AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Allegato B alla delibera n. 96/25/CONS

QUADRO EUROPEO E NAZIONALE SULLE MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI

Sommario

I. Premessa

Metodi di verifica online dell'età per i minori

Per oltre due decenni, è stata disponibile una gamma limitata di metodi di verifica dell'età *online* per proteggere i minori dall'accesso a contenuti *online* non adatti alla loro età. Tuttavia, la protezione di tale fascia di utenti nell'ambito delle attività svolte *online* sta diventando un aspetto sempre più vitale nell'attuale contesto sociale.

Come riportato nel report "*On line age verification methods for children*", redatto dall'EPRS (*European Parliamentary Research Service*), di febbraio 2023, numerosi Paesi stanno introducendo leggi e/o codici di condotta per affrontare questo tema. Anche a livello dell'UE si stanno intensificando gli sforzi in questo senso mediante l'adozione di un codice di condotta, in fase di analisi. L'individuazione delle misure di verifica dell'età dell'utente presenta, come meglio chiarito di seguito, diversi elementi di complessità, non ultimo nell'ambito della tutela della privacy, del monitoraggio e della necessità di migliorare le competenze digitali di genitori e figli.

In base a quanto contenuto nel citato documento, si osserva che, anche a seguito della pandemia di coronavirus, i minori si sono abituati a trascorrere più tempo *online*. Stime globali rivelano che un minore su tre è un utente di Internet e che un utente di Internet su tre ha meno di 18 anni. Nell'UE, la maggior parte dei minori utilizza il proprio smartphone ogni giorno, quasi il doppio rispetto a 10 anni fa. Nella maggior parte dei casi, però, gli ambienti *online* a cui accedono non sono stati originariamente progettati per loro (ad esempio in alcuni casi i *social media* richiedono un'età minima di 13 anni per i loro utenti). A livello generale si rileva che i servizi digitali non utilizzano metodi adeguati di verifica dell'età o di consenso dei genitori.

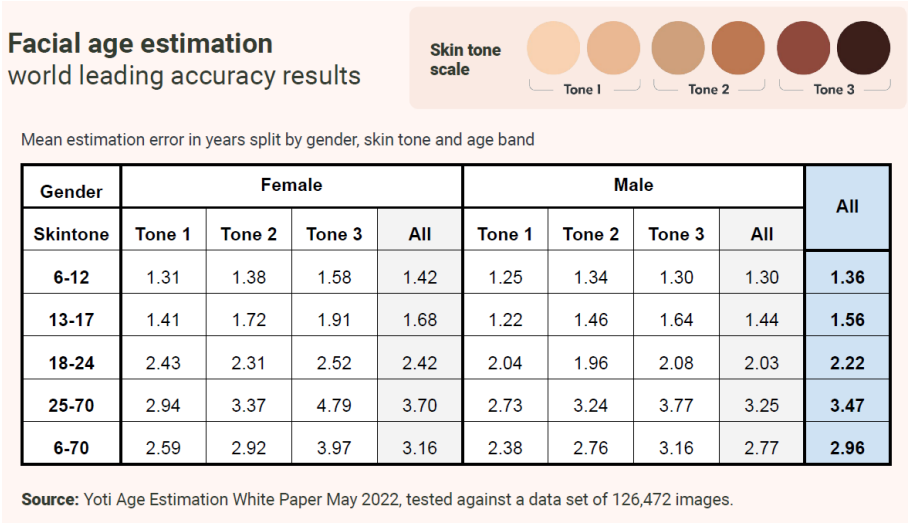
I metodi di verifica dell'età *online* sono sempre più diversificati. Di seguito è riportato un elenco di quelli che secondo il report dell'EPRS sono ritenuti i più comuni.

A. **Autodichiarazione:** i metodi che richiedono, ad esempio, all'utente di inserire la propria data di nascita senza ulteriori prove per confermare tale informazione, oppure che chiedono all'utente di spuntare una casella di un form online per confermare di avere almeno 18 anni. È stato dimostrato che questo metodo, il più comune tra tutti, può essere facilmente aggirato. Gli esempi più diffusi includono l'autodichiarazione della propria data di nascita.

B. **Carta di credito:** qui gli utenti sono tenuti a far verificare la validità delle loro carte, inserendo i dati della carta di credito o, in alcuni casi, effettuando un pagamento bancario o con carta di 0,01 €. Il *payment provider* fornisce la conferma della maggiore età. Questo metodo viene utilizzato principalmente da siti di e-commerce e app che vendono prodotti per adulti come alcolici o contenuti per adulti. Al di là del rischio intrinseco di *phishing*, nel documento in parola si ritiene che non sia possibile accertare che la persona che utilizza la carta ne sia il legittimo titolare; inoltre, l'età per possedere una carta di credito varia da Paese a Paese.

C. **Biometria:** questo metodo si basa sull'intelligenza artificiale (AI), che alimenta l'uso delle tecnologie biometriche, comprese le applicazioni di riconoscimento facciale. Questi sistemi possono essere utilizzati per analizzare le caratteristiche del viso con un *selfie* per accertare che la persona che richiede l'accesso abbia più di 18 anni. Tuttavia, tale approccio comporta un margine di errore; inoltre, i minorenni potrebbero utilizzare il volto di una persona maggiorenne per ottenere accessi non consentiti. I metodi di autenticazione che utilizzano la biometria sollevano problemi di *privacy* per via di un trattamento eccessivo dei dati e alla profilazione.

   Viene considerato, da alcuni fornitori, un processo istantaneo - scalabile fino a decine di milioni di unità al giorno – ove nessuna immagine viene archiviata. Di seguito si riporta una tabella contenente, sulla base di analisi effettuate da alcuni analisti, una indicazione sulle prestazioni in termini di errore statistico della stima.



Mean estimation error in years split by gender, skin tone and age band

Gender	Female				Male				All
Skintone	Tone 1	Tone 2	Tone 3	All	Tone 1	Tone 2	Tone 3	All	
6-12	1.31	1.38	1.58	1.42	1.25	1.34	1.30	1.30	**1.36**
13-17	1.41	1.72	1.91	1.68	1.22	1.46	1.64	1.44	**1.56**
18-24	2.43	2.31	2.52	2.42	2.04	1.96	2.08	2.03	**2.22**
25-70	2.94	3.37	4.79	3.70	2.73	3.24	3.77	3.25	**3.47**
6-70	2.59	2.92	3.97	3.16	2.38	2.76	3.16	2.77	**2.96**

Source: Yoti Age Estimation White Paper May 2022, tested against a data set of 126,472 images.

D. **Analisi dei modelli di utilizzo *online* (analisi del comportamento online):** si tratta di sistemi di verifica dell'età per inferenza, come l'importazione della cronologia di navigazione in Internet dell'individuo o l'analisi della sua "maturità" tramite un questionario o dei contenuti o degli acquisti online generati dagli utenti.

E. **Verifica *offline*:** viene effettuata utilizzando cosiddette "scratch cards", ossia acquisendo in ID che attesta la maggiore età, o controlli dell'età *offline in-situ* tramite documenti. Si tratta di una verifica cosiddetta *one-time.*

F. **Verifica *online*:** viene effettuata tramite controlli a mezzo documenti. A esempio nel caso del confronto con foto-tessera (Photo-ID matching) sono confrontate la fotografia presente sul documento di identità caricato dall'utente, dove è presente anche la data di nascita, e con una immagine fotografica dell'utente scattata all'atto del caricamento del documento per verificare che si tratta o meno della stessa persona.

G. **Consenso dei genitori:** alcune app e servizi richiedono il consenso dei genitori per registrare un minorenne a un servizio digitale. Tuttavia, la potestà genitoriale raramente è completamente verificata. Dimostrare la potestà/tutela genitoriale potrebbe comportare il controllo dei documenti di identità tradizionali e dei registri di famiglia.

H. ***Vouching*:** viene chiesto a utenti diversi dai genitori di fornire *online* conferma che un bambino che richiede l'accesso *online* ha l'età giusta.

I. **Identificazione digitale (ID digitale):** questo metodo si basa sugli strumenti offerti dalle autorità statali per verificare l'identità e l'età delle persone prima di concedere loro l'accesso ai servizi digitali (es. SPID).

J. **Portafoglio per l'identità digitale (*Digital identity wallet*):** il portafoglio per l'identità digitale consente agli utenti di dimostrare la propria identità quando necessario per accedere a servizi *online*, condividere documenti digitali o semplicemente dimostrare un attributo personale specifico, come ad esempio l'età, senza rivelare le generalità complete o altri dati personali. In ambito UE c'è la proposta di creare un portafoglio europeo di identità digitale[1].

K. **Verifica dell'età tramite un'app specifica:** si tratta di applicativi che sono, per lo più, collegati alla preventiva acquisizione di un documento di identità e di un selfie. In alcune applicazioni disponibili nel mercato, gli utenti forniscono copia di un documento d'identità e

[1] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox

scattano un selfie biometrico per creare il proprio ID digitale riutilizzabile. Una volta verificati, l'accesso avviene a seguito di scansione di un codice QR.

L. Alla suddetta lista è possibile aggiungere i modelli che si basano **sul numero di telefono mobile** e il confronto con i dati in possesso del gestore telefonico. Altri effettuano una verifica mediante **e-mail** o anche mediante **analisi vocale**.

M. **Open banking:** questo metodo utilizza alcune informazioni che un istituto di credito ha registrato riguardo all'età di un utente, con il consenso dell'utente. La conferma se l'utente ha o meno più di 18 anni viene condivisa con il sito/provider del servizio che richiede la verifica dell'età dell'utente. I dati personali dell'utente, tra cui la data di nascita, non vengono condivise con il sito/provider del servizio.

Solo di recente, in base alla ricerca svolta, le piattaforme social hanno iniziato ad applicare misure per verificare l'età.

A. Nel 2022, **Instagram** ha iniziato a testare uno strumento per garantire che gli utenti abbiano l'età che dichiarano di avere; in alcuni casi ha anche iniziato a utilizzare la tecnologia biometrica per l'analisi facciale.

B. **YouTube** ha lanciato un'app dedicata ai minori e ha introdotto nuove pratiche relative ai dati.

C. **Meta** ha creato Messenger Kids su Facebook che consente ai minori di connettersi solo con contatti approvati dai genitori.

D. **Tik tok** non dispone di un metodo di verifica dell'età ma potrebbe vietare gli account dopo la registrazione.

E. **Twitte**r verifica il consenso dei genitori richiedendo documentazione (carta d'identità/certificato di nascita, ecc.). Twitter afferma che i documenti vengono trattati in modo confidenziale e sono cancellati dopo la verifica.

F. I siti di commercio elettronico che vendono prodotti e servizi per adulti come giochi d'azzardo, alcol o pornografia dispongono di un'ampia gamma di metodi di verifica dell'età come carte di credito, scratch cards e dati biometrici.

