GOUVERNEMENT
Liberté
Égalité
Fraternité

Pôle d'expertise de la régulation numérique

Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ?

Éclairage sur…

Mai 2022

#04

Collecte de données personnelles, cyberharcèlement et haine en ligne, les risques liés à la présence d'enfants ou mineurs en ligne sont multiples. Pour y remédier, le Règlement général sur la protection des données (RGPD) et des réglementations spécifiques plus récentes imposent désormais à de nombreuses plateformes, directement ou indirectement, de vérifier la tranche d'âge de leurs utilisateurs.

Ce n°4 d'Éclairage sur…dresse un panorama critique des solutions actuellement déployées. Constat : aujourd'hui, pratiquement aucun service en ligne n'utilise de procédé fiable permettant de vérifier l'âge. Malgré leur multiplicité, peu de méthodes sont à la fois faciles à mettre en œuvre, peu contraignantes et respectueuses de la vie privée des utilisateurs, performantes et robustes face à des tentatives de fraude.

Dans le cadre d'un partenariat, le PEReN a participé au développement d'une solution expérimentale de transmission de preuve de l'âge par double tiers interopérable avec plusieurs méthodes de vérification.

Par « individu mineur » dans ce document, il faut entendre tout individu dont l'âge est inférieur à l'âge requis pour accéder à un service en ligne conformément à la réglementation en vigueur dans un pays considéré et sur ledit service. Ainsi, il peut s'agir d'utilisateurs de moins de 13 ans pour l'accès à des réseaux sociaux en France, de moins de 16 ans pour l'accès à des réseaux sociaux dans certains autres États membres européens comme l'Allemagne, ou encore d'utilisateurs de moins de 18 ans dans le cadre de l'accès à des sites pornographiques.

Le contrôle de l'accès à un service en ligne interdit aux individus mineurs repose souvent sur un ensemble de trois couches techniques : le procédé utilisé pour **vérifier l'âge de l'individu ou sa majorité**, le **mécanisme de transmission du résultat de la vérification à la plateforme** ou au service à l'origine de la demande de vérification le cas échéant, et le **mode de blocage** ou la restriction de fonctionnalités, que nous n'aborderons pas dans cet éclairage sur… (nous considérerons par défaut un blocage au niveau du site).

ACTIVITÉ DES MINEURS EN LIGNE : UNE RÉGLEMENTATION QUI PEINE À ÊTRE MISE EN ŒUVRE

Au niveau européen, la question du contrôle de l'âge découle de facto du RGPD, et en particulier de son article 8 qui interdit l'utilisation de données personnelles d'utilisateurs âgés de moins de 13 à 16 ans suivant les États membres (avant quoi un consentement conjoint de l'enfant et du titulaire de l'autorité parentale est nécessaire[1]). Cette obligation motivée par le potentiel ciblage publicitaire d'enfants[2], a conduit les plateformes concernées, notamment les réseaux sociaux, à mettre en place certains procédés de vérification de l'âge.

En France, cette mesure générale s'accompagne de mesures sectorielles ou de précisions sur les modalités de vérification, certaines préexistant au RGPD comme c'est le cas pour les jeux d'argent et les paris en ligne pour lesquels le processus de vérification de l'âge d'un utilisateur est régi par le décret 2010 – 518[3]. Les sites présentant du contenu à caractère pornographique, sont quant à eux régis par les nouvelles dispositions de l'article 227-24 du Code Pénal modifié par la loi sur les violences conjugales[4], qui mentionne explicitement que les systèmes de vérification de l'âge basés sur l'auto-déclaratif ne constituent pas des systèmes valides sur de tels sites[5].

À ces mesures contraignantes s'ajoutent des avis ou des lignes directrices d'autorités indépendantes ou encore de publications par des consortiums. Au niveau européen, on peut par exemple citer l'initiative euCONSENT[6] financée par la Commission qui vise à établir un socle

[1] https://www.cnil.fr/fr/les-bases-legales/consentement
[2] https://ec.europa.eu/newsroom/article29/items/623051/en
[3] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000022235495/
[4] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042176652
[5] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043409165/
[6] https://euconsent.eu/

commun pour les systèmes de vérification de l'âge permettant leur interopérabilité internationale, permettant la compatibilité des différentes régulations européennes et de leurs systèmes de données. En France, la CNIL a publié en août 2021 des recommandations générales[7] s'articulant autour de six piliers : proportionnalité, minimisation, robustesse, simplicité, standardisation, intervention d'un tiers. Elles complètent l'avis rendu le 3 juin 2021[8] sur le décret d'application des nouvelles dispositions du Code pénal spécifiant les modalités de mise en œuvre de mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique. Cet avis recommandait la mise en place d'un dispositif de double anonymat afin de protéger la vie privée des utilisateurs. À cet égard, l'Arcom[9] (ex – CSA), par sa décision du 13 décembre 2021, a mis en demeure cinq sites pornographiques et les a enjoints de se mettre en conformité avec les nouvelles dispositions du Code pénal sous un délai de 15 jours. À ce jour, la procédure est toujours en cours.

Double anonymat : « mécanisme […] empêchant, d'une part, le tiers de confiance vérificateur d'identifier le site ou l'application à l'origine d'une demande de vérification et, d'autre part, faisant obstacle à la transmission de données identifiantes relatives à l'utilisateur au site ou à l'application proposant des contenus [à accès restreint] » (Source : avis de la CNIL)

De son côté, le Royaume-Uni a formalisé les bonnes pratiques en matière de protection des données des mineurs au sein du *Age Appropriate Design Code*[10] juridiquement contraignant depuis le 2 septembre 2021 et dont le contrôle est confié à l'ICO (homologue britannique de la CNIL). Ce code fournit notamment de grandes lignes directrices sur le processus de vérification de l'âge sans pour autant affirmer une préférence pour une solution particulière. Il encourage également le *privacy by default* qui implique que les paramètres de confidentialité soient par défaut les plus élevés pour les enfants.

Privacy by default (protection des données par défaut) : concept introduit dans le RGPD qui signifie que le système de protection des données mis en place est directement activé par défaut, sans intervention de l'utilisateur.

