traitées de manière sécurisée et conforme aux réglementations sur la protection des données (notamment au "*Règlement européen 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*", ou "*RGPD*").

Sur la vérification à partir de pièces d'identité

La lecture d'une puce intégrée dans un document biométrique est reconnue comme la méthode la plus fiable pour garantir l'authenticité d'une pièce d'identité. Bien que les documents physiques soient conçus pour être difficilement reproductibles grâce à des méthodes d'impression spéciales et des types d'encre répondant à des longueurs d'onde spécifiques, les caméras des appareils mobiles utilisés par les utilisateurs, notamment les smartphones, ne sont pas toujours capables de détecter l'ensemble de ces détails avec la précision nécessaire lors d'une reconnaissance optique de document. Dès lors, la vérification des signatures cryptographiques contenues dans la puce demeure être le moyen le plus sûr de confirmer que la pièce d'identité est authentique.

S'il est estimé qu'environ 65% de la population possède à ce jour des documents d'identité équipés de puces électroniques en France, ce chiffre est amené à augmenter mécaniquement avec la péremption progressive des pièces d'identité actuellement en circulation. Couper 35% de la population de certains services tel que ce serait le cas à ce jour n'est pas envisageable. **Toutefois, la généralisation des documents d'identité biométriques pourrait permettre de restreindre l'usage de documents alternatifs, augmentant ainsi la fiabilité de la vérification d'attributs avec le temps.**

Un obstacle subsistera cependant à l'utilisation de documents biométriques pour la vérification de l'âge. En effet, la réglementation actuelle limite la capacité de lecture des puces aux entités de l'État, restreignant ainsi l'utilisation de cette méthode par les acteurs privés. Cette restriction, initialement mise en place pour des raisons de sécurité et de

protection de la vie privée, constitue aujourd'hui un obstacle à l'adoption généralisée d'une méthode de vérification de l'âge pourtant sécurisée.

- **L'Adan recommande une évolution du droit afin de permettre à certains acteurs privés la lecture des puces. Cette ouverture, sous strictes conditions de sécurité et de confidentialité, permettrait une utilisation plus large de cette méthode fiable, augmentant ainsi l'efficacité des systèmes de vérification d'âge tout en maintenant des standards élevés de protection des données personnelles.**

⇒ *Critère n°4 : vérification de l'âge à chaque consultation d'un service*

Le critère n°4 implique que chaque fois qu'un utilisateur consulte un service en ligne, une vérification de son âge doit être effectuée. Cette exigence vise à limiter les risques de contournement, notamment lorsque plusieurs individus utilisent un même appareil. Si l'Adan n'a pas d'objection spécifique à ce critère, une fréquence d'identification trop élevée peut être perçue comme contraignante pour les utilisateurs et conduire à une fuite des utilisateurs vers des plateformes non sujettes à la réglementation ou vers des outils de type VPN. Une ligne de crête doit donc ici être suivie afin de préserver l'efficacité de la mesure.

- **Pour répondre à cette exigence tout en préservant l'expérience utilisateur, l'Adan propose deux solutions alternatives :**

    1. **Session anonymisée conservée dans les cookies**. Une première solution technique consiste à utiliser une session anonymisée (et non un compte utilisateur) stockée dans les *cookies* du navigateur. Après avoir réussi la première vérification de l'âge, une session anonyme serait activée et enregistrée dans les *cookies*. Cette session permettrait à l'utilisateur de consulter le service sans avoir à refaire la vérification à chaque fois. Concrètement, une fois qu'un utilisateur a prouvé son âge pour la première fois, une session unique et anonyme est créée et stockée dans les cookies de son navigateur. Cette session contiendrait les informations nécessaires pour confirmer que l'utilisateur a déjà été vérifié et peut donc accéder aux contenus réservés aux adultes sans avoir à refaire la vérification à chaque visite ultérieure.