In base alle conclusioni del report suddetto rimangono alcune sfide chiave, di cui le tre seguenti sono particolarmente rilevanti:

A. Rischi in materia di privacy/sicurezza informatica: nonostante l'uso diffuso di metodi di verifica dell'età in alcuni settori, si teme ancora che essi comportino rischi per la privacy e la sicurezza informatica. Data la sensibilità dei dati raccolti da alcuni sistemi di verifica dell'età, **alcuni suggeriscono di implementare una certificazione fornita da terze parti**. Ad oggi non esistono orientamenti comuni dell'UE sui metodi per determinare la verifica dell'età ed è constatato che i minorenni aggirano facilmente la maggior parte delle soluzioni.

B. Contenuti non sufficientemente attraenti per i minorenni: poiché le app e i servizi digitali per minorenni tendono a fornire un insieme limitato di funzionalità, molti preferiscono mentire sulla loro età pur di utilizzare quelli pensati per gli adulti. Ciò rende i minorenni più vulnerabili non solo ai rischi per la privacy ma anche alle minacce alla sicurezza, come l'adescamento online o all'esposizione a contenuti inappropriati per la loro età. È necessario considerare l'usabilità per i giovani utenti durante la fase di progettazione del software.

C. Migliori competenze digitali: genitori, bambini e tutori necessitano di migliori competenze digitali e di una maggiore consapevolezza dei rischi connessi.

A livello normativo, in ambito UE, si presenta il seguente quadro.

Prima dell'adozione del Regolamento generale sulla protezione dei dati **(GDPR),** entrato in vigore nel 2018, non esistevano restrizioni specifiche al trattamento online dei dati dei minori in Europa. Il GDPR all'articolo 8 introduce la verifica, da parte dei titolari del trattamento dei dati, per quanto riguarda l'età e il consenso dei genitori. Inoltre, al considerando (38) viene specificato che i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. La **direttiva sui servizi di media audiovisivi (AVMSD)** richiede l'adozione di misure adeguate a proteggere i minori dai contenuti dannosi online, anche attraverso la verifica dell'età. Inoltre, la nuova strategia europea per un'Internet migliore per i minorenni prevede un **codice di condotta dell'UE** per una **verifica adeguata all'età entro il 2024**, basandosi sulle nuove norme della legge sui servizi digitali (DSA) e in linea con l'AVMSD e il GDPR. Un codice simile esiste già in altre parti del mondo, come il Regno Unito e la California.

Nel contesto della **proposta UE sull'eID**, la **Commissione intende rafforzare i metodi di verifica dell'età mediante un solido quadro di certificazione e interoperabilità**. Inoltre, la **proposta di regolamento per combattere gli abusi sessuali sui minori online** prevede una migliore verifica dell'età online. Va citato anche il **progetto euCONSENT**, cofinanziato dall'UE, che sta sviluppando un metodo di verifica dell'età interoperabile basato su browser. Il Parlamento europeo ha chiesto in diverse occasioni metodi migliori di verifica dell'età per proteggere i minori online, anche nella sua relazione di iniziativa sulla protezione dei consumatori nei videogiochi online adottata nel gennaio 2023 e nella sua risoluzione del marzo 2021 sui diritti dei minori alla luce *della Strategia UE sui diritti del bambino*. Allo stesso modo, metodi migliori di verifica dell'età per proteggere i minori online fanno parte della proposta della Commissione Europea di Dichiarazione europea sui diritti e principi digitali per il decennio digitale e della Dichiarazione dell'OCSE su un futuro digitale affidabile, sostenibile e inclusivo.

Ulteriori utili informazioni di contesto sono riportate nel documento "***Consistent implementation and enforcement of the European framework for audiovisual media services***", AVMS, redatto **dall'ERGA Subgroup 1**.

Infatti, nel 2023, il sottogruppo 1 dell'ERGA che si occupa dell'attuazione della Direttiva suddetta ha condotto un'analisi comparata dei meccanismi di verifica dell'età (AVM) esistenti, in particolare per le piattaforme di condivisione video nell'Unione Europea (UE).

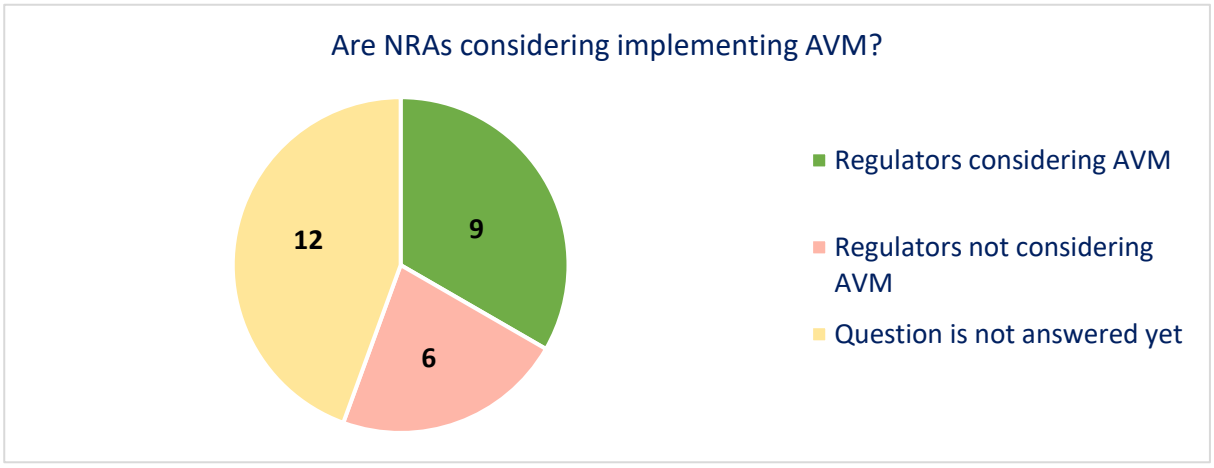
Anche l'ERGA riconosce che identificare e implementare meccanismi efficienti per impedire ai bambini di accedere a contenuti dannosi, e in particolare a contenuti pornografici, solleva una serie di sfide, sia in termini di efficienza (poiché alcuni di questi meccanismi possono essere facilmente aggirati) che di privacy. La sfida per i legislatori e i regolatori è trovare il giusto equilibrio tra garantire un elevato livello di privacy per gli utenti, un meccanismo efficiente e la sua ampia attuazione da parte di tutti gli attori interessati.

Per raccogliere dati al riguardo, in data 17.07.2023 è stato inviato ai Paesi che partecipano all'ERGA un questionario in merito al recepimento degli articoli 6(a) e 28-ter (comma 3, letteraf) della Direttiva AVMS e all'attuazione nazionale dell'AVM, con particolare attenzione all'accesso dei minori a materiale pornografico. 27 ANR hanno risposto in rappresentanza di 25 Stati membri dell'UE e uno Stato membro dell'EFTA.

23 NRA hanno risposto che esistono restrizioni legali che vietano ai minori l'accesso a contenuti pornografici, indipendentemente dal tipo di servizio (servizi lineari, non lineari o online).

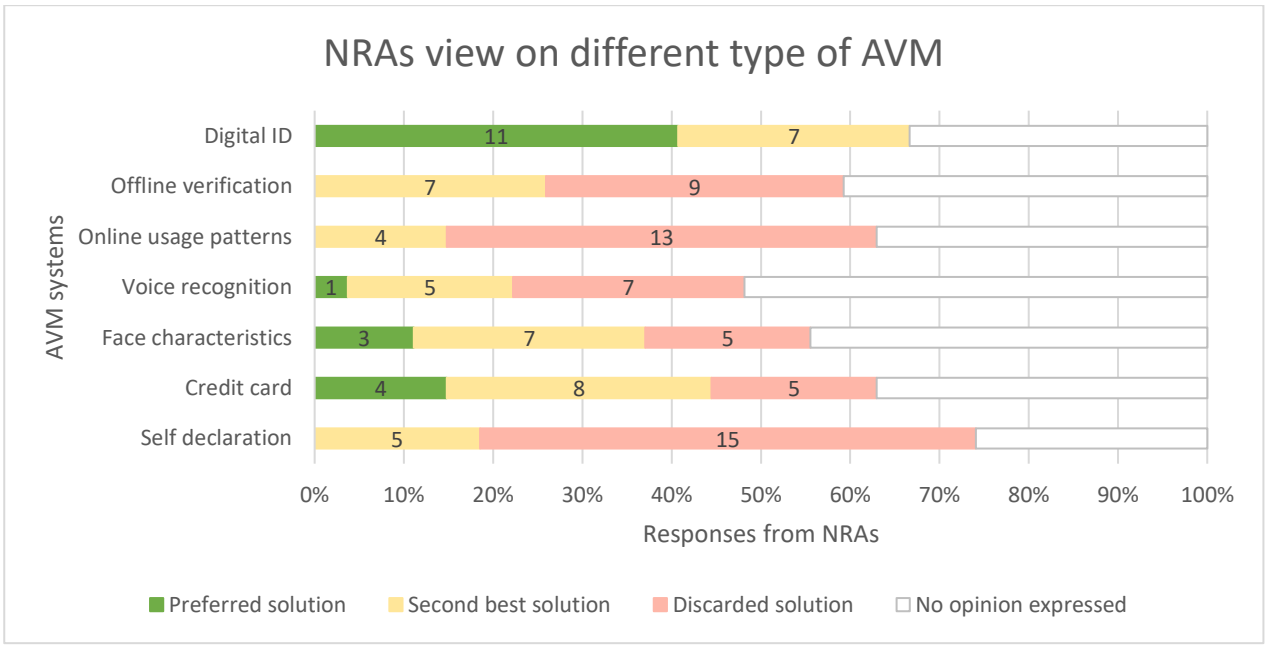
Avuto particolare riguardo alla implementazione di meccanismi di verifica dell'età negli stati membri dell'ERGA per limitare l'accesso dei minori ai contenuti pornografici, 12 ANR hanno risposto di non avere ancora una specifica posizione.

9 NRA hanno risposto che l'AVM è stata presa in considerazione, mentre 6 NRA hanno risposto in senso contrario.



Nella maggior parte dei Paesi dove sono state adottate iniziative (CZ, DE, DK, ES, FR, IT, LU, PL, PT) il meccanismo adottato o di prossima adozione è previsto dalla legge.

Per quanto riguarda la soluzione tecnica emerge il seguente quadro, in risposta alla domanda su quale sia **la soluzione preferita dai membri ERGA per AVM:**



La verifica dell'età basata sull'identità digitale, come il ricorso agli strumenti offerti dallo Stato per verificare l'identità delle persone in generale, **sembra essere la soluzione preferita[2].**

Al contrario, l'autodichiarazione è la soluzione meno preferita tra quelle proposte in base alle risposte, poiché 15 NRA l'hanno scartata e 5 NRA l'hanno collocata al secondo livello migliore e nessuna come soluzione preferita.