Aux États-Unis, le *Children's Online Privacy Protection Act* (COPPA)[11] impose aux éditeurs de sites internet ou de services collectant des données personnelles d'enfants de moins de 13 ans d'obtenir le « consentement parental vérifiable ». Sur le fondement de ce texte, Google a été condamné en 2019 à payer 170 Millions de dollars d'amende pour avoir utilisé des cookies d'utilisateurs regardant du contenu enfant sur YouTube à des fins de publicité ciblée, sans le consentement des parents. Suite à cette décision, par souci de simplicité, plusieurs plateformes, comme TikTok, ont simplement interdit l'accès aux utilisateurs de moins de 13 ans. Afin de renforcer le COPPA, plusieurs projets de loi bipartisans sont actuellement à l'étude, dont le *Children and Teens' Online Privacy Protection Act*[12] et le *Kids PRIVCY Act*[13], qui s'inspirent du *Age Appropriate Design Code* britannique. Ils incluent tous deux notamment des obligations quant à la publicité ciblée sur les enfants et remplacent la notion de « connaissance réelle de l'âge de l'utilisateur » par une notion de « connaissance constructive de l'âge des

[7] https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy

[8] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781

[9] Arcom : Autorité de régulation de la communication audiovisuelle et numérique

[10] Code pour une conception adapté à l'âge

[11] Loi pour la protection de la vie privée des enfants en ligne

[12] Loi pour la protection de la vie privée des enfants et adolescents en ligne

[13] Loi pour la vie privée des enfants

utilisateurs »[14] plus englobante sans imposer directement de vérification de l'âge à proprement parler.

En Union Européenne, la législation sur les services numériques (DSA), va introduire une interdiction de la publicité ciblée pour les mineurs. Les modalités de mise en œuvre de cette interdiction qui était au cœur des négociations restent à être définies. Ce texte interdira aux plateformes d'utiliser les données personnelles des mineurs dont elle a la connaissance effective qu'elles collectent à des fins de publicité ciblée. Par ailleurs, le texte devrait préciser que cette obligation ne doit pas conduire à la collecte d'informations personnelles supplémentaires.

Malgré tout, plus de 60% des enfants de moins de 13 ans disposeraient d'un compte sur au moins un réseau social selon l'enquête effectuée par Génération numérique en 2021[15], en dépit des législations ou conditions générales d'utilisations (CGU) l'interdisant, et des obligations de vérification d'âge incombant aux plateformes. Les risques associés sont nombreux comme souligné notamment par cette étude et par une étude de l'Institut Montaigne[16] : la haine en ligne toucherait 56% des jeunes[17], et 40% des jeunes déclarent avoir été exposés au moins une fois à des contenus violents, et 36% à des contenus pornographiques.

VÉRIFICATION DE L'ÂGE : LES MÉTHODES DES GRANDES PLATEFORMES SE RÉVÈLENT PEU EFFICACES

Pour répondre aux obligations légales, les grandes plateformes, et en particulier les réseaux sociaux, ont développé et mis en place sur leurs services en ligne des solutions de vérification de l'âge.

Au moment de l'inscription, la méthode de vérification de l'âge presque systématiquement utilisée est celle de l'auto-déclaratif avec différentes variantes : soit un simple clic pour confirmer que l'on a bien l'âge requis, soit une entrée manuelle de la date de naissance avec blocage (au bout d'une ou plusieurs tentatives) lors de la procédure d'inscription.

Par nature, l'auto-déclaratif est peu fiable et très peu efficace. Afin de réduire la présence de mineurs sur leurs plateformes, la plupart des réseaux sociaux utilisent donc en complément une méthode de détection de mineurs en continu. Activée en arrière-plan, celle-ci se fonde le plus souvent sur la recherche de mots-clés prédéfinis dans le contenu publié par l'utilisateur et pouvant suggérer son âge. De l'avis même des grandes plateformes **cette méthode n'est actuellement pas satisfaisante à deux titres : le taux de fausses alertes (faux-positifs) est très élevé et la précision de la méthode dépend de la quantité de**

[14] La notion de « Constructive knowledge » signifie que la plateforme a des raisons de savoir que l'utilisateur en question est mineur (par exemple parce qu'elle collecte, utilise, achète, analyse ou vend directement ou indirectement des données pour estimer l'âge ou la tranche d'âge de l'utilisateur)

[15] https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf

[16] https://www.institutmontaigne.org/blog/digital-services-act-moderer-les-contenus-et-proteger-les-mineurs

[17] de 11 à 20 ans dans l'étude

contenu publié par l'utilisateur. Pour preuve, un utilisateur mineur présent sur une plateforme sans y publier de contenu, ne pourra jamais être détecté comme tel par ce type d'algorithme. Les plateformes qui en ont la possibilité utilisent en complément des signaux venant de l'âge moyen des cercles sociaux ainsi que de la nature des contenus consultés. En parallèle, certaines plateformes ont mis en place la possibilité de signaler des utilisateurs mineurs. Ces signalements peuvent alors être examinés par une équipe humaine, qui, si besoin, va demander une pièce d'identité à l'utilisateur suspecté d'être mineur.

Les grandes plateformes possédant plusieurs services en ligne ont ainsi la possibilité d'utiliser davantage de signaux pour inférer l'âge d'un utilisateur. À titre d'exemple, l'historique des recherches, la date de création du compte, des signaux issus du temps passé sur les différents contenus et l'âge moyen des amis sur le graphe social peuvent être utilisés. En cas d'incertitude, ou si l'utilisateur a été catégorisé comme mineur, une pièce d'identité peut être demandée afin d'accéder à certains services réservés aux utilisateurs majeurs. Celle-ci est alors vérifiée, souvent automatiquement par un algorithme confirmant son authenticité dans au mieux 70% à 80% des cas. Pour les cas restants, une vérification manuelle a lieu. Une fois l'âge de l'utilisateur établi, celui-ci peut être validé comme majeur sur tous les services d'une telle plateforme.

Bien que ces méthodes de recherche de signaux faibles soient plus efficaces que la simple analyse du contenu publié ou l'auto-déclaratif à l'inscription, leur efficacité reste limitée. De plus, le recours à ces méthodes ou à la demande d'une pièce d'identité doit être mis en balance avec l'impact sur la vie privée des utilisateurs, quand bien même l'obligation de vérification de l'âge des utilisateurs s'accompagne pour les plateformes d'un encadrement du traitement de données personnelles.