        Techniquement, cette solution pourrait fonctionner comme suit :

        Après une vérification initiale de l'âge, un jeton JWT est généré et stocké dans les *cookies* de l'utilisateur. Ce token contiendrait un identifiant unique généré aléatoirement, respectant un niveau d'aléa minimum, et une date d'expiration pré-définie. Aucune information supplémentaire sur l'utilisateur n'est stockée à ce stade.

Lorsque la date d'expiration du jeton est atteinte, le jeton perd sa validité, nécessitant ainsi une nouvelle vérification de l'âge pour accéder de nouveau au contenu. Côté serveur, l'identifiant du jeton est conservé pour permettre sa révocation en cas de nécessité, par exemple, si l'utilisateur perd son appareil ou pour d'autres raisons de sécurité.

Pour prévenir l'utilisation et le partage abusif de la preuve d'âge, il est important de mettre en place des mesures pour empêcher la réutilisation du jeton par une autre personne. En outre, pour éviter une mauvaise utilisation de cette session anonymisée, il est proposé de cocher préalablement une case si l'appareil est utilisé exclusivement par eux. Cette démarche permettrait de responsabiliser les parents et de ne pas activer cette option si l'appareil est partagé avec des mineurs.

Cette approche propose un compromis entre la facilité d'utilisation et la conformité aux exigences de protection des mineurs, tout en mettant l'accent sur la responsabilisation des parents dans la gestion de l'accès aux contenus à caractère adulte. En termes de durée de la session, une période de 24 à 48 heures pourrait être envisagée pour équilibrer entre accessibilité et sécurité, bien que techniquement des durées plus courtes soient possibles et puissent être ajustées en fonction des retours des utilisateurs et des considérations de sécurité.

2. **Signature d'une connexion (tx) associée à une adresse (wallet)**. Chaque utilisateur aurait une adresse de wallet unique, et chaque fois qu'il effectue une vérification de l'âge, une transaction cryptographique (tx) serait générée. Cette transaction ne contiendrait aucune donnée personnelle de l'utilisateur, mais serait uniquement signée numériquement par l'adresse du wallet de l'utilisateur. Cette signature prouve que l'utilisateur possède la clé privée correspondant à l'adresse du wallet sans révéler d'informations personnelles.

⇒ *Critère n°5 : encadrement du recours à un compte utilisateur*

L'Adan soutient pleinement le critère n°5 relatif à l'encadrement du recours à un compte utilisateur, indiquant qu'une **solution de vérification de l'âge ne doit pas contraindre les utilisateurs à créer un compte pour accéder à des contenus à caractère pornographique.** Cette directive préserve la confidentialité des utilisateurs en évitant la collecte de données personnelles, particulièrement sensibles dans ce contexte. En conséquence, l'Adan approuve l'approche de l'ARCOM, qui affirme que la vérification de l'âge peut et doit être effectuée efficacement sans imposer de barrières supplémentaires susceptibles de dissuader un accès légitime et sécurisé à ces contenus.

⇒ *Critère n°6 : non-discrimination*

Selon le critère n°6 relatif à la non-discrimination, les solutions de vérification de l'âge ne doivent pas discriminer certains groupes d'utilisateurs. S'il est vrai que ce critère est particulièrement pertinent pour les technologies basées sur l'apprentissage automatique (ou *machine learning*), il ne l'est pas pour les solutions Web 3 que l'Adan présente à l'ARCOM, qui sont technologiquement neutres et objectives. En effet, elles sont exemptes des risques de biais qui sont associés aux solutions basées sur l'apprentissage automatique.