Anche i modelli di **utilizzo online e la verifica offline** sono considerati non adeguati e nessuna ANR li cita come soluzione preferita[3].

Per quanto riguarda **l'AVM basato su carta di credito**, 4 NRA hanno risposto a favore, 5 NRA risultano contrarie e 8 NRA non sono contrarie ma riscontrano ancora problemi al riguardo.

Scarso consenso può essere evidenziato con riferimento ai metodi basati sull'analisi delle caratteristiche del volto o sul riconoscimento vocale[4].

Il report dell'ERGA individua **le seguenti principali sfide per i sistemi di AV:**

- l'efficacia del sistema;

- le questioni relative alla protezione dei dati;

- la facilità d'uso e accessibilità.

Il report ERGA conclude che, sebbene gli AVM non siano ancora pienamente attuati (ad eccezione dei sistemi di autodichiarazione) nella maggior parte degli Stati membri, molte ANR stanno affrontando il tema con particolare riferimento ai temi relativi all'efficienza e alla sicurezza dei vari sistemi. L'intervento di un intermediario indipendente è un'opzione presa in considerazione da molte ANR, a dimostrazione delle preoccupazioni relative alla privacy. A questo proposito, la soluzione basata **sull'identità digitale** sembra quella preferita dalla maggior parte delle ANR, anche se alcune non ne sono del tutto convinte. **L'autodichiarazione viene scartata quasi all'unanimità** come un'efficace AVM.

Soluzioni tecniche disponibili nel mercato

I sistemi realizzati da soggetti terzi, che forniscono il servizio di verifica dell'età ai richiedenti consentono di ottenere le seguenti informazioni:

- se l'età dell'utente è superiore al requisito minimo;
- l'età dell'utente.

In genere si utilizzano diverse metodologie, tra cui quelle più utilizzate risultano le seguenti:

1. Stima dell'età mediante riconoscimento facciale (biometria)
2. Scansione del documento d'identità
3. App

[2] 11 ANR (BE – VRM, BE – CSA, DE, EE, HR, LT, LU, LV, NL, SI, SK) l'hanno classificata come la soluzione preferita, 7 ANR (AT, CZ, EL, FR, IT, PL, PT) come la soluzione di seconda scelta e nessuna ANR ha risposto respingendo la soluzione.
[3] I modelli di utilizzo online hanno 13 risposte (AT, BE – VRM, BE – CSAbe, CZ, EE, FR, LT, LU, NL, NO, PL, PT, SK) contro e 4 risposte (HR, IT, LV, SI) come secondo migliore; la verifica offline ha 9 risposte (BE – VRM, BE – CSA, EE, FR, LT, LU, LV, NL, PL) contro e 7 risposte (AT, CZ, HR, IT, PT, SI, SK) come seconda migliore.
[4] la prima raccoglie 3 risposte (AT, DE, NL) a favore, 7 risposte (HR, FR, IT, LV, LU, PL, SK) come seconda migliori opinioni e 5 risposte (BE – VRM, BE – CSA, CZ, EE, LT) contrarie; la seconda ha 1 risposta (NL) a favore, 5 risposte (AT, IT, LU, LV, SK) come seconda migliore e 7 risposte (BE – VRM, BE – CSA, CZ, EE, HR, LT, PL) contro.

4. Carta di credito
5. Numero di cellulare
6. Confronto con i dati presenti in database certificati.

1. Stima dell'età

Viene chiesto all'utente di scattare un selfie usando la telecamera del proprio dispositivo. Questo cattura più immagini e una verrà analizzata dal sistema di stima dell'età basato su algoritmi di Intelligenza Artificiale.

2. Scansione del documento d'identità

Viene chiesto all'utente di scansionare il documento di identità usando la telecamera del proprio dispositivo. Il fornitore estrae le informazioni dal documento di identità e verifica se l'età è superiore a quella richiesta dall'organizzazione usando la data di nascita.

All'utente può essere chiesto anche di scattare un selfie usando la telecamera del dispositivo. Questo per verificare che il documento d'identità appartenga all'utente. I dati acquisiti, come il documento d'identità e il selfie, sono immagazzinati nel centro dati. Una volta completata la sessione, vengono cancellate tutte le informazioni personali.

3. App

Viene chiesto all'utente di scansionare un codice QR direttamente dall' app che effettua la verifica e invia al sito/piattaforma le informazioni sulla data di nascita. Prima di questo passaggio l'utente deve completare un processo di verifica one-time con l'app caricando il documento d'identità e un selfie.

4. Carta di credito

Viene chiesto all'utente di inserire il numero, la data di scadenza, il codice postale e il numero CV2 della carta di credito.

I dati sono inviati al fornitore del servizio di pagamento e viene trattenuta una minima somma per verificare che la carta sia attuale e valida. Una volta verificata l'età la somma viene restituita.

5. Numero di cellulare

Gli utenti inseriscono il loro nome, data di nascita, numero di cellulare e indirizzo.

Questi dati sono inviato all'operatore. Gli utenti riceveranno un SMS con la richiesta di confermare l'età rispondendo al messaggio. Ciò serve a confermare che siano in possesso del cellulare. Il fornitore del servizio di telefonia conferma quindi che i dati inseriti sul sito corrispondono ai dati dell'account del servizio radiomobile, che sono usati per determinare che l'utente ha più di 18 anni.

6. Controllo del database

Viene chiesto di dimostrare l'età usando il nome, la data di nascita e l'indirizzo.

Questi dati sono inviati a un ente di certificazione anagrafica per confermare che siano accurati e ottenere o confermare la tua data di nascita.

Controlli dell'età riutilizzabili

Per ridurre il numero di volte in cui è richiesta la verifica dell'età online, alcuni fornitori sviluppano un sistema di "token di età". I token di età funzionano come prove digitali di un controllo dell'età e consentono di riutilizzare il risultato del controllo dell'età per tutto il tempo in cui l'organizzazione

lo consente. È possibile salvare i token di età in un "account età". Ciò consente di accedere al sito web dell'organizzazione, a un altro browser o a un altro dispositivo senza dover dimostrare l'età ogni volta[5].

II. Quadro normativo nazionale

L'ordinamento italiano si è occupato in più previsioni della disciplina dell'età da parte dei destinatari dei servizi offerte dalle piattaforme online.

Il decreto legislativo 8 novembre 2021, n. 208 recante *"Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato",* (di seguito TUSMA), così come modificato dal decreto legislativo del 25 marzo 2024, n. 50, ha introdotto, all'articolo 3, comma 1, lett. c) nell'ordinamento italiano la definizione di *servizio di piattaforma per la condivisione di video* quale *"un servizio, quale definito dagli articoli 56 e 57 del Trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso, di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi o video generati dagli utenti destinati al grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento".*

Inoltre, ha dedicato due specifiche norme alla disciplina dei servizi di piattaforma per la condivisione di video: l'articolo 41 e 42 del TUSMA.

In particolare, l'articolo 41, fornisce i criteri per identificare i fornitori di detti servizi stabiliti o che si considerano stabiliti in Italia.

Inoltre, detta previsione ha introdotto nell'ordinamento italiano, una specifica disciplina rivolta ai fornitori di tali servizi stabiliti in un altro Stato membro i cui contenuti ivi diffusi sono rivolti al pubblico italiano.

Al riguardo al comma 7 dell'articolo 41 stabilisce che:

Fatti salvi gli articoli da 14 a 17 del decreto legislativo 9 aprile 2003, n. 70, e fermo quanto previsto ai commi precedenti, la libera circolazione di programmi, video generati dagli utenti e comunicazioni commerciali audiovisive veicolati da una piattaforma per la condivisione di video ***il cui fornitore è stabilito in un altro Stato membro e diretti al pubblico italiano può essere limitata,*** *con provvedimento dell'Autorità, secondo la procedura di cui all'articolo 5, commi 2, 3 e 4 del decreto legislativo n. 70 del 2003, per i seguenti fini: a) la tutela dei minori da contenuti che possono nuocere al loro sviluppo fisico, psichico o morale a norma dell'articolo 38, comma 1;*

Ai sensi dell'art. 42, commi 1 e 6, dello stesso TUSMA, inoltre, è previsto che:

[5] Quando si visita un sito Web che usa i token di età, cliccando su un pulsante per verificare l'età tramite il fornitore, si presenterà l'opzione di accedere all'account età. Verrà chiesto di inserire username e password. Il sito Web verifica se ci sono token di età nel browser dell'utente che corrispondono ai criteri definiti dall'azienda collegata con l'account dell'utente. Se sì, il fornitore restituisce un risultato per confermare è stato già effettuato un controllo precedente e se il tuo token età soddisfa i suddetti criteri.

1. *Fatti salvi gli articoli da 14 a 17 del decreto legislativo 9 aprile 2003, n. 70, i fornitori di piattaforme per la condivisione di video soggetti alla giurisdizione italiana devono adottare misure adeguate a tutelare:*
   a) *i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale a norma dell'articolo 38, comma 3;*

   [omissis]

6. *Ai fini della tutela dei minori di cui al comma 1, lettera a), i contenuti maggiormente nocivi sono soggetti alle più rigorose misure di controllo dell'accesso.*

L'articolo 42, invece, disciplina le nuove regole da applicare ai fornitori di servizi di piattaforma per la condivisione di video stabiliti o che si considerano in Italia.

Con specifico riferimento agli strumenti di verifica dell'età, al comma 7 dell'art.42 del TUSMA è previsto che:

7. *I fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a:*

   [omissis]

   f) predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori;

   [omissis]

   h) dotarsi di sistemi di controllo parentale sotto la vigilanza dell'utente finale per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori;

Da ultimo, il decreto-legge 15 settembre 2023 n. 123, convertito con modificazioni dalla legge 13 novembre 2023, n. 159, ha introdotto *"Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale"* (di seguito *Decreto*).

In particolare, l'articolo 13-bis recante *"Disposizione per la verifica della maggiore età per l'accesso a siti pornografici"* è stabilito che:

1. *E' vietato l'accesso dei minori a contenuti a carattere pornografico, in quanto mina il rispetto della loro dignità e ne compromette il benessere fisico e mentale, costituendo un problema di salute pubblica.*
2. *Fermo restando quanto previsto dall'articolo 42 del decreto legislativo 8 novembre 2021, n. 208, i gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto.*
3. *L'Autorità per le garanzie nelle comunicazioni stabilisce, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con proprio provvedimento, sentito il Garante per la protezione dei dati personali,* ***le modalità tecniche e di processo*** *che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato*

al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo.