Enfin, les mesures de blocage prises en cas de détection d'une personne mineure sont variables selon les plateformes : le compte, navigateur ou l'appareil de l'utilisateur peuvent être bannis, avec ou sans possibilité d'appel. Si l'âge vérifié est entre 13 et 17 ans, les publicités réservées aux majeurs ne leur seront pas montrées non plus.

Parallèlement aux solutions souvent internes développées par les grandes plateformes, différents acteurs ont développé des solutions de vérification de l'âge dans le but de les commercialiser à des sites tiers. On peut citer par exemple Yoti, une entreprise britannique qui revendique aujourd'hui 500 millions de vérifications. Sa solution repose sur l'estimation de l'âge à partir d'une courte vidéo ou photo de l'utilisateur et d'intelligence artificielle, avec une marge d'erreur auto-déclarée de 1 an et demi pour les utilisateurs âgés entre 13 et 24 ans[18].

[18] https://yoti.world/age-scan

De leur côté, certains services soumis à des obligations de vérification de l'âge ont commercialisé leurs propres solutions. C'est le cas de AgeID[19], une solution développée par MindGeek, également propriétaire de plusieurs sites pornographiques. En 2017, lors de l'adoption du *Digital Economy Act*[20] britannique, MindGeek a fortement promu la mise en place de vérifications strictes de l'âge sur les sites pornographiques, mais aussi sur l'ensemble des réseaux sociaux ou sites susceptibles d'afficher des contenus sensibles[21]. Pourtant, actuellement MindGeek n'utilise pas sa propre solution de vérification d'âge sur ses sites et continue d'utiliser le déclaratif comme moyen exclusif de vérification d'âge, comme l'a récemment constaté l'Arcom[22].

VÉRIFICATION DE L'ÂGE : LES MÉTHODES PASSÉES AU CRIBLE

Dans cette partie, nous examinons en détail le fonctionnement général des solutions de vérification de la tranche d'âge et passons en revue différentes options souvent mentionnées dans le débat public, tout en spécifiant leur pertinence au regard de critères mentionnés plus bas. La revue détaillée des différentes solutions est disponible en Annexe 2.

Tout d'abord, les solutions de vérification de l'âge peuvent être classées selon le mode de preuve employé :

- Le **contrôle** de l'âge, à l'aide d'un document portant l'identité et la date de naissance de la personne, à l'aide d'un document dont toutes les parties identifiantes auraient été supprimées avant tout traitement ou enfin par les parents (contrôle parental) ;
- **L'estimation algorithmique** de l'âge sur la base du contenu publié ou utilisé par l'utilisateur sur le site ou bien à partir de données biométriques (voix, images, vidéos,…) ;
- Le **déclaratif** se basant uniquement sur les déclarations des internautes.

Au sein de ces catégories, différentes déclinaisons peuvent exister. Par exemple, les solutions fondées sur l'analyse de données peuvent utiliser l'intelligence artificielle ou bien des algorithmes plus classiques comme la détection de mots-clés actuellement mise en œuvre par plusieurs réseaux sociaux (voir plus haut). De même, le support de vérification d'identité peut être de différente nature : présentation seule d'une carte d'identité à une personne physique ou en ligne, présentation d'une carte d'identité en ligne avec photo ou vidéo de confirmation supplémentaire, etc..

Il convient également d'évaluer la pertinence des ces catégories de solutions du point de vue des parties prenantes et de leur efficacité. Au

[19] https://www.ageid.com/

[20] Loi sur l'économie numérique

[21] https://www.lemonde.fr/pixels/article/2019/07/13/le-filtrage-du-porno-brxit-un-projet-britannique-qui-a-tourne-a-la-catastrophe-industrielle_5488904_4408996.html

[22] https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Controle-de-l-age-des-mineurs-cinq-sites-mis-en-demeure-de-mettre-en-place-des-dispositifs-adaptes-pour-repondre-a-leurs-obligations-legales

total, 7 critères ont été définis pour les parties prenantes et l'efficacité de la solution, dont le détail figure en Annexe 1 :

- La plateforme : **facilité d'implémentation** ;
- Les utilisateurs : **lisibilité, commodité** et **degré d'intrusion** dans la vie privée (utilisation de données biométriques, identifiantes,…) ;
- L'efficacité de la solution : **robustesse à la fraude, performance** (taux de faux-négatifs, possibilité de distinguer différents âges,…) et **flexibilité** de la méthode.

Le Tableau 1 présente la synthèse de l'évaluation des différentes méthodes de vérification d'âge selon ces critères.

Tableau 1 – Analyse résumée des solutions de vérification de l'âge

	Plateforme	Utilisateurs			Efficacité		
	Facilité d'implémentation	Lisibilité	Commodité	Peu intrusive	Robuste à la fraude	Performance	Flexibilité
Contrôle de carte bancaire	✔	⚠	⚠	✔	✔	⚠	⚠
Contrôle par un bureau de tabac	✔	⚠	✖	✔	⚠	⚠	✔
Utilisation d'une base de données nationale	✔	✖	✔	✔	✔	✔	✔
Contrôle d'une pièce d'identité et d'une photo	✔	✖	✖	✖	✔	✔	✔
Service de garantie de l'identité numérique (SGIN)	✔	✔	✖	✔	✔	✔	✔
Contrôle parental	✔	✔	✔	✔	✔	⚠	✔
Profilage social basé sur le contenu	✖	✖	✔	⚠	✖	✖	✖
Utilisation de données biométriques	✔	✖	✖	⚠	✖	✖	⚠
Auto-déclaration	✔	✔	✔	✔	✖	⚠	✔

Source : PEReN

✔ Satisfaisant ⚠ Peu satisfaisant ✖ Non satisfaisant

Descriptif et catégorisation des solutions

Parmi les solutions efficaces et comparativement peu contraignantes ou intrusives pour l'utilisateur, on peut citer :

- La **vérification par carte bancaire** : cette solution consisterait à effectuer un micropaiement avec le numéro de carte fourni par l'utilisateur. L'inconvénient principal réside dans l'absence de granularité sur l'estimation de l'âge. De plus, en France, il est possible de détenir une carte bancaire avant 18 ans. Cette méthode ne pourrait donc pas être utilisée par exemple dans le cas des sites pornographiques ;
- La **vérification par base de données nationale** : cette solution consiste à vérifier l'âge de l'utilisateur à partir d'un identifiant national (numéro de sécurité sociale par exemple). Cette méthode permet d'alerter l'utilisateur à chaque vérification utilisant son identifiant. Néanmoins l'acceptabilité sociale de cette méthode est conditionnée à l'existence d'un mécanisme de double anonymat afin de garantir que le tiers ayant accès à la base nationale ne connaisse pas le service depuis lequel la requête de vérification a été émise ;