- **Pour les systèmes qui emploient l'apprentissage automatique, il serait effectivement prudent d'exiger de mener des tests préalables pour s'assurer de l'absence de discrimination.**

II. Protection de la vie privée

Dans le contexte actuel où la protection de la vie privée devient un sujet d'importance majeure pour l'ensemble des individus - et ce notamment en matière de vérification d'âge pour l'accès à des contenus sensibles en ligne - les solutions dites Web3 présentées par l'Adan se distinguent particulièrement par leur adhérence stricte aux principes de minimisation des données et de protection dès la conception. Ces solutions garantissent que rien n'est conservé qui puisse compromettre l'anonymat des utilisateurs. Cette approche est d'autant plus pertinente qu'elle répond au droit à l'oubli, lequel offre aux utilisateurs le droit de contrôler l'effacement de leurs données, conformément à l'**Article 17** du RGPD.

Par ailleurs, l'usage intensif de méthodes de vérification basées sur des documents d'identité, comme le passeport avec vérification par puce NFC, peut sembler disproportionné pour accéder à des contenus pornographiques. Cette observation souligne l'importance de proportionnalité dans la collecte de données, un principe fondamental du RGPD trouvant une assise textuelle à l'**Article 6**, **paragraphe 3** du Règlement, et qui préconise la collecte et l'utilisation des données strictement nécessaires. Les solutions Web3, en utilisant des techniques telles que les preuves à divulgation nulle de connaissance (ZKPs), offrent un compromis entre la nécessité de vérifier l'âge et le besoin impératif de minimiser l'empreinte des données personnelles des utilisateurs.

Principes de protection de la vie privée

D'après la consultation, 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.

Comme évoqué ci-dessus, l'Adan soutient fermement le respect des principes énoncés dans la consultation concernant la protection de la vie privée, soulignant leur alignement avec les exigences du RGPD. L'accent mis sur la minimisation des données, la transparence de l'information, des durées de conservation appropriées, ainsi que le respect des droits des utilisateurs garantira une gestion responsable et sécurisée des données personnelles.

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

⇒ *Critère n°7 : indépendance du prestataire de système de vérification de l'âge vis-à-vis des services visés diffusant des contenus à caractère pornographique*

Le critère n°7 de la consultation pose la question de l'indépendance juridique et technique des prestataires de systèmes de vérification de l'âge vis-à-vis des services diffusant des contenus à caractère pornographique. Ce point est important en ce sens qu'il garantit l'objectivité et la fiabilité des processus de vérification, en évitant tout conflit d'intérêts potentiel qui pourrait compromettre l'intégrité de ces systèmes, notamment que les sites de communication en ligne développent en interne des systèmes de vérification.

L'ARCOM devrait clarifier ce qu'elle entend précisément par *"indépendance juridique"* afin de comprendre les limites exactes de cette indépendance, surtout pour les petits acteurs du secteur et les entreprises du Web 3 qui pourraient développer des solutions innovantes pour ce marché. La possibilité pour ces acteurs de contribuer à la palette de solutions disponibles pourrait être affectée si l'indépendance est définie de manière trop restrictive. En outre, l'ARCOM devrait déterminer si l'indépendance nécessaire entre le prestataire du système de vérification de l'âge et les services diffusant des contenus à caractère pornographique implique une séparation totale au sein d'un même groupe d'entreprises, ou si elle permet une certaine flexibilité opérationnelle tout en garantissant l'étanchéité du processus de vérification. Si l'interprétation de l'indépendance exige que les entités de vérification et d'émission de preuve d'âge soient totalement distinctes et non affiliées, cela pourrait non seulement restreindre le nombre de solutions disponibles ainsi que le financement permettant de les développer et donc de multiplier leur disponibilité sur le marché.

- **L'Adan suggère donc que l'ARCOM envisage une définition de l'"indépendance juridique" qui permette aux entreprises du même groupe de proposer des solutions**

de vérification, à condition qu'elles puissent démontrer une séparation opérationnelle et technique claire qui préserve l'intégrité et l'objectivité de la vérification. Dans un secteur où divers acteurs, y compris des entreprises émergentes, sont en mesure de proposer des solutions, il serait judicieux de permettre une variété d'options initiale pour non seulement stimuler l'innovation mais aussi évaluer différentes approches en termes d'efficacité et de conformité, avant de potentiellement resserrer les critères d'approbation. Une restriction trop précoce pourrait limiter sévèrement les solutions disponibles et, par extension, l'effectivité de la loi elle-même.