4. *Entro sei mesi dalla data di pubblicazione del provvedimento di cui al comma 3, i soggetti di cui al comma 2 si dotano di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni impartite nel predetto provvedimento.*
5. *L'Autorità per le garanzie nelle comunicazioni vigila sulla corretta applicazione del presente articolo e, in caso di inadempimento, contesta ai soggetti di cui al comma 2, anche d'ufficio, la violazione, applicando le disposizioni di cui all'articolo 1, comma 31, del decreto legislativo 31 luglio 1997, n. 249, e li diffida ad adeguarsi entro venti giorni. In caso di inottemperanza alla diffida, l'Autorità per le garanzie nelle comunicazioni adotta ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino, da parte dei soggetti di cui al comma 2, di condizioni di fornitura conformi ai contenuti della diffida dell'Autorità.*

Detta previsione ha dunque previsto l'introduzione di nuovi strumenti di tutela nei confronti dei minorenni nei confronti dei contenuti, immagini e video, a carattere pornografico diffusi in Italia presso " *i gestori di siti web" e " i fornitori delle piattaforme di condivisione video".*

Alla luce del quadro normativo sopra illustrato, e nella prospettiva di rendere il medesimo effettivo, l'Autorità, nell'ambito dei propri compiti istituzionali, ha avviato con delibera n.9/24/CONS un procedimento che coinvolge tutti i soggetti a vario titolo interessati, al fine di adottare un provvedimento che fissa le modalità tecniche e di processo che i soggetti di cui al comma 2 dell'art. 13-bis del *Decreto* sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo.

La citata delibera ha previsto, all'articolo 3, l'avvio di una consultazione pubblica, della durata di 30 giorni, tramite pubblicazione di una delibera dell'Autorità con allegato documento di consultazione.

In ossequio a quanto previsto dallo stesso articolo 3 della delibera, l'Autorità ha, in esito alla consultazione, acquisito il parere del Garante per la protezione dei dati personali.

Tale approccio è stato ritenuto quello maggiormente efficace vista la varietà di possibili soluzioni per l'accertamento della maggiore età degli utenti, potenzialmente suscettibili di creare differenti livelli di protezione per i minori e, al contempo, di tutela dei dati personali.

III. Gli interventi in ambito europeo

In ambito europeo diverse sono state le previsioni normative atte a proteggere i minori da contenuti diffusi presso piattaforme digitali online che possano nuocere al loro sviluppo, morale, fisico e psicologico.

In particolare, la Direttiva (UE) 2018/1808 del 14 novembre 2018 che ha modificato la direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), ha aggiunto, all'articolo 1, della direttiva 2010/13/UE la lettera a-bis) introducendo la definizione di servizi "*servizio di piattaforma per la condivisione di video*" quale "*servizio quale definito agli articoli 56 e 57 del trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso, di una sua sezione distinguibile o di una sua funzionalità*

essenziale sia la fornitura di programmi, video generati dagli utenti o entrambi per il grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento"»

Inoltre, la predetta Direttiva ha osservato al Considerando (45) che "*Nuove sfide si presentano, in particolare in relazione alle piattaforme per la condivisione di video, su cui gli utenti, in particolare i minori, fruiscono in misura crescente di contenuti audiovisivi. In tale contesto, i contenuti nocivi e i discorsi di incitamento all'odio messi a disposizione sui servizi di piattaforma per la condivisione di video destano crescente preoccupazione. Al fine di proteggere i minori e il grande pubblico da siffatti contenuti, è necessario stabilire norme proporzionate su tali aspetti".*

Inoltre, la predetta Direttiva ha altresì rilevato al successivo Considerando 47 che "*Una quota significativa dei contenuti messi a disposizione sui servizi di piattaforma per la condivisione di video non è sotto la responsabilità editoriale del fornitore di piattaforme per la condivisione di video. Tali fornitori, tuttavia, in genere determinano l'organizzazione dei contenuti, ossia programmi, video generati dagli utenti e comunicazioni commerciali audiovisive, anche in modo automatizzato o con algoritmi. Essi dovrebbero pertanto essere tenuti ad adottare le misure appropriate per tutelare i minori dai contenuti che possono nuocere al loro sviluppo fisico, mentale o morale. Dovrebbero inoltre essere tenuti ad adottare le misure appropriate per tutelare il grande pubblico dai contenuti che istigano alla violenza o all'odio nei confronti di un gruppo o di un membro di un gruppo per uno dei motivi di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea («Carta») o la cui diffusione costituisce reato ai sensi del diritto dell'Unione".*

La predetta Direttiva ha introdotto l'articolo 28-*ter* della Direttiva 2010/13/UE ai sensi del quale al paragrafo 1 ha previsto che *"Fatti salvi gli articoli da 12 a 15 della direttiva 2000/31/CE, gli Stati membri assicurano che i fornitori di piattaforme per la condivisione di video soggetti alla loro giurisdizione adottino misure adeguate per tutelare: a) i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale a norma dell'articolo 6 bis, paragrafo 1".*

Infine, il medesimo articolo 28-*ter* al paragrafo 3 ha previsto che gli Stati membri debbano assicurano che tutti i fornitori di piattaforme per la condivisione di video sotto la loro giurisdizione applichino misure adeguate per la protezione dei propri utenti, determinate alla luce della natura del contenuto in questione, del danno che possono causare, e che siano praticabili e proporzionate; in particolare ai fini della tutela dei minori ha previsto che i contenuti maggiormente nocivi, diffusi presso una piattaforma per la condivisione di video siano soggetti alle più rigorose misure di controllo dell'accesso. A tal fine, ha previsto alla lettera f) che tali misure consistono, a seconda del caso, nelle attività di "i*stituire e applicare sistemi per verificare l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori".*

Il recente Regolamento (UE) 2022/2065 del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali o anche DSA) ha definito, all'articolo 1, par. 1, lett. i) le piattaforme *online* quali: "*un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento*";

Con tale regolamento la Commissione Europea si è adoperata sul tema, sostenendo e promuovendo l'attuazione di norme mirate alla tutela dei minori online: in particolare, all'art. 28 del *Digital Service Act* richiede che tutti i fornitori di piattaforme on-line accessibili ai minori adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori, anzitutto mediante l'attivazione dei meccanismi di verifica dell'età come di seguito chiarito.

In particolare, il predetto Regolamento all'articolo 35 ha previsto che i fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi debbano adottare misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali. In particolare, al paragrafo 1, lett. j) viene previsto che tali misure possono comprendere, ove opportuno: "*l'adozione di misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi*".

L'adozione del regolamento eIDAS[6] nel 2014 ha consentito l'utilizzo, da parte degli Stati membri, degli schemi nazionali di identificazione elettronica (eID) per accedere ai servizi pubblici *online* a livello transfrontaliero. Con l'evolversi del panorama digitale, sia in riferimento ai servizi del settore pubblico che privato offerti *online*, si è assistito ad una crescente necessità di identificare e autenticare gli utenti con un livello elevato di garanzia. Allo stesso tempo, le minacce alla privacy digitale sono diventate evidenti e sono aumentati i rischi di profilazione e sorveglianza delle persone. Per cui, nel 2021, la Commissione Europea ha proposto una revisione del regolamento originario del 2014, basato sul principio che tutti i cittadini dovrebbero avere la possibilità di controllare la propria identità digitale, attraverso la creazione di un ***portafoglio di identità digitale dell'UE*** (di seguito denominato EUDI wallet). I cittadini dovrebbero essere in grado di portare con sé la propria identità digitale in tutta l'UE, spostandosi senza problemi attraverso i confini senza mai perdere il controllo dei propri dati, con la privacy e la sicurezza al centro del progetto. Il portafoglio sostiene i principi delineati nella Dichiarazione dell'UE sui diritti e principi digitali[7] e contribuisce a raggiungere l'obiettivo del programma politico del decennio digitale[8] di far sì che il 100% dei cittadini dell'UE abbiano accesso all'identità digitale entro il 2030.

Ad **aprile 2024** il Consiglio europeo ha approvato definitivamente la proposta di modifica del regolamento che riguarda l'istituzione di un nuovo quadro per un'identità digitale europea[9]. L'obiettivo è avere a disposizione un sistema di identità digitale riconosciuto in tutta Europa, indipendentemente dallo stato in cui questo sistema viene reso disponibile (quadro armonizzato di identità digitale).

Il Regolamento **dispone che gli Stati membri rilascino un portafoglio europeo di identità digitale**[10] nel quadro di un regime di identificazione elettronica **in linea con norme tecniche comuni**, a seguito di una valutazione obbligatoria della conformità e di una certificazione volontaria nel

[6] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

[7] https://digital-strategy.ec.europa.eu/en/policies/digital-principles

[8] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Regolamento 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[10] Il portafoglio europeo di identità digitale è definito come un prodotto o servizio che consente all'utente di conservare dati di identità, credenziali e attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione, online e offline, per un servizio, conformemente all'articolo 6 bis del regolamento eIDAS, nonché per creare firme elettroniche qualificate e sigilli elettronici qualificati

contesto del quadro europeo di certificazione della cybersicurezza, come stabilito dal regolamento sulla cybersicurezza[11] . Le disposizioni sono volte a garantire che le persone fisiche e giuridiche abbiano la possibilità di richiedere e ottenere, conservare, combinare e utilizzare in maniera sicura i dati di identificazione personale, gli attributi e gli attestati elettronici di attributi per l'autenticazione *online* e *offline* nonché per accedere a beni e a servizi pubblici e privati *online*, con il pieno controllo dell'utente.

Tra le motivazioni, alla base del Regolamento, vi è il fatto che attualmente, nella maggior parte dei casi, i cittadini non possono scambiare digitalmente a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni relative alla loro identità quali indirizzi, età e qualifiche professionali, patenti di guida e altri permessi e dati di pagamento. Pertanto, l'EUDI wallet consentirebbe di superare tali limiti offrendo la possibilità di scambiare attributi minimi dell'identità necessari ad accedere determinati servizi *online* per cui è richiesta l'autenticazione, come ad esempio la prova dell'età. Inoltre, il nuovo Regolamento eIDAS prevede che, **qualora le piattaforme online di dimensioni molto grandi, come definite dal DSA, impongano agli utenti di autenticarsi per accedere ai servizi online, queste dovranno accettare anche l'uso dei portafogli europei di identità digitale, rigorosamente su richiesta volontaria dell'utente, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio *online* per il quale è richiesta l'autenticazione, come la prova dell'età[12].**

In aggiunta, è previsto che gli utenti del EUDI wallet abbiano a disposizione anche la funzionalità gratuita di firma digitale qualificata.

Entro il 2026 ciascuno Stato membro dovrà mettere a disposizione dei cittadini un portafoglio di identità digitale e accettare portafogli europei di identità digitale di altri Stati membri.

La Task force sull'age verification

In data 23 gennaio 2024 è stato avviato il lavoro della ***Task Force on age verification*** con la presentazione, da parte della Commissione, di alcuni studi svolti da esperti del settore.