- L'utilisation du futur « **Service de garantie de l'identité numérique** » (SGIN)[23] : ce service proposera aux personnes équipées d'une carte d'identité électronique et d'un outil (smartphone) capable de lire la puce de celle-ci, de scanner leur carte d'identité afin de fournir une attestation ne présentant que les informations minimales requises. Bien que limitée à un public restreint et ne pouvant donc être la seule alternative proposée, cette solution semble intéressante à suivre ;
- Le **contrôle parental installé par défaut avec activation par les parents** : cette méthode, proposée par la loi Studer[24], présente l'avantage d'être centralisée au niveau du système d'exploitation du terminal, sa diffusion et son adoption peuvent donc être plus rapides. Néanmoins, les modalités d'application précises de la loi ne sont pas encore connues et la part des parents qui utiliseraient réellement le dispositif reste incertaine. Elle soulève aussi plusieurs interrogations concernant son implémentation sur le parc existant d'une part, et son efficacité sur des ordinateurs partagés.

D'autres solutions sont efficaces mais plus contraignantes ou intrusives pour l'utilisateur. Parmi elles, se trouve notamment :

- La **vérification par pièce d'identité adossée à une base de données nationale ou une photo** : cette méthode est la plus efficace et l'une des plus robustes à la fraude. Toutefois, elle présente l'inconvénient de demander aux utilisateurs un document identifiant et des données biométriques.

Enfin certaines solutions sont soit très peu efficaces, soit peu efficaces et contraignantes ou intrusives pour l'utilisateur :

- **Auto-déclaratif** : cette méthode, utilisée par plusieurs réseaux sociaux, ne permet pas de déterminer de manière fiable l'âge d'un utilisateur. Bien qu'elle soit facile à mettre en place et peu contraignante, même avec des mesures de désincitation à la fausse déclaration (interdiction de soumettre immédiatement un nouvel âge après un refus,…), elle **ne constitue pas une solution fiable et robuste**.
- **Vérification par un bureau de tabac** avec délivrance d'un code unique : cette méthode, dont l'efficacité dépend de la fiabilité des contrôles par les buralistes, peut être perçue comme contraignante pour certains utilisateurs ;
- **Profilage social basé sur le contenu publié par l'utilisateur** : cette méthode, en l'état, est peu fiable, dépend du contenu publié par l'utilisateur et n'est donc pas applicable à toutes les plateformes ;
- **Estimation basée sur des données biométriques** : les méthodes actuelles parviennent dans certains cas à détecter l'âge avec une marge d'erreur annoncée de l'ordre de 1 an et demi dans la tranche d'âge d'intérêt, ce qui n'est parfois pas

[23] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825
[24] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054

suffisant. Par ailleurs, elles donnent lieu à la collecte de données biométriques d'individus potentiellement âgés de moins de 13 ans.

Bien que la catégorisation présentée tente d'inclure toutes les parties prenantes, il est important de souligner que le classement effectué à partir des critères définis plus haut reste subjectif. En particulier, chaque individu peut accorder davantage de poids à certains critères plutôt que d'autres. Par exemple la protection des données personnelles peut pour certains être un critère essentiel, tandis que d'autres favoriseront la commodité. Compte-tenu de cette observation et dès lors qu'aucune solution de vérification ne répond à l'ensemble des critères, il pourrait être envisagé de laisser le choix entre plusieurs solutions de vérification qui répondent à des exigences minimales : vérification par carte bleue, base nationale, bureau de poste ou buraliste à titre d'exemples et selon la préférence de chacun.

Des solutions à mettre en regard avec le niveau de risque potentiel sur la plateforme

Par ailleurs, parmi les solutions choisies, certaines sont plus efficaces que d'autres, parfois au prix de davantage de contraintes pour les utilisateurs. Là encore, imposer une solution universelle à tous les services serait ignorer la variété des niveaux de risques encourus par des mineurs lors de l'accès à des services en ligne restreints. Le risque est parfois inhérent au service proposé, comme c'est le cas pour l'accès à un catalogue de vidéos pornographiques et ne peut donc pas être atténué. Mais pour une part importante des plateformes — les réseaux sociaux notamment —, ce risque peut être réduit par une politique de modération et d'interdiction de certains types de contenus (violents, haineux, pornographiques…). Une modération efficace diminue le risque d'exposition à des contenus sensibles, de même que l'importance de la vérification d'âge.

Si la qualification et la modération de contenu, apportant leurs propres difficultés, ne se substituent pas à une vérification de l'âge, la proportionnalité des mesures de contrôle reste à évaluer : il apparaîtrait démesuré de demander une carte d'identité pour accéder aux contenus de Disney, au motif que certains sont déconseillés aux moins de 13 ou 16 ans). Mais corollairement, si une plateforme se prévaut du caractère inoffensif de son contenu pour justifier une politique permissive de vérification de l'âge, il devient d'autant plus primordial que sa politique de modération soit efficace et activement mise en œuvre.