⇒ *Critère n°8 : confidentialité vis-à-vis des services visés diffusant des contenus à caractère pornographique*

L'Adan n'a pas de commentaire sur ce critère.

⇒ *Critère n°9 : confidentialité vis-à-vis des prestataires de génération de preuve d'âge*

L'Adan n'a pas de commentaire sur ce critère, si ce n'est rappeler que les solutions Web3 sont en conformité avec ce critère puisqu'elles n'ont ni besoin de conserver les données ni de les faire transiter en dehors de l'appareil de l'utilisateur. D'un point de vue technique, ces solutions reposent sur une technologie de chiffrement qui laisse à l'utilisateur le soin de contrôler ses propres données sans avoir à les partager avec des tiers. Dès lors, seules les informations nécessaires à la vérification de l'âge sont utilisées, sans être stockées ou partagées de manière centralisée. Notons que ces solutions s'alignent parfaitement avec les principes de protection des données définis par le règlement RGPD (voir *supra*).

⇒ *Critère n°10 : confidentialité vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge*

L'Adan estime que lorsque des tiers autres que les prestataires de génération de preuve d'âge sont impliqués dans le processus de vérification de l'âge, comme dans la gestion des preuves ou la facturation du service, ces acteurs ne doivent pas conserver de données à caractère personnel des utilisateurs. La seule exception serait le stockage d'une preuve d'âge, mais uniquement à la demande expresse de l'utilisateur.

⇒ *Critère n°11 : mesures de sauvegarde des droits et libertés des personnes par les vérificateurs de l'âge*

L'Adan n'a pas de commentaire sur ce critère.

Exigences spécifiques pour les systèmes protecteurs de la vie privée respectant le principe de “double anonymat”

⇒ *Critère n°12 : confidentialité renforcée vis-à-vis des services visés diffusant des contenus à caractère pornographique*

En ce qui concerne le critère 12 du référentiel ARCOM sur la confidentialité renforcée vis-à-vis des services visés diffusant des contenus à caractère pornographique, l'Adan note que, dans certaines solutions Web 3 basées sur les titres d'identité, il est possible de déduire le type de vérification utilisée. Cela ne compromet pas pour autant l'anonymat de la méthode : la seule information divulguée, outre la majorité de l'utilisateur, est le type de vérification, ce qui n’entre pas dans la définition “*donnée personnelle*” au sens du RGPD.

Au-delà de cet aspect, l'exigence de ne pas pouvoir déduire la méthode de preuve d'âge semble potentiellement inadaptée à certaines technologies de pointe comme les *zero knowledge proofs* (preuves à divulgation nulle de connaissance en français). Dans les systèmes utilisant les *zk-SNARKs*, par exemple, il est essentiel de pouvoir identifier que la preuve provient d'une source fiable (par exemple les services de l'État) sans pour autant compromettre l'anonymat de l'utilisateur. Cette capacité à vérifier l'origine de la preuve sans accéder à d'autres détails personnels est cruciale pour préserver à la fois la sécurité et la confidentialité des utilisateurs.

