

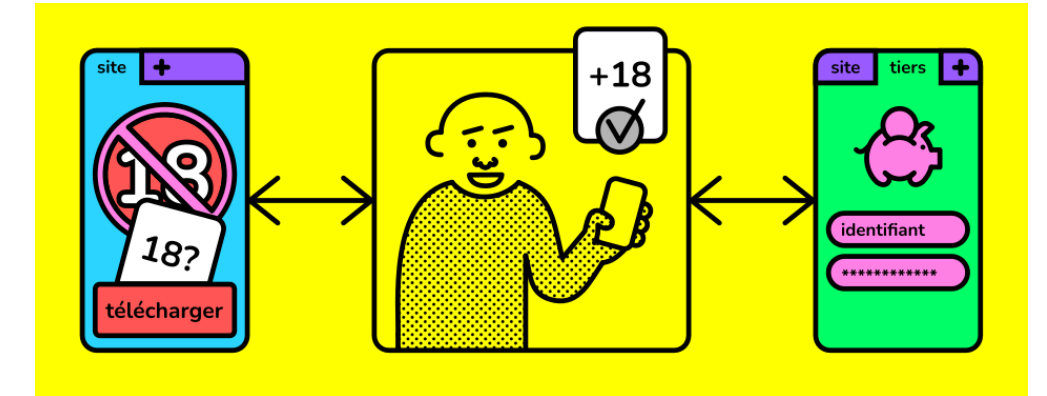
Contrôle de l'âge en ligne

Enjeux relatifs à la protection des données

Une évolution favorable à la prise en compte de la protection des données

› Le démonstrateur publié en 2022 (Olivier Blazy, CNIL, PEReN)

- › Zero-knowledge proofs, double anonymat...



› La prise en compte de la protection des données et de la vie privée dans la réglementation européenne et les standards internationaux

- › Une nécessité notamment pour l'acceptabilité des dispositifs ;
- › Règlement sur les services numériques (2022/2065) ;
- › Règlement eIDAS v2 sur l'identité numérique (2024/1183) ;
- › Norme ISO/IEC 27566-1 (2025) ; etc.



› Des positions de la CNIL reprises par la commission européenne

- › Concept de « double aveugle » (lignes directrices de la CE, 2025)
- › Intégration de ZKP (age verification blueprint, 2026)



› La CNIL n'est pas directement compétente sur la protection des mineurs en ligne

- › Le gouvernement, le parlement, la commission européenne et les coordinateurs des services numériques sont en charge de définir et de faire appliquer les obligations et éventuelles restrictions concernant les services numériques.

› La CNIL est une autorité de protection des données, s'assurant de la conformité des traitements, notamment :

- › En lien avec ses homologues européens et le comité européen de protection des données ;
- › Au regard du principe de proportionnalité ;
- › Au regard du principe de minimisation ;
- › Au regard des droits des personnes concernées ;
- › Au regard du principe de protection des données personnelles par défaut et dès la conception.

L'application du principe de minimisation

› Ne transmettre que l'information nécessaire

- › Un service en ligne n'a généralement pas besoin de connaître l'identité, la date de naissance ou l'âge exact de ses utilisateurs.

› Éviter que les services en ligne collectent l'identité de leurs utilisateurs

- › La CNIL recommande depuis 2021 de confier à des tiers le traitement des données personnelles nécessaires pour contrôler l'âge des utilisateurs.

› Minimiser les durées de conservation

- › Les données collectées dans le cadre d'un contrôle de l'âge devraient être supprimées dès qu'elles ne sont plus strictement nécessaires ;
- › Les identifiants, journaux techniques et autres métadonnées liés aux opérations de contrôle de l'âge ne devraient pas permettre de profiler les utilisateurs ou de remonter à leur identité.

L'intérêt des preuves ou attestations d'âge

› Limiter les traitements répétés de données personnelles

- › L'utilisation de preuves d'âge permet de réaliser plusieurs contrôles de l'âge après un unique traitement de document d'identité, selfie vidéo, etc.

› Conserver la preuve localement ou dans une espace en ligne protégé

- › Une preuve d'âge peut par exemple être conservée sur le terminal de l'utilisateur ou auprès d'un service en ligne sous forme chiffrée, accessible et utilisable uniquement par l'utilisateur.

› Cloisonner émission et utilisation de la preuve

- › Les architectures de type « *wallet* » permettent d'atteindre facilement les garanties de « double aveugle », c'est-à-dire :
 - Le service en ligne n'apprend que l'information d'âge strictement nécessaire ;
 - L'émetteur de la preuve ne sait ni auprès de quelle plateforme la preuve est utilisée, ni à quel moment.

Pour des solutions inclusives, diversifiées et contestables

- **Ne pas imposer un équipement ou un document unique**
 - › L'accès aux services numériques ne devrait pas obliger les utilisateurs à disposer d'un smartphone récent, d'une webcam ou d'une carte d'identité électronique.
- **Proposer plusieurs méthodes de contrôle**
 - › Les utilisateurs devraient disposer d'un choix réel entre des solutions accessibles et offrant un niveau suffisant de protection des données.
- **Permettre la contestation et le recours**
 - › Une solution devrait être proposée en cas d'erreur ou d'impossibilité d'utiliser les méthodes proposées.

Merci pour votre attention