LE DOUBLE ANONYMAT EN PRATIQUE

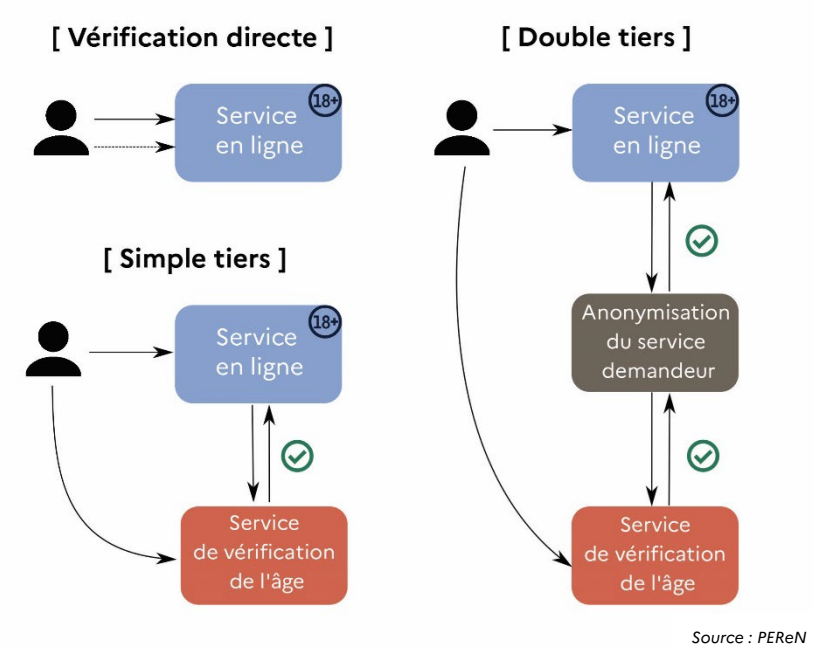
Comme mentionné précédemment, la vérification de l'âge n'est que la première des trois étapes d'un contrôle d'accès à un service restreint aux mineurs. Le mécanisme de transmission de la preuve de majorité joue également un rôle critique, trop souvent minimisé. Aujourd'hui en effet, il est fréquent que les grandes plateformes effectuent elles-mêmes la

vérification de l'âge. Or cette situation les conduit à collecter davantage de données personnelles qu'elles sont ensuite en mesure de croiser avec d'autres données en leur possession ou d'utiliser à des fins commerciales. Certaines plateformes en effet utilisent le prétexte d'une vérification d'âge pour demander une date de naissance précise, qui est alors utilisée pour raffiner le profilage et le ciblage publicitaire de leurs utilisateurs majeurs.

Indépendamment de la solution choisie, il semble donc primordial que la vérification de l'âge ne soit pas directement opérée par la plateforme ou le service en ligne afin de réduire le risque de croisement ou de réutilisation des données collectées lors de la vérification. **Un mécanisme de tiers, voire de double tiers, peut être mis en place pour la transmission du résultat de la vérification précisément afin de minimiser ce risque**. Illustrés en Figure 1 ces mécanismes jouent un rôle fondamental dans l'acceptabilité sociale de la solution. Comme expliqué précédemment, en l'absence de tiers, un site à accès restreint endosserait également le rôle de vérificateur d'âge de ses utilisateurs. Il pourrait alors rattacher des données personnelles ou sensibles en sa possession à l'identité de la personne. Le mécanisme de tiers permet de pallier ce problème en reportant la vérification de l'âge sur un service extérieur de vérification, vers lequel l'utilisateur est automatiquement redirigé. L'utilisateur fournit une preuve de son âge sur le service tiers, qui génère ensuite un « jeton » à destination du service requérant la vérification pour en indiquer le résultat. Sans protection supplémentaire, ce tiers vérificateur a néanmoins accès aux données utilisées pour la vérification, ainsi qu'à l'identité du site visité, qui peut parfois être sensible et pourrait être utilisée par le site vérificateur. Le mécanisme de double tiers ajoute à ce mécanisme un second tiers, qui est chargé de transférer les informations entre le site à accès restreint et le site vérificateur, de sorte que ce dernier ne connaisse pas le site réellement visité. Ainsi, aucune partie n'a accès à la fois aux données de vérification et aux données de navigation. En cela, ce mécanisme de double-tiers constitue une mise en œuvre possible du double anonymat recommandé par la CNIL.

Jeton :
Donnée chiffrée utilisée pour transmettre l'information qu'un individu est majeur.

Figure 1 – Illustration des mécanismes de tiers.



Source : PEReN

Un tel système reposerait sur la standardisation d'une part d'une demande générée par les sites à accès restreint et d'autre part d'un jeton généré par le vérificateur d'âge après réception de la demande et fonction de l'âge de l'utilisateur. Comme on l'a vu, le transfert de ce jeton respectant le double-anonymat pourrait être assuré par un système de double tiers. Ce cumul de tiers n'apporte cependant pas de garantie d'anonymat en cas de collusion entre deux des entités concernées.

Alternativement, le transfert du jeton pourrait être assuré par exemple par le système d'exploitation du terminal, manuellement ou encore par une extension de navigateur, supprimant non seulement le contact direct entre tiers et réduisant ainsi le risque de collusion, mais également la nécessité d'un tiers intermédiaire. Nous décrivons cette dernière possibilité, en nous appuyant sur l'exemple d'une extension de navigateur *ad hoc*.

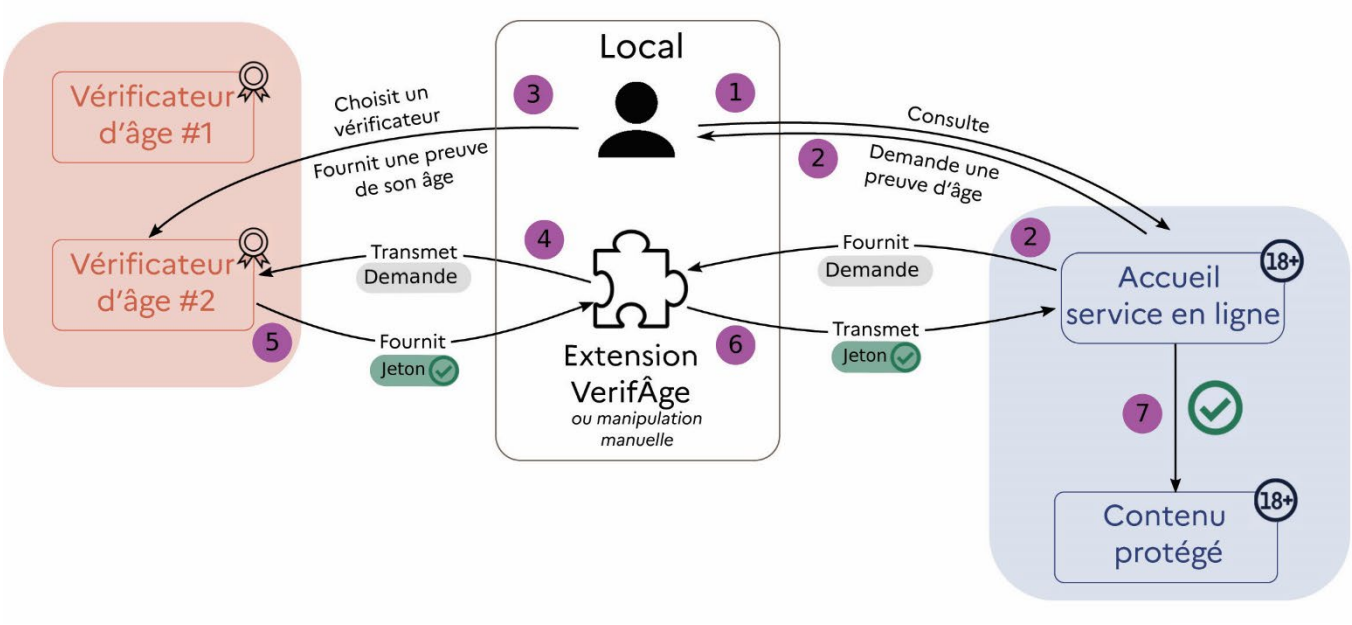
Une extension de navigateur, baptisée ici « VérifÂge », faciliterait la procédure d'accès aux services qui requièrent une vérification d'âge (réseaux sociaux, sites pornographiques,…), et permettrait à l'internaute de récupérer de manière automatique des demandes d'âge sur les sites à accès restreint puis de les faire valider lorsqu'il navigue sur un service de vérification d'âge, pour renvoyer enfin les jetons correspondants aux sites concernés. Sans jeton valide, l'accès au site serait bloqué. Remarquons que cette extension, fortement conseillée, ne serait néanmoins pas nécessaire : sa fonction se limite à stocker des jetons localement et à les transférer, et il demeure tout à fait possible, quoi que fastidieux, d'effectuer ce processus manuellement en copiant et collant les données relatives au jeton entre le site de vérification et le site demandant le résultat de la vérification.