- **L'Adan recommande à l'ARCOM de reconsidérer ou préciser ce critère pour prendre en compte les nuances des technologies de vérification de l'âge qui permettent d'attester de la fiabilité de la source sans compromettre la confidentialité des données personnelles. Il est important de maintenir une flexibilité dans les normes pour soutenir l'innovation technologique tout en assurant une protection efficace des utilisateurs. L'incapacité de déterminer l'émetteur d'une preuve pourrait ouvrir la voie à des acteurs malveillants qui pourraient exploiter cette opacité pour émettre des preuves non fiables, ce qui compromettrait l'intégrité du système de vérification de l'âge.**

⇒ *Critère n°13 : confidentialité renforcée vis-à-vis des émetteurs d’attributs d’âge*

En vertu de ce critère, 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. L'Adan souligne que, bien que cette mesure renforce la confidentialité, elle pourrait complexifier la gestion de la facturation, car il est essentiel pour les opérateurs de connaître l'entité demandant la vérification afin d'attribuer les coûts appropriés. Notons toutefois que cette opération peut déjà être menée sans nécessiter l'accès à des informations personnelles sur les utilisateurs.

⇒ *Critère n°14 : confidentialité renforcée vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification de l'âge*

Selon le critère n°14 du référentiel ARCOM, la confidentialité renforcée dans les processus de vérification de l'âge, particulièrement concernant les tiers impliqués, doit être assurée. L'Adan n'a pas de commentaire particulier sur ce critère mais tient à souligner les avantages des solutions Web 3 dans le respect de ce critère. En effet, les solutions Web 3 garantissent une vérification de l'âge sans nécessiter de stockage centralisé des données personnelles, ce qui réduit significativement les risques d'accès ou d'usage inapproprié des données par des tiers et permet d'assurer une confidentialité renforcée conformément aux exigences du référentiel ARCOM.

De plus, en utilisant les solutions dites Web3, les processus de vérification maintiennent l'anonymat des utilisateurs tout en validant leur âge, ce qui prévient efficacement le risque de retraitement ou de suivi de l'activité des utilisateurs par des tiers non autorisés. Cette approche s'aligne de nouveau parfaitement avec les principes de protection de la vie privée par conception et par défaut (et renforce par ailleurs la confiance des utilisateurs dans l'utilisation des services en ligne respectueux de leur vie privée).

⇒ *Critère n°15 : disponibilité et à la couverture de la population*

Le critère n°15 exige que les services de vérification d'âge offrent au moins deux méthodes de génération de preuve et assurent une couverture d'au moins 80% de la population adulte résidant en France.

L'Adan s'interroge sur la pertinence d'exiger deux modalités pour la génération de preuve d'âge, surtout si une seule modalité peut suffisamment couvrir les besoins de vérification tout en respectant la vie privée des utilisateurs. Cette contrainte, uniquement imposée dans le cadre des solutions de "double anonymat", semble disproportionnée et risque de limiter inutilement l'offre de solutions disponibles sur le marché.

Il est aujourd'hui impossible de mesurer précisément le taux de couverture d'un système de vérification d'âge. Les données statistiques fiables permettant d'évaluer avec certitude la proportion de la population adulte couverte par ces méthodes de vérification n'étant tout simplement pas disponibles. Les variables, par exemple la diversité des utilisateurs, les différents contextes d'utilisation et les éventuelles limitations techniques, rendent difficile, voire impossible, une mesure précise de la couverture.

Cette exigence pose un défi, contraint nécessairement l'émergence d'innovations qui pourraient être portées par de nouveaux acteurs, dont les solutions ne pourront par définition pas être immédiatement adoptées par une majorité de la population.

Aussi, les sites de communication en ligne seront contraints de proposer à leurs utilisateurs plusieurs solutions. Ce panel d'outils de vérification porte en lui l'objectif d'une couverture large de la population.

L'Adan propose de considérer une approche plus modulée pour cette exigence de couverture.

- **Ainsi, la fixation d'un seuil initial plus bas serait plus réaliste. En outre, il serait cohérent d'imposer que la somme des solutions proposées aux utilisateurs couvre un certain pourcentage de la population. Un objectif initial de couverture à 65% de la population,** en ligne avec l'estimation des adultes possédant un titre d'identité électronique en France, semble à ce titre approprié.