In primo luogo, sono state fornite alcune definizioni, di seguito richiamate.

Age assurance è il termine generico per i metodi utilizzati per determinare l'età o la fascia di età di un individuo a vari livelli di confidenza o certezza. Le tre categorie principali di metodi di assicurazione dell'età sono la **stima dell'età, la verifica dell'età e l'autodichiarazione**.

Self-declaration si riferisce a quando un utente inserisce una data o seleziona una casella per dichiarare di essere sopra/sotto una determinata età.

Age estimation consiste in metodi che stabiliscono con una certa probabilità che un utente abbia una certa età, rientri in una fascia di età o sia superiore o inferiore a una certa età. I metodi di stima dell'età includono l'analisi automatizzata di dati comportamentali e ambientali, confrontando il modo in cui un utente interagisce con un dispositivo con altri utenti della stessa età, e metriche derivate dall'analisi del movimento o testando le loro capacità o conoscenze.

[11] Consiste nell'insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici

[12] Comma 3 dell'articolo 12-ter introdotto dal Regolamento eIDAS 2.0

Age verification è un sistema che si basa su identificatori rigidi (fisici) e/o fonti di identificazione verificate che forniscono un elevato grado di certezza nel determinare l'età di un utente. Può stabilire l'identità di un utente ma può anche essere utilizzato per stabilire l'età minima.

Tra le varie azioni in relazione all'oggetto di questa consultazione la Commissione intende creare uno standard europeo sulla verifica dell'età online definendo i requisiti per le soluzioni di verifica dell'età per l'industria.

In tale contesto la *Task torce sull' age verification* dovrà discutere e sostenere lo sviluppo di un quadro e di un approccio europeo per la verifica dell'età, oltre a garantire la coerenza e un approccio comune in tutta l'UE.

Uno studio presentato dagli esperti incaricati dalla Commissione riepiloga le metodologie di verifica dell'età rilevate:

- **Autodichiarazione:** gli utenti dichiarano la propria età/fascia di età senza fornire altre prove.
- **Identificatori rigidi:** gli utenti forniscono documenti di identità verificati (ad esempio passaporto) per dimostrare la loro età.
- **Carte di credito:** utilizzo dei dati della carta di credito per verificare che un utente abbia più di 18 anni.
- **Identità basata su blockchain:** utilizzo di tecnologie decentralizzate come blockchain per creare identità digitali degli utenti, per utilizzare tali identità per l'Age Verification.
- **Conferma del titolare del conto:** basarsi sulla conferma di un titolare di conto verificato esistente che un altro utente ha l'età richiesta per utilizzare la piattaforma.
- **Autenticazione multipiattaforma:** utilizzo di account utente già esistenti con piattaforme di grandi dimensioni (ad esempio Google, Apple ecc.) per autenticare l'età di un utente per altri prodotti/ Servizi.
- **Stima del viso:** utilizzo dell'intelligenza artificiale per analizzare le caratteristiche del viso di una persona per stimarne l'età.
- **Profilazione comportamentale:** utilizzo dell'intelligenza artificiale per analizzare l'attività online degli utenti per stimarne l'età.
- **Test di capacità:** testare la capacità o l'attitudine dell'utente per stimare l'età.
- **Servizi di assicurazione sull'età di terze parti:** utilizzo di società terze per i servizi di assicurazione sull'età. Le terze parti potrebbero utilizzare uno qualsiasi degli altri metodi per la garanzia dell'età.

Di seguito i requisiti individuati nello studio:

i. **Proporzionalità e sussidiarietà:**

- Requisito generale che può svolgere un ruolo nel rispetto di altri requisiti.
- Equilibrio tra i mezzi utilizzati per raggiungere l'obiettivo prefissato e il suo impatto sulla limitazione dei diritti delle persone.
- Utilizzo dello strumento meno invasivo per raggiungere l'obiettivo prefissato.

ii. **Privacy:**

- È necessario seguire i principi di protezione dei dati stabiliti dal GDPR (minimizzazione dei dati, accuratezza, limitazione della conservazione, ecc.).
- Elevato livello di tutela della privacy dei minori (OSA).

- La garanzia dell'età può entrare in conflitto con i diritti alla privacy.

iii. **Sicurezza:**

- È necessario attuare misure di sicurezza informatica sufficienti (GDPR, proposta CRA).
- La sofisticazione degli attacchi informatici rende il raggiungimento della cybersicurezza difficile ma anche più importante.

iii. **Precisione ed efficacia:**

- La precisione è importante per garantire la sicurezza dei bambini online.
- Tuttavia, l'accuratezza potrebbe avere una relazione inversa con la privacy.
- La piena precisione è difficile da ottenere ma dovrebbe essere perseguita.

iii. **v. Funzionalità e facilità d'uso:**

- Le tecnologie di assicurazione dell'età dovrebbero essere facili da usare e basate sulle capacità in evoluzione dei bambini.
- La funzionalità può favorire l'adozione da parte degli utenti.
- Tuttavia, la funzionalità potrebbe diluire l'efficacia.

vi. **Inclusività e non discriminazione:**

- La non discriminazione è uno dei quattro principi generali della CRC delle Nazioni Unite.
- Le differenze tra i bambini in termini di lingua, abilità, status socioeconomico, ecc. dovrebbero essere prese in considerazione durante l'assicurazione dell'età.
- La garanzia dell'età potrebbe portare alla discriminazione e all'esclusione in vari modi.

vi. **Promuovere la partecipazione e l'accesso:**

- La verifica dell'età non dovrebbe equivalere a bloccare erroneamente i bambini o a fornire loro servizi inferiori.
- Le tecnologie digitali danno potere ai bambini e la garanzia dell'età non dovrebbe ostacolare questo, ma piuttosto favorirlo.

viii. **Trasparenza e responsabilità:**

- I fornitori di assicurazione sull'età dovrebbero essere trasparenti con gli utenti per quanto riguarda l'assicurazione sull'età impiegata e l'assicurazione sull'età dovrebbe essere comprensibile ai bambini.
- Le piattaforme devono essere responsabili dell'implementazione della garanzia dell'età.

viii. **Meccanismi di notifica, contestazione e riparazione:**

- Dovrebbe essere seguito il giusto processo per le decisioni relative alla garanzia dell'età.
- È necessario che vi siano vie di comunicazione per notificare, contestare e cercare riparazione contro decisioni errate di Assurance.

viii. **Ascoltare le opinioni dei minori:**

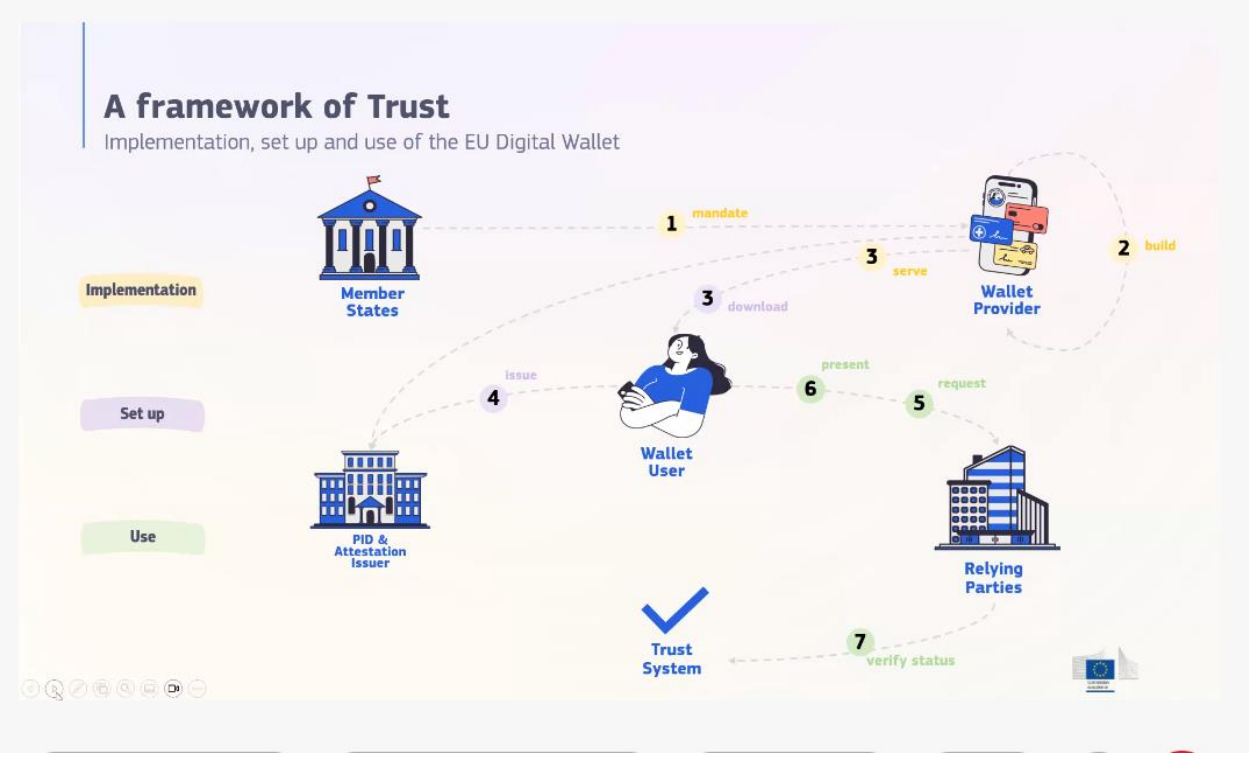
- Secondo la CRC delle Nazioni Unite, i minori hanno il diritto di essere ascoltati.

- Le piattaforme dovrebbero impegnarsi e prestare attenzione alle opinioni dei bambini riguardo alla garanzia dell'età.

Nell'ambito dei lavori del 18 marzo 2024, i rappresentanti della Commissione Europea hanno illustrato il progetto di implementazione del EUDI wallet[13] che ha l'obiettivo di definire un *framework* di regole e specifiche comuni a tutti gli stati membri, per la creazione di portafogli di gestione dell'identità digitale. I cittadini, i residenti e le imprese europee potranno utilizzare l'APP del wallet per ottenere, archiviare e condividere in modo sicuro importanti documenti digitali e avranno la possibilità di dimostrare facilmente chi sono quando accedono ai servizi digitali *online*.

I presupposti alla base del progetto sono di **mantenere nascosta l'identità dell'utente quando viene richiesta una prova della sua età, e che eventuali terze parti coinvolte nel processo di prova dell'età non siano a conoscenza dell'utilizzo che l'utente farà della certificazione**.

Il processo previsto dalla Commissione per l'implementazione, il set-up e l'utilizzo del EUDI wallet segue lo schema di seguito riportato.