Une autorité devrait être en charge d'accréditer ou révoquer les tiers autorisés à valider ces jetons afin de garantir l'effacement des données et un haut niveau de protection de celles potentiellement sensibles. Dans le cas d'une extension, afin d'accroître la confiance des utilisateurs, le code source de l'extension et des procédés d'émission et de validation devrait être publié en *open source*.

Le principe de fonctionnement de ce mécanisme est représenté Figure 2. La CNIL, en partenariat avec un laboratoire de l'École polytechnique, et le PEReN, ont développé un prototype de ce mécanisme de vérification

de l'âge par double anonymat pour en démontrer la faisabilité technique. Cette preuve de concept est disponible ici : https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee .

Figure 2 – Schéma de principe du mécanisme de double anonymat avec extension de navigateur



Source : PEReN

CONCLUSION

Alors même que plusieurs dispositions légales enjoignent à de nombreux services en ligne de contrôler l'accès aux mineurs sur leurs sites, les méthodes actuellement mises en œuvre par les plateformes numériques ne permettent pas de filtrer efficacement les mineurs au moment de leur inscription sur les réseaux sociaux ou d'une première consultation sur un site pornographique par exemple. Si certaines plateformes mettent en place des mesures complémentaires pour détecter en continu des mineurs déjà inscrits, les performances du dispositif restent semble-t-il mesurées. Par ailleurs, la vérification de l'âge, directement opérée par ces plateformes, peut constituer un prétexte supplémentaire pour collecter davantage de données, et dans certains cas les croiser avec les données existantes ou celles d'autres services.

De l'analyse effectuée des différentes méthodes de vérification existantes, il ressort qu'aucune n'est à la fois performante, totalement transparente pour l'utilisateur, peu intrusive et accessible à tous, bien que certaines paraissent meilleures. Laquelle choisir et quel protocole de transmission des preuves d'âge adopter ? L'acceptabilité sociale du contrôle doit guider ces choix et à cet égard il est nécessaire de s'assurer du respect de trois points :

- en premier lieu, les méthodes proposées aux utilisateurs doivent être proportionnées et adaptées au niveau de risque encouru par un mineur si celui-ci déjouait la vérification ;

- ensuite, la plateforme doit être en mesure de proposer à l'utilisateur différentes options, car les préférences de chacun peuvent varier ;
- enfin, l'objectif étant aussi avant tout de protéger les utilisateurs en ligne, le recours à un mécanisme de double anonymat reposant sur une séparation étanche entre le service à accès contrôlé et le service effectuant la vérification d'âge semble un critère essentiel aujourd'hui : il n'est pas souhaitable que la plateforme effectue elle-même cette étape de vérification.

L'ouverture du code source et l'interopérabilité de la solution ressortent également comme des critères nécessaires à son acceptabilité et donc sa diffusion et à son adoption. Le protocole de transmission de preuve d'âge proposé en dernière partie et élaboré en partenariat avec la CNIL propose une mise en œuvre concrète d'un tel dispositif.

ANNEXE 1

LISTE DES CRITÈRES UTILISÉS POUR L'ÉVALUATION DES MÉTHODES

Plateformes

→ **Facilité de mise en œuvre de la solution pour la plateforme**
- La méthode requiert-elle une expertise technique importante ?
- Des données spécifiques à la plateforme sont-elles utilisées au cours de la vérification ?
- La méthode est-elle fondée sur un algorithme existant ou un tiers ?

Utilisateurs

→ **Lisibilité de la solution pour les utilisateurs**
- Les méthodes utilisées sont-elles accessibles au grand public et facilement vulgarisables ?
- Y a-t-il des tiers impliqués dans le processus ?
- La solution peut-elle être publiée dans son intégralité ?
- Les garanties de vie privée sont-elles facilement compréhensibles ?

→ **Facilité et rapidité de prise en main pour l'utilisateur**
- La vérification a-t-elle lieu entièrement en ligne ?
- La vérification est-elle transparente pour l'utilisateur (en arrière-plan) ?
- La vérification est-elle rapide et sans outillage non-requis pour le service (micro, caméra, scanner,…) ?

→ **Degré d'intrusion dans la vie privée de l'utilisateur**
- Des données biométriques (non-nominatives) sont-elles utilisées ?
- Le service vérifiant l'âge disposerait-t-il théoriquement de suffisamment d'informations pour désanonymiser les preuves de majorité ?
- La solution implique-t-elle l'utilisation de documents identifiants ?