Solution existante issue du Web3

La Solution repose sur deux technologies principales, l'une sur la puce électronique contenue dans les passeports et cartes d'identité électroniques, et l'autre plus novatrice, sur les preuves à divulgation nulle de connaissance ou plus communément appelées *zero knowledge proofs* (ZKPs).

Un site ou service ayant besoin de vérifier un attribut de l'identité de ses visiteurs, tel que l'âge, peut passer par cette Solution en intégrant un bouton déclenchant la génération d'un QR Code encodant une demande de preuve (dont les données sont indépendantes de toute information liée au visiteur). Le visiteur peut ainsi scanner le QR Code avec son téléphone, qui le guidera ensuite vers l'application ou la page de téléchargement de l'application s'il ne la possède pas encore. L'application en elle-même ne requiert aucun compte, et après scan du QR Code, récupère les critères demandés par le site ou service. Elle guide le visiteur à effectuer le scan de son passeport, carte d'identité ou titre de séjour électronique. L'application récupère les données de la puce, les analyse en local sur le téléphone et vérifie si le visiteur correspond bien aux critères tout en lui montrant visuellement et clairement les critères demandés (utile au cas où le site ou service essaye de cacher une partie des critères sur son interface).

Si le visiteur correspond aux critères et accepte de partager les informations demandées, l'application enclenche la génération de la preuve *zero knowledge* directement sur le téléphone du visiteur. Une fois la preuve générée, elle est conservée en local sur le téléphone, les données du titre d'identité sont immédiatement supprimées du téléphone et la preuve est envoyée à nos serveurs qui ensuite la relaie au site ou service qui peut la vérifier indépendamment de son côté avec nos outils ou directement avec son propre vérifieur. La preuve contient uniquement l'information que le visiteur respecte les critères demandés (comme avoir au moins 18 ans) sans aucune autre information sur le visiteur. De ce fait, ni l'entité à l'origine de la Solution, ni le site ou service ne conserve ou reçoit à aucun moment les informations personnelles du visiteur.

À terme, la preuve des attributs déjà générée par l'utilisateur, et conservée en local sur le téléphone, sera réutilisable sans avoir à re scanner le titre d'identité. Cette Solution est utilisable par les sites ou services que pour une seule vérification, grâce à l'utilisation de

preuves récursives, un moyen de protection sur le téléphone (exemples, Face ID, Touch ID, PIN, etc.) et ce qu'on appelle un "*nullifier*" .

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

⇒ *Critère n°16 : affichage explicite du niveau de protection de la vie privée des utilisateurs*

L'Adan n'a pas de commentaire sur ce critère.

Objectifs souhaitables et bonnes pratiques

Dans le cadre des objectifs souhaitables et des bonnes pratiques susmentionnés, l'Adan promeut l'adoption de solutions Web3 qui respectent pleinement ces recommandations. Certaines solutions Web3, dont l'Adan porte la voix, respectent particulièrement ces bonnes pratiques. Pour illustrer, certaines permettent aux utilisateurs de générer localement des preuves d'âge sur leurs appareils. Dans ce processus, les données personnelles contenues dans leur titre d'identité ne quittent jamais le téléphone de l'utilisateur. Tout est analysé et traité localement, garantissant ainsi une confidentialité maximale.

De plus, la preuve d'âge générée est basée sur une technique de *zero knowledge proof,* par exemple, une *zk-SNARK*. Ce mécanisme avancé vérifie l'authenticité des signatures, RSA ou ECDSA, sur le titre d'identité et compare la date de naissance extraite à la date actuelle. Ces données sont traitées comme des entrées privées dans un circuit cryptographique qui ne révèle que le fait que l'utilisateur a au moins 18 ans, sans divulguer d'autres informations personnelles. Cette approche ne transmet donc rien d'autre que la preuve de majorité, en alignement parfait avec les exigences de minimisation et de protection des données personnelles du RGPD.