Inizialmente gli Stati membri conferiscono mandato (step 1 e step 2) ai fornitori (*wallet provider*) di implementare portafogli di identità digitale nel rispetto del *framework* definito dal Regolamento, sviluppando, ad esempio, un'APP wallet scaricabile dagli utenti sui propri dispositivi mobili.

Mediante l'APP del portafoglio di identità digitale, l'utente potrà conservare e gestire la sua identità digitale, nonché eventuali attributi (es. età, nazionalità, genere etc..) e attestazioni (es. prova dell'età, patente di guida, certificati di studi, etc..) validate da appositi emittenti (*PID & Attestation*

[13] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/

issuer, step 3 e step 4) che interagiscono con i provider del *digital wallet*. Gli utenti potranno quindi utilizzare il portafoglio di identità digitale per identificarsi e autenticarsi *online* quando richiesto da enti pubblici/privati per accedere ai propri servizi (*relying parties*, step 6 e 5).

Per quanto riguarda la verifica dell'età mediante il portafoglio di identità digitale, la Commissione ha descritto **i requisiti chiave alla base del progetto**:

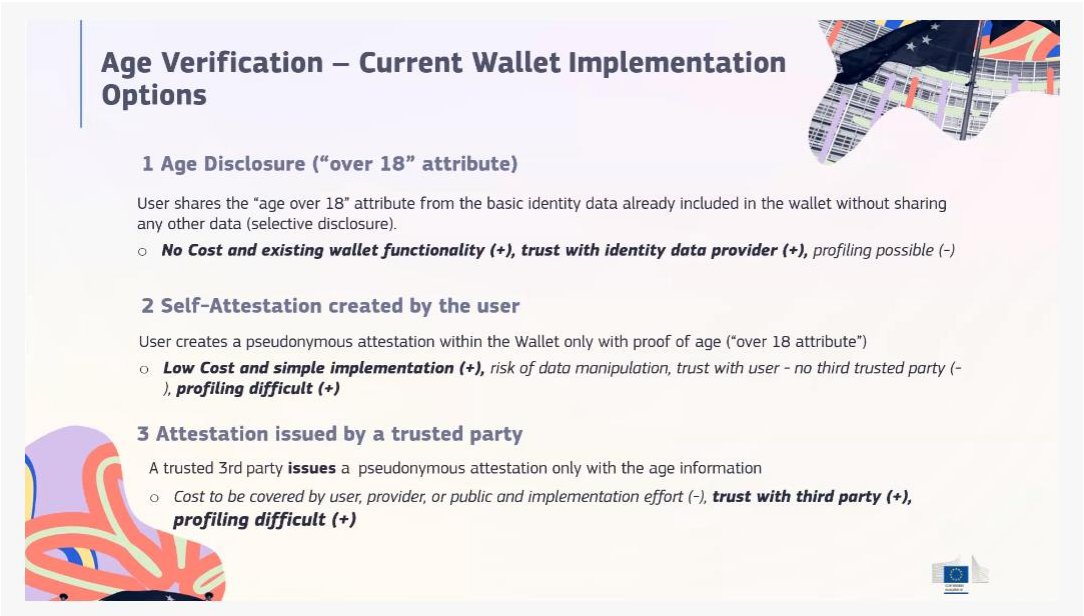
- Fornire una prova dell'età (+18) *online* quando richiesto da un service provider/piattaforma;
- **La prova dell'età non deve divulgare alcuna informazione personale dell'utente**;
- **La prova dell'età non deve divulgare nessuna informazione sul processo di verifica dell'età a nessuna delle terze parti coinvolte nel processo**;

Per quanto riguarda i meccanismi di verifica dell'età, la Commissione ha proposto quattro scenari di processi che saranno resi disponibili agli utenti utilizzando l'EUDI wallet. **I presupposti sono di mantenere nascosta l'identità dell'utente quando viene richiesta una prova della sua età, e che eventuali terze parti coinvolte nel processo di prova dell'età non siano a conoscenza dell'utilizzo che l'utente farà della certificazione**.

Il primo scenario (*Age Disclosure – over 18 attribute*) consiste nella possibilità, da parte dell'utente, di condividere l'attributo "maggiorenne" partendo dalle informazioni base sulla sua identità, che sono memorizzate nel *digital wallet*, senza fornire alcun dato personale al provider che richiede la prova dell'età.

Il secondo scenario (*self-attestation created by user*) prevede la creazione di una attestazione pseudonima, da parte dell'utente, direttamente all'interno del *digital wallet*, che includa la sola informazione della "maggiore età" dell'utente. Tale attestazione potrà essere inviata al provider che richiede la prova dell'età.

Il terzo scenario (*Attestation issued by a trusted 3rd party*) prevede la generazione di una attestazione pseudonima da parte di un soggetto terzo certificato, che contiene solo l'informazione della maggiore età dell'utente.



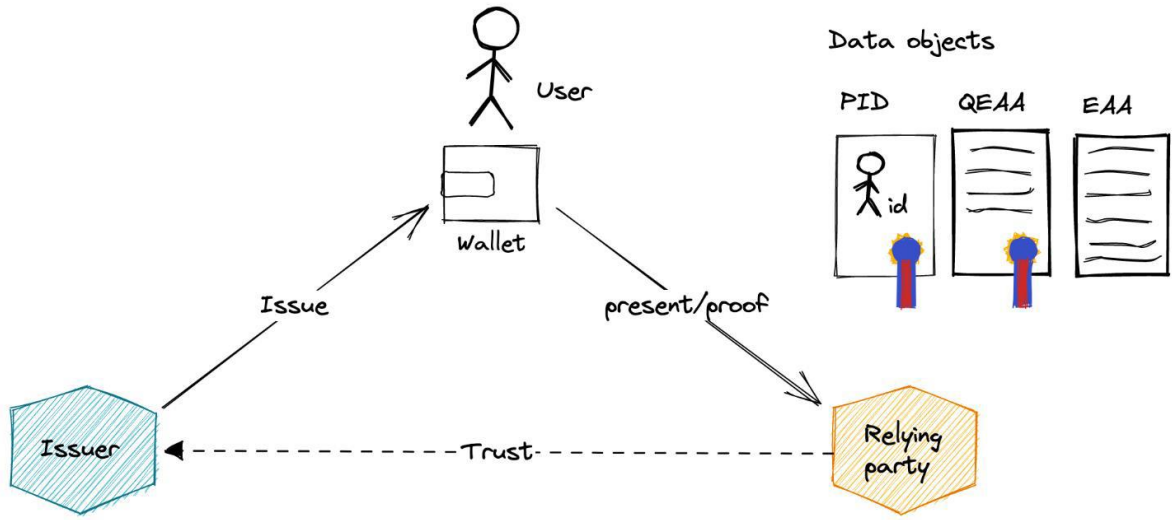
Un quarto scenario (*Age disclosure using zero knowledge proof protocols*), la cui implementazione è prevista in futuro, prevede l'utilizzo di **protocolli di crittografia** di tipo "zero-knowledge" con cui l'utente può generare attestazioni della maggiore età senza condividere nessun'altra informazione personale ed evitando in ogni caso la profilazione da parte dei provider che richiedono la prova dell'età e di altri soggetti terzi coinvolti nel processo.

La Commissione ha realizzato una versione pilota del *digital wallet* che sarà sottoposta ad una prima fase di test con il coinvolgimento degli stati membri volontari. Durante questa fase (trattasi di *POC - Proof of Concept),* verranno recepite eventuali osservazioni e suggerimenti, da parte degli stati membri, sui meccanismi di verifica della maggiore età implementati tramite il *wallet*.

La Commissione procederà poi, nel corso della seconda metà del 2024, ad avviare il progetto pilota su larga scala a livello europeo con l'obiettivo di **rendere disponibile il portafoglio di identità digitale agli utenti a partire dal 2026**.

Nell'ambito dei lavori del 23 aprile 2024, finalizzati a dare avvio alle attività di PoC con la partecipazione attiva degli Stati membri, la Commissione ha fornito ulteriori dettagli sui meccanismi che saranno implementati per la verifica dell'età attraverso il portafoglio europeo di identità digitale.

Nello schema seguente vengono riportate le diverse entità che interagiscono nel processo di richiesta, certificazione e verifica, ossia lo *user* che utilizza il portafoglio digitale, l'*issuer* che fornisce la prova dell'età e il *relying party* a cui l'utente presenta la prova dell'età.



Come rappresentato in figura, gli oggetti gestiti dal portafoglio di identità digitale sono il *Personal Identification (PID), l'Electronic Attestation of Attributes (EAA) e il Qualified Electronic Attestation of attributes (QEAA):*

1. **PID (Personal Identification):** trattasi di un insieme di dati che vengono rilasciati ai sensi di regolamenti dell'Unione o di leggi nazionali e che consentono di stabilire l'identità di una persona fisica. Il PID include sia informazioni obbligatorie (nome, nome veloce, data di nascita,) che facoltative ("Età in anni, Cognome di nascita, indirizzo di residenza, Paese di residenza, nazionalità");
2. **EAA (electronic attestation of attributes):** consiste in un'attestazione in formato elettronico che consente l'autenticazione di particolari attributi[14] (es. "maggiore età");
3. **QEAA (qualified electronic attestation of attributes):** attestato in formato elettronico rilasciato da un prestatore di servizi fiduciari (qualificato) come ad esempio la patente di guida, la maggiore età, etc..

Come stabilito dalla Commissione le attività del PoC si concentreranno sui due scenari di seguito riportati:

- **<u>Scenario 1 - divulgazione dell'età (attributo "aver 18 anni")</u>**

L'utente condivide l'attributo "age over 18" dai dati di identità di base già inclusi nel portafoglio senza condividere altri dati (divulgazione selettiva). In questo caso il sito/piattaforma richiede all'utente di verificare la sua età fornendo allo stesso un QRCODE. L'utente, inquadrando il QRCODE mediante l'APP del portafoglio digitale, riceve la richiesta di presentazione delle informazioni contenute nel PID (es. attributo della "maggiore età") e consente a condividere le informazioni richieste. Il sito/piattaforma riceve così le informazioni sulla maggiore età dal portafoglio digitale.

- **<u>Scenario 2 - attestazione (pseudonimo) rilasciata da un soggetto di fiducia</u>**

[14] L' "attributo" è definito come una prerogativa, una caratteristica o una qualità di una persona fisica o giuridica o di un'entità, in forma elettronica

Una terza parte fidata rilascia un'attestazione pseudonima[15] che contiene solo le informazioni sull'età. In questo caso l'utente richiede ad un ente certificatore di emettere un'attestazione certificata di maggiore età. L'ente certificatore richiede all'utente di condividere le informazioni del PID al fine di rilasciare un'attestazione pseudonima di maggiore età. Il sito/piattaforma richiede all'utente di verificare la sua età fornendo un QRCODE. L'utente, inquadrando il QRCODE mediante l'APP del portafoglio digitale, riceve la richiesta di presentazione dell'attestazione pseudonima di maggiore età e consente a condividere le informazioni richieste. Il sito/piattaforma riceve così le informazioni sulla maggiore età dal portafoglio digitale.