Efficacité de la solution

→ **Facilité d'accès à la fraude**
- L'utilisateur peut-il être averti à chaque utilisation de la solution (alerte SMS, etc.) ?
- Est-il nécessaire de réitérer la fraude à chaque tentative d'accès au service ?
- Peut-on acheter facilement la preuve de majorité (carte bleue, France Connect) ?

→ **Performance de la solution**
- Le taux de faux-négatifs est-il faible ?
- La détection est-elle aussi précise quelle que soit la tranche d'âge considérée (détection par image) ?
- La fiabilité de la détection varie-t-elle suivant d'autres critères (couleur de peau, sexe, niveau de langue, etc.) ?

→ **Flexibilité de la solution**
- Le résultat peut-il être obtenu avant l'utilisation du service en ligne ?
- La solution permet-elle de distinguer différentes tranches d'âge ?

ANNEXE 2

PANORAMA DES SOLUTIONS

Simple auto-déclaratif

+	−
· Simple et rapide pour l'utilisateur · Respectueux des données personnelles · Facile à mettre en place pour les plateformes	· Très peu fiable (taux de faux-négatifs très élevé) · Dans certains cas, comme Twitter avec les comptes institutionnels, le taux de faux-positifs peut être non négligeable également

Vérification basée sur une pièce d'identité

Dans cette catégorie, plusieurs variantes sont analysées selon que l'utilisateur fournit uniquement sa carte d'identité ou bien également une preuve supplémentaire permettant de confirmer son identité.

Vérification de l'âge présent sur la pièce d'identité sans vérification additionnelle

+	−
· Modérément contraignant pour l'utilisateur · Très bonne précision et granularité dans l'estimation de l'âge en l'absence de fraude	· Récolte de données identifiantes · Possibilité de fraude simple (carte d'identité des parents, ou toute carte d'identité en ligne en l'absence de stockage des cartes contrôlées)

Vérification de l'âge accompagnée d'une comparaison de la photo d'identité avec une photo ou vidéo prise par l'utilisateur

+	−
· Fraude très complexe à mettre en œuvre · Très bonne précision et granularité dans l'estimation de l'âge	· Assez contraignant pour l'utilisateur · Récolte de données identifiantes · Vérification de la photo possiblement complexe (si la carte d'identité date d'il y a 10 ans par exemple)

Vérification de l'âge par une pièce d'identité adossée à une base de données nationale	
✚	▬
· Fraude très complexe à mettre en œuvre · Très bonne précision et granularité dans l'estimation de l'âge · Modérément contraignant pour l'utilisateur	· Récolte de données identifiantes

Vérification de l'âge sur la pièce d'identité accompagnée d'une vérification du nom à l'aide d'un autre document (justificatif de domicile,…)	
✚	▬
· Fraude très complexe à mettre en œuvre · Très bonne précision et granularité dans l'estimation de l'âge	· Contraignant pour l'utilisateur · Récolte de données identifiantes

Vérification par la carte bleue

✚	▬
· Peu contraignant et rapide pour l'utilisateur · Facile à mettre en place pour les plateformes · Relativement respectueux des données personnelles	· Permet simplement de savoir si l'utilisateur a plus de 16 ans mais ne permet pas de différencier différents âges. Des cartes bleues pour mineurs se développent. · Fraude peu complexe à mettre en œuvre

Vérification basée sur le SGIN

✚	▬
· Respectueux de la vie privée (possibilité de minimiser les données fournies) · Très bonne précision et granularité dans l'estimation de l'âge · Possibilité d'ajouter une date limite d'utilisation aux attestations pour limiter les risques de fraude	· Requiert un appareil (téléphone) compatible · Requiert une pièce d'identité compatible · Solution difficilement généralisable au niveau international

Profilage social basé sur une analyse sémantique ou lexicale du contenu publié sur la plateforme

L'idée est d'utiliser les données sociales de l'utilisateur pour estimer son âge. Il peut s'agir de liens de proximité avec d'autres personnes dont l'âge est connu, de structures sociales spécifiques, du fait de suivre certaines personnalités, d'afficher une inscription à une école, de détecter des souhaits d'anniversaires, etc.

+	−
· Peu contraignant et transparent pour l'utilisateur · Fraude *a priori* complexe à mettre en œuvre	· En l'état, le taux de faux-positifs est très élevé · Dépend de la quantité et du type de contenu publié par l'utilisateur · N'est pas applicable sur toutes les plateformes · Requiert un profilage actif et massif · Ne fonctionne qu'après inscription sur la plateforme, et au bout d'une durée variable

Vérification par un bureau de tabac et délivrance d'un jeton unique

+	−
· Très bonne précision et granularité dans l'estimation de l'âge en l'absence de fraude · Ne nécessite pas la mise en ligne de documents identifiants	· Très contraignant pour l'utilisateur · Incertitude sur le taux de fraudes (cf vente de tabac ou d'alcool ne se fait pas toujours avec une vérification de l'âge)

Test de cohérence sur les déclarations

Cette solution consiste à périodiquement redemander à l'utilisateur sa date de naissance ou bien à vérifier que la date de naissance concorde avec celle fournie à d'autres services de la même plateforme (par exemple que celle mentionnée sur Instagram correspond à celle fournie sur Facebook)

+	−
· Peu contraignant pour l'utilisateur	· Ne permet pas de détecter des mineurs avant leur utilisation de la plateforme (dans le cas du test de cohérence temporelle) · N'est pas applicable à toutes les plateformes (dans le cas du test de cohérence entre services)

	· Efficacité limitée dès lors que la solution est connue · Fraude aisée · Implique la communication d'informations sur l'utilisateur entre différents services (dans le cas du test de cohérence entre services)

Bases de données gouvernementales

Dans ce système, on considère des vérificateurs agréés, qui auraient accès à des bases nationales d'identité (Insee, sécurité sociale, impôts, etc.).

L'utilisateur rentre des identifiants (par exemple nom, prénom, date de naissance, ville de naissance, ou éventuellement numéro de sécurité sociale), et le système vérifie la validité de ces données (en particulier la date de naissance).

Une double-authentification peut éventuellement être requise (e.g. envoi d'un SMS ou d'un mail par le service concerné) afin d'augmenter la fiabilité de la procédure.