III. Solutions de génération de preuve dérogatoires acceptées à titre temporaire

En ce qui concerne l'utilisation exclusive des cartes bancaires comme méthode de vérification pendant la période transitoire de 6 mois, l'Adan a plusieurs réserves à exprimer.

Favoriser cette méthode plutôt qu'une autre induit les risques suivants :

- Elle expose les utilisateurs à un risque d'hameçonnage en ligne, où des individus malveillants pourraient exploiter la vérification par carte bancaire pour obtenir frauduleusement des informations sensibles. Notons que ce type

d'escroquerie, qui compromet la sécurité des données personnelles des utilisateurs, est de plus en plus fréquent.

- Il est possible qu'une personne mineure utilise les cartes bancaires de ses parents ou possède sa propre carte bancaire. Les personnes mineures ont désormais un accès facilité aux comptes bancaires, notamment *via* des services en ligne tels que la néo bank *Revolut*, ce qui rend la vérification *via* carte bancaire moins pertinente. Dans un tel scénario, contourner cette méthode de vérification devient relativement facile.

- L'utilisation exclusive des cartes bancaires pendant cette période pourrait, en plus de privilégier une solution technique plutôt qu'une autre, engendrer une accoutumance à cette méthode, même après l'expiration des 6 mois. Les utilisateurs, habitués à cette vérification, pourraient préférer continuer à l'utiliser par commodité, même si des méthodes plus sécurisées et respectueuses des données personnelles deviennent disponibles ultérieurement.

- **Par conséquent, l'Adan estime qu'exiger la vérification de l'identité *via* l'utilisation exclusive d'une carte bancaire pendant un délai de 6 mois ajoute une friction et un risque non négligeable pour un gain relativement minime, comparé à l'attente de l'implémentation de solutions répondant aux critères du référentiel.**

IV. Audit et évaluation des solutions de vérification de l'âge

Sur cette dernière partie de la consultation, l'Adan exprime des préoccupations en ce qui concerne les modalités d'audit définies par le référentiel ARCOM pour les solutions de vérification de l'âge. Principalement, l'Adan questionne les critères de qualification des auditeurs et la nature de l'audit, notamment si celui-ci implique une certification distincte similaire ou moins contraignante que celle des Prestataires de vérification d'identité à distance (PVID).

De plus, il conviendrait de prendre en considération le défi technique et juridique lié à la nécessité de tester les systèmes avec de *"faux documents"*, une procédure qui implique que seuls des auditeurs spécialement accrédités effectuent ces tests, augmentant ainsi les coûts d'entrée.

L'Adan note également que l'exigence d'un "*audit annuel*" pourrait être trop onéreuse et disproportionnée. D'autant plus que les entreprises du secteur Web3, qui ont la capacité de proposer des solutions innovantes et efficaces, sont encore jeunes. En comparaison, des

certifications reconnues (comme l'ISO27001) sont valides pendant une durée totale de trois ans, ce qui questionne la récurrence annuelle des audits préconisée par le référentiel.

Enfin, il peut être difficile de concilier les audits fréquents (s'ils sont annuels, notamment) avec les impératifs de protection de la vie privée dans la mesure où le délai de mise en œuvre d'un audit doit être raisonnable ; c'est-à-dire qu'il ne doit compromettre les principes de confidentialité des systèmes évalués.

❖ **Contacts à l'Adan**

- Faustine Fleuret, Présidente : faustine.fleuret@adan.eu
- Mélodie Ambroise, Directrice stratégie de relations institutionnelles : melodie.ambroise@adan.eu
- Alizée Van Den Schrieck, Chargée des affaires juridiques et réglementaires : alizee.vandenschrieck@adan.eu
- Adriana Torres Vergara, Responsable des affaires européennes : adriana.torresvergara@adan.eu

❖ **Contributions spécifiques**

L'Adan remercie les membres du Comité NFT pour leurs contributions, notamment : Capsule Corp Labs, Hyperweb.dev, Synaps.io et Wagmi Studio.

~