Il working group n.6 "protection of minors"

A luglio 2024 il DSA board ha definito la struttura dei gruppi di lavoro tecnici incaricati di sviluppare le varie attività previste da DSA nel corso del 2025. Tra questi, è stato istituito il working group n.6 "*protection of minors*" (di seguito WP6) cui l'Autorità partecipa attivamente con i propri esperti designati.

Il WP6 si occupa, tra gli altri, di definire le specifiche tecniche della soluzione per l'*age verification* che verrà implementata dal fornitore selezionato dalla Commissione europea nell'ambito della gara d'appalto avviata il 15 ottobre 2024, e avente ad oggetto lo sviluppo di una soluzione europea per la verifica dell'età[16]. Il progetto prevede la realizzazione di una "white label APP[17]" sulla base delle specifiche stabilite dal gruppo, che verrà messa a disposizione degli stati membri nel corso del primo quadrimestre del 2025, al fine di garantire la disponibilità di una soluzione europea , nelle more del completamento delle attività di sviluppo del portafoglio europeo di identità digitale (EUDI Wallet) previsto per fine 2026.

Inoltre, il WP6 si occupa di definire le linee guida relative all'articolo 28 del DSA al fine di assistere i fornitori di piattaforme online accessibili ai minori nell'applicazione di misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio.

IV. Le iniziative in ambito di standardizzazione e regolamentare

In ambito europeo o, in generale, internazionale sono state attuate o risultano tutt'ora in corso di elaborazione numerose iniziative di cui è fornita una panoramica nell'**Allegato 1** al presente documento a cui si rinvia.

[15] Con il termine "pseudonimo" si intende un identificativo che rappresenta univocamente un utente e che al suo interno non contiene nessun riferimento, dato o informazione circa attributi propri all'utente o suoi dati personali.
[16] La Commissione europea ha selezionato i fornitori Deutsche Telekom AG e Scytáles AB a conclusione della gara d'appalto pubblicata al seguente link https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/ae950883-112f-4139-989e-1c8d794bb77a-CN
[17] Un software di tipo "white label" è un software generico realizzato per poter essere poi personalizzato, configurato e distribuito da altri distributori, consentendo di sovrapporre il proprio marchio, identità o altre caratteristiche.

ALLEGATO 1

I. Le iniziative in ambito di standardizzazione e regolamentare

In ambito europeo o, in generale, internazionale sono state attuate o in corso numerose iniziative di cui è fornita una panoramica in Allegato 1 al presente documento a cui si rinvia.

I.1 Il progetto euConsent

Trattasi di un progetto europeo, cofinanziato dall'UE, che si occupa di costruire un metodo di verifica dell'età (*age assurance*) interoperabile, basato sui browser.

Nell'ambito delle attività del progetto euCONSENT è stato pubblicato un documento, ancora in versione draft, denominato "ISO Working Draft Age Assurance Systems Standard".

Si riportano alcuni elementi del documento che si ritengono utili ai fini della predisposizione di specifiche tecniche sui processi di verifica dell'età.

Caratterizzazione dei sistemi di verifica dell'età

Nel citato documento, per sistema di "assicurazione" (o garanzia di età) dell'età - *age assurance* – si intende un processo di determinazione e comunicazione dell'età di un individuo. La verifica dell'età può essere condotta tramite uno o più processi di verifica degli *attributi di identità* che non richiedono necessariamente una verifica completa dell'identità e possono operare su un modello federato.

La garanzia dell'età può applicarsi a età specifiche o a fasce di età (classificazione in base all'età). In base al documento **un sistema di age assurance** è composto da:

(a) Uno o più **componenti di verifica** che indicano l'età di una persona,

(b) Un **sottosistema di elaborazione** che analizza il *livello di confidenza* che può essere applicato alle *componenti di verifica* dell'età (il grado in cui un *attributo di età* può essere considerato affidabile; l'affidabilità è di seguito classificata nei livelli "zero", "base", "standard", "potenziato" o "rigoroso" in conformità con determinati standard ISO), e lo comunica a una parte che fa affidamento su tale verifica (nel caso in cui il fornitore del sito sia differente dal soggetto che svolge la verifica dell'età). Per *attributo di età* si intende la caratteristica o proprietà di una entità, nel caso di specie l'età (ad esempio superiore a 18 anni). Per *attributo* si intende la caratteristica o proprietà di una entità, nel caso di specie l'età (ad esempio maggiore di anni 18).

Le ***componenti di verifica*** dell'età di un individuo possono includere:

(a) Un processo o sistema che ottiene un *attributo di età* da un documento (es. passaporto),

(b) Un processo o sistema che deriva un *attributo di età* da altre *credenziali primarie o secondarie* (si veda la successiva spiegazione),

(c) Un processo o sistema che utilizza l'*intelligenza artificiale* (branca dell'informatica dedicata allo sviluppo di sistemi di elaborazione dati che svolgono funzioni normalmente associate all'intelligenza umana, come il ragionamento, l'apprendimento e l'auto-miglioramento) per accertare l'età da uno o più identificatori biometrici, da comportamenti, caratteristiche o azioni di individui,

(d) Un processo o sistema che implementa una ***prova sociale*** (social *proofing*: analisi, con il consenso dell'utente, della sua impronta digitale – digital footprint - e dei relativi grafici sociali –

social graphs -, che possono essere interrogati per valutare la veridicità di un'auto asserita garanzia di età,) per ottenere o verificare gli attributi di età,

(e) Un processo o sistema basato sull'attestazione di parti fidate (come genitori o tutori legali),

(f) Una valutazione, di persona o online, condotta da una persona qualificata che valuta elementi che tengono conto dell'aspetto, del comportamento, del background e della credibilità di una persona,

(g) Un processo o sistema che ricava attributi di età da qualsiasi altro metodo in grado di stabilire *livelli di confidenza* come descritto nel presente documento.

Un ***sottosistema di elaborazione*** della garanzia dell'età può includere:

(a) Un processo o sistema per riunire *componenti di verifica* provenienti da più fonti,

(b) Un processo o sistema per identificare eventuali attacchi da parte di malintenzionati, proteggere da attacchi di presentazione - *presentation attacks* - , e valutare la "vitalità" – liveness - degli individui,

(c) Un processo o sistema per identificare e affrontare i *controindicatori* (prove o informazioni che mettono in dubbio o indicano in altro modo che l'età dichiarata potrebbe non essere quella reale),

(d) Un processo o sistema per aumentare la fiducia (trust, grado in cui un'entità ha fiducia nell'accuratezza e nell'affidabilità dei processi di verifica dell'età) in un *attributo di età* attraverso più fonti,

(e) Possibilità per gli individui di esercitare i diritti sui propri dati (data rights),

(f) Un processo o sistema per la trasmissione degli attributi relativi all'età, a un livello dichiarato di garanzia dell'età, alle parti che fanno affidamento,

(g) Un processo o sistema per il monitoraggio, il miglioramento continuo e l'apprendimento dalle attività di verifica dell'età.

Credenziali primarie e secondarie

I sistemi di verifica dell'età dovrebbero prestare particolare attenzione alla differenza tra credenziali primarie e secondarie.

Una **credenziale primaria** è uno strumento, documento o registrazione rilasciata un soggetto autorevole e utilizzato da un individuo per fornire prova dell'età. Il soggetto autorevole può essere un ente pubblico o di un ente privato istituito a tal fine. Va considerato il rischio intrinseco che la credenziale primaria possa essere stata rilasciata in modo inappropriato, alla persona sbagliata, con dati errati o possa essere stata oggetto di falsificazione.

Una **credenziale secondaria** è un attributo relativo a un individuo derivato da una credenziale primaria. Ad esempio, la creazione di una registrazione nel sistema bancario dei dati relativi alla persona fisica costituisce la creazione di una credenziale secondaria. La banca apre il conto a seguito dell'acquisizione di dati dal passaporto di un individuo. L'esame da parte della banca di tale passaporto è l'esame di una credenziale primaria.

I sistemi di garanzia dell'età possono fare affidamento sia su credenziali primarie che secondarie, ma devono adottare ulteriori approcci valutati in termini di rischio per la gestione delle credenziali secondarie, compresa la capacità di errori nell'acquisizione dei dati e i vincoli, la supervisione normativa e l'affidabilità del produttore delle credenziali secondarie.

Controindicatori

I sistemi di verifica dell'età possono implementare più componenti di verifica e possono avere più fonti di informazioni provenienti da credenziali sia primarie che secondarie. Ciò potrebbe portare a errate corrispondenze di dati o informazioni che indicano che l'età dichiarata potrebbe non corrispondere all'età reale. Questi sono chiamati controindicatori.

I fornitori di sistemi di assicurazione dell'età hanno due opzioni quando si presentano con un controindicatore:

(a) Agire per risolvere il controindicatore raccogliendo ulteriori prove a sostegno dell'età dichiarata; O

(b) Comunicare l'esistenza del controindicatore a ciascuna parte facente affidamento.

Classificazione dei livelli di garanzia dell'età

Il livello di confidenza associato a un attributo di età può essere determinato dal processo utilizzato per acquisire, convalidare e verificare l'età dichiarata nel sistema di verifica dell'età. Il livello di confidenza può essere stabilito dal regolatore in funzione del bene tutelato, nel caso di specie, la salute del minore. Di seguito i cinque *livelli di confidenza* descritti nel citato documento.

1. Livello di Garanzia Zero della verifica dell'età

Tale livello corrisponde ai processi basati sull'età dichiarata dall'individuo mediante autodichiarazione e senza l'applicazione delle componenti di verifica età. Non viene effettuato alcun tentativo di convalidare l'attributo di età rivendicato.

La modifica nel tempo del valore di età dichiarato rappresenta un cosiddetto controindicatore.

2. Livello di Garanzia Base della verifica dell'età

All'acquisizione dell'età dichiarata dall'individuo si aggiunge l'applicazione di almeno un componente di verifica dell'età testato al livello di garanzia della valutazione 1 (EAL1, nel documento draft sono previsti sette livelli di garanzia della valutazione - da EAL1 a EAL7 - che corrispondono ai crescenti sforzi per la verifica e il test della progettazione).

Il sistema acquisisce la dichiarazione dell'età facendo riferimento a domande poste all'individuo, invitando l'utente a presentare prove a supporto di un componente del processo di garanzia dell'età.