✚	▬
· Procure une certitude forte quand est associé à de la double-authentification · Ce qui est transmis et le destinataire sont clairement établis pour l'utilisateur · Rapide d'exécution	· Demande une certification des vérificateurs · L'identité de l'utilisateur est transmise au vérificateur · Sans double-authentification la fraude est facile · Le service de base d'identité est informé de l'existence d'une demande de l'utilisateur

Estimation biométrique de l'âge

L'âge est vérifié à partir de facteurs biométriques, par exemple par analyse faciale photo ou vidéo. L'analyse faciale est à distinguer de la reconnaissance faciale : on cherche ici à vérifier l'âge, pas à faire un appariement avec une base de photos d'individus connus. D'autres paramètres peuvent inclure la voix, la vitesse/manière dont on frappe le clavier, etc.

✚	▬
· Raisonnablement efficace sur les populations éloignées de la limite.	· Fraude facile à mettre en œuvre selon le degré de complexité de l'estimation (grimage, enregistrement d'autrui) · Faible fiabilité aux limites

· Peu d'informations sont fournies, pas besoin de fournir une identité en tant que telle · Rapide pour l'utilisateur	· Les enregistrements peuvent être transmis à des tiers selon les CGU (NB : l'acteur Yoti indique ne pas le faire) · Besoin d'ajouter une autre méthode en cas d'échec de l'utilisateur pendant la vérification · Afin d'éviter de potentielles discriminations, les modèles doivent être aussi efficaces pour toutes les populations, indépendamment du sexe ou de la couleur de peau notamment.

Une variante de cette estimation biométrique de l'âge externalisée chez un vérificateur tiers pourrait consister à installer le modèle de reconnaissance de l'âge directement sur l'appareil de l'individu. L'application pourrait ainsi fournir une garantie de l'âge, sans transmettre d'information à quelque tiers que ce soit. Cette proposition n'ayant été trouvée nulle part, il serait nécessaire de recevoir l'avis d'experts extérieurs afin de mieux cerner le champ des possibles sur cette question.

+	−
· Voir supra · Respect de la vie privée : aucune information ne sort de l'appareil	· Voir supra · Possible lourdeur du modèle sur les vieux appareils

Quelques exemples de solutions commerciales de vérification d'âge

AgeID (MindGeek)
Nécessite de renseigner une adresse mail et un mot de passe puis contrôle à l'aide de fournisseurs d'identité tiers avec une carte de crédit, passeport, permis ou bon. Doutes par rapport à l'utilisation des données (politique de confidentialité permet le transfert des informations).

AgeChecked
Vérification à l'aide d'une application. Une fois la preuve de majorité apportée, un identifiant et un mot de passe sont générés automatiquement.
Ce système est assez similaire à l'idée de bon précédemment évoquée

AgePass (AVSecure)
Preuve de la majorité soit par bon, soit par numéro de téléphone, puis blockchain privée.

Yoti
Reconnaissance de l'âge à partir de courtes vidéos (ou de pièces d'identité).

Effort de standardisation internationale

Parmi les efforts pour faire émerger des solutions sur le sujet, des acteurs privés se sont regroupés notamment par le biais de *EU Consent Consortium*[25] et supportent une proposition de norme ISO, qui est actuellement en cours d'étude (ISO/IEC PWI 7732 - vérification d'âge), et a donné lieu à une version préliminaire[26].

Ce projet de norme propose plusieurs niveaux de certitude, suivant le niveau de certitude souhaité, présentés Figure 3.

Figure 3 – Niveaux de certitude de la vérification d'âge

Zero	Basic	Standard	Enhanced	Strict
• Based on self-asserted age attributes • No validation or trust elevation deployed • No attempt has been made to address contra indicators • Could be utilised in low risk or only where indicative age is required • Unlikely to be satisfactory for legally defined age-related eligibility	• Based on self-asserted age attributes with a single age assurance component that has low evaluation assurance level • Partial or simple validation or trust elevation; contra indicators may still be present • Could be used for unregulated age gateways	•Based on at least one age assurance component with standard evaluation assurance levels •Validated and all contra indicators addressed • Considered to be the minimum standard required for regulated age related eligibility unless a higher level is specified	• Based on two or more age assurance components with standard evaluation assurance levels • Validated and all contra indicators addressed • Likely to be useful for enhanced risk goods, content or services age-related eligibility	•Based on two or more age assurance components with higher evaluation assurance levels •Validated and all contra indicators addressed •Likely to be useful where age-related eligibility is critical to safeguarding or protecting the rights or freedoms of individuals

Source : euCONSENT

Bien que les descriptions ne soient pas fournies pour chaque élément du schéma fourni par l'AVPA, on peut émettre les suppositions suivantes :

- → Le niveau basique devrait se contenter d'auto-déclaratif, de "*Passive AI*" (comme les IAs de Facebook détectant les anniversaires) et de "*Contra Indicators*" (blocages après avoir rentré une date de naissance non-compatible).
- → Le niveau standard pourrait procéder à des estimations d'âge par le biais d'IA de reconnaissance faciale par exemple ("*Active Age Estimation*").
- → Le niveau avancé proposerait une validation de pièce d'identité, détection des mouvements (vérifier qu'il ne s'agit pas d'une simple photo de majeur), et serait testé à l'aide d'attaques dites de présentations[27] (tentatives de frauder le système, incluant notamment de faux papiers d'identité, masques, etc.).
- → Le niveau strict exigerait une authentification multi-facteurs (par exemple pièce d'identité et SMS qui devraient être liés, utilisation d'un voucher, estimation d'âge par des IAs, etc.).

Notons que ces standards de vérification peuvent également être utilisés avec un tiers (qui prendrait en charge ces vérifications), avec ou sans double-anonymat.

[25] https://euconsent.eu/

[26] https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/

[27] https://www.accscheme.com/services/age-assurance/presentation-attack-detection

Dépôt légal : Mai 2022
ISSN (en ligne): 2824-8201

Service à compétence nationale, le Pôle d'expertise de la régulation numérique (PEReN) fournit, aux services de l'État et autorités administratives intervenant dans la régulation des plateformes numériques, une expertise et une assistance technique dans les domaines du traitement des données, des data sciences et des procédés algorithmiques. Il s'investit également dans des projets de recherche en science des données à caractère exploratoire ou scientifique.

PEReN – 120 rue de Bercy, 75572 Paris Cedex 12 – contact.peren@finances.gouv.fr