Il componente del processo di garanzia dell'età può includere la semplice convalida dell'attributo di età dichiarato. Il processo non deve comportare un tasso di **false accettazioni o di falsi rifiuti superiore al 5%.**

Il livello base prevede sistemi per ridurre i tentativi di elusione (attack vector) da parte di bot o processi automatizzati o da autodichiarazioni false o inesatte, oltre a tecniche per stabilire la vitalità (liveness) di un individuo. Tali tentativi dovrebbero essere supportati da metodi volti a ridurre o eliminare i pregiudizi sistemici (systemic bias) nel processo di verifica dell'età. Una garanzia sull'età di base può lasciare controindicatori irrisolti, che dovrebbero essere comunicati alla parte che fa affidamento sulla verifica.

L'autenticazione deve essere rinnovata almeno ogni 3 mesi.

3. Livello di Garanzia Standard della verifica dell'età

All'acquisizione dell'età dichiarata dall'individuo si aggiunge l'applicazione di almeno un componente della garanzia dell'età testato al livello di garanzia della valutazione 2 (EAL2).

Il sistema acquisisce la dichiarazione dell'età, facendo riferimento a domande poste all'individuo, invitando l'utente a presentare prove a supporto di un componente del processo di garanzia dell'età.

Il processo della componente di garanzia dell'età deve includere la convalida dell'attributo di età dichiarato. Il processo non deve comportare un tasso di false accettazioni o di falsi rifiuti superiore all'1%.

Se il processo viene intrapreso da remoto, dovrà essere necessario stabilire la vitalità (liveness) dell'individuo in conformità alla norma ISO/IEC 30107. Il tasso di mancata acquisizione dovrà essere inferiore all'1%.

Se il processo prevede l'impiego dell'intelligenza artificiale, l'errore di classificazione o l'errore di parità statistica dovuto alle caratteristiche peculiari degli individui, non deve superare una varianza del 3%.

Il processo comprende meccanismi volti a scoraggiare la presentazione di autodichiarazioni false o inesatte. Il sistema deve prevenire gli attacchi da parte di bot o processi automatizzati e riconoscere autodichiarazioni false o inesatte. Ciò include la verifica della liveness di un individuo. Tali contromisure devono essere basate su metodi volti a ridurre o eliminare i pregiudizi sistemici nel processo di verifica dell'età.

Tutti i controindicatori identificati devono essere risolti o comunicati alla componente facente affidamento.

L'autenticazione dovrebbe essere rinnovata almeno ogni mese.

4. Livello di Garanzia Rafforzata della verifica dell'età

In questo caso all'età dichiarata (autodichiarazione implicita o effettiva) vanno aggiunte almeno altre due componenti di garanzia dell'età provenienti da due fonti indipendenti (una delle quali deve essere una credenziale primaria o secondaria).

I componenti della garanzia dell'età devono essere testati fino al livello di garanzia della valutazione 3 (EAL3).

I processi relativi alla componente di garanzia dell'età devono includere la convalida dell'attributo di età dichiarato. Il processo non deve comportare un tasso di false accettazioni o di falsi rifiuti superiore allo 0,1%.

Se il processo di verifica dell'età avviene online, dovrà essere necessario stabilire la vitalità dell'individuo in conformità alla norma ISO/IEC 30107. Il tasso di mancata acquisizione dovrà essere inferiore all'1%. Se il processo prevede l'impiego dell'intelligenza artificiale, la parità di errore di classificazione o di risultato per le caratteristiche protette degli individui non deve superare una varianza del 3%.

Il processo comprende meccanismi volti a scoraggiare la presentazione di autodichiarazioni false o inesatte. Tutti i controindicatori identificati devono essere risolti o comunicati alla componente facente affidamento. L'autenticazione dovrebbe essere rinnovata almeno ogni settimana.

5. Livello di Garanzia Rigoroso della verifica di età

All'autodichiarazione implicita o effettiva si somma la verifica di almeno altri due componenti dell'assicurazione dell'età provenienti da due fonti indipendenti (una delle quali deve essere una credenziale primaria) per convalidare l'età dichiarata.

I componenti della garanzia dell'età devono essere testati fino al livello di garanzia della valutazione 4 (EAL4). L'asserzione sull'età può essere acquisita in un processo di acquisizione dei dati invitando l'utente a presentare prove a supporto dei processi dei componenti di garanzia dell'età.

I processi relativi alla componente di garanzia dell'età devono includere la convalida dell'attributo di età dichiarato. Il processo non deve comportare un tasso di false accettazioni o di falsi rifiuti superiore allo 0,01%. Se il processo viene intrapreso in remoto, dovrà essere necessario stabilire la vitalità dell'individuo in conformità alla norma ISO/IEC 30107. Il tasso di mancata acquisizione dovrà essere inferiore all'1%.

Se il processo prevede l'impiego dell'intelligenza artificiale, la parità di errore di classificazione o di risultato per le caratteristiche protette degli individui non deve superare una varianza del 3%. Il processo comprende meccanismi volti a scoraggiare la presentazione di autodichiarazioni false o inesatte. Tutti i controindicatori identificati devono essere risolti o comunicati alla componente facente affidamento. La verifica dell'età dovrebbe essere ripetuta ad ogni decisione di ammissibilità legata all'età, ripetendo il processo di garanzia dell'età.

Il tema della sicurezza: attacchi informatici, tentativi di elusione del processo di verifica e controindicatori

Tutti i processi sono più o meno vulnerabili agli attacchi informatici o a tentativi di elusione del sistema di verifica da parte dei minori stessi. I sistemi di verifica dell'età dovrebbero identificare i possibili elementi di vulnerabilità del processo, come:

(a) L'accuratezza, l'affidabilità, il rischio di frode della fonte dei dati, inclusa la considerazione dei rischi associati alla deduzione o alla derivazione di dati da altre fonti utilizzate per altri scopi;

(b) La possibilità di un attacco al sistema;

(c) La possibilità per un individuo di eludere il sistema;

(d) La possibilità di una collusione o complicità tra le parti (anche tra i minorenni e maggiorenni);

Per la verifica dell'età online, gli sviluppatori di sistema dovrebbero valutare il rischio che un processo non umano possa essere utilizzato per un attacco a livello di sistema. Diventa importante, pertanto, un sistema di rilevamento della cosiddetta liveness, come definita dalla norma ISO/IEC 30107.

Altre tipologie di attacco, cosiddette *Attacco di presentazione*, possono verificarsi:

(a) mediante acquisizione di dati biometrici direttamente da una persona, online o tramite database esistenti, utilizzandoli per la presentazione di uno spoofing biometrico (ad esempio l'immagine del

volto o il video di una persona su un tablet o un'impronta digitale falsa in silicone o gelatina) a un sensore biometrico;

(b) Un altro esempio di attacco di presentazione si può avere con riferimento a un documento falsificato (ad esempio una patente di guida falsa, un passaporto falsificato o una registrazione falsificata in una banca dati).

L'affidabilità del sistema di verifica dell'età va valutata rispetto a tale tipologia di attacco.

I.2 La consultazione pubblica del regolatore inglese OFCOM

Il 5 dicembre 2023 Ofcom ha avviato una consultazione pubblica su un documento di linee guida su controlli dell'età "altamente efficaci" che dovranno essere implementati dai fornitori di servizi online per impedire ai minori di accedere ai servizi porno online.

Tra i metodi di verifica dell'età presi in considerazione da OFCOM sono inclusi la verifica della corrispondenza dei documenti d'identità con foto, la stima dell'età mediante riconoscimento facciale e l'utilizzo delle carte di credito.

I fornitori di servizi sono tenuti a salvaguardare la privacy degli utenti e il diritto degli adulti di accedere alla pornografia legale.

Nel documento pubblicato si riporta che le ultime ricerche mostrano che l'età media in cui i minori hanno accesso per la prima volta alla pornografia online è 13 anni, anche se quasi un quarto all'età di 11 anni (27%) e uno su dieci a 9 anni (10%). Inoltre, quasi 8 giovani su 10 (79%) hanno avuto accesso alla pornografia violenta che raffigurava atti sessuali coercitivi, degradanti o che inducono dolore prima di compiere 18 anni.

L'Online Safety Act prevede che i siti e le app che visualizzano o pubblicano contenuti pornografici devono garantire che i minori non siano normalmente in grado di accedere a materiale pornografico sui loro servizi.

A tal fine sono tenuti a introdurre un sistema per la "garanzia dell'età" – attraverso la verifica dell'età, la stima dell'età o una combinazione di entrambi – che sia "altamente efficace" nel determinare correttamente se un utente è un bambino o meno**.**

Metodi altamente efficaci per la garanzia dell'età

In base alla citata legge OFCOM è stata incaricata di adottare delle linee guida per supportare i fornitori di servizi di pornografia online ad adempiere alle proprie responsabilità legali e di vigilare sull'implementazione. Lo schema di linee guida stabilisce criteri i controlli sull'età devono soddisfare per essere considerati altamente efficaci; i criteri si rifanno ai principi di accuratezza tecnica, robustezza, affidabilità ed equità.

Resta ferma la salvaguardia del diritto alla privacy e, per gli adulti, ad accedere alla pornografia legale.

Considerato che è probabile che la tecnologia alla base della verifica dell'età si svilupperà e migliorerà in futuro, le linee guida includono un elenco non esaustivo di metodi che attualmente OFCOM ritiene che potrebbero essere altamente efficaci. Questi includono:

- **Attività bancarie**. Un utente può acconsentire alla condivisione delle informazioni bancarie confermando di avere più di 18 anni con il servizio di pornografia online. La loro data di nascita completa non è condivisa.

- **Corrispondenza dell'identificazione con foto**. Gli utenti possono caricare un documento d'identità con foto, come una patente di guida o un passaporto, che viene poi confrontato con un'immagine dell'utente al momento del caricamento per verificare che si tratti della stessa persona.
- **Stima dell'età del viso**. Le caratteristiche del volto di un utente vengono analizzate per stimarne l'età.
- **Controllo dell'età dell'operatore di rete mobile**. Alcuni operatori di telefonia mobile del Regno Unito applicano automaticamente una restrizione che impedisce ai bambini di accedere a siti Web soggetti a limiti di età. Gli utenti possono rimuovere questa restrizione dimostrando al proprio operatore di telefonia mobile di essere maggiorenni e questa conferma verrà quindi condivisa con il servizio di pornografia online.
- **Controlli sulle carte di credito**. Nel Regno Unito, gli emittenti di carte di credito sono obbligati a verificare che i richiedenti abbiano più di 18 anni prima di fornire loro una carta di credito. Un utente può fornire i dettagli della propria carta di credito al servizio di pornografia online, dopodiché un processore di pagamento invia una richiesta per verificare la validità della carta alla banca emittente. L'approvazione da parte della banca può essere considerata come prova che l'utente ha più di 18 anni.
- **Portafogli di identità digitale**. Utilizzando una varietà di metodi, inclusi quelli sopra elencati, gli utenti possono archiviare in modo sicuro la propria età in un formato digitale, che l'utente può quindi condividere con il servizio di pornografia online.

Nelle Linee guida OFCOM riporta esempi di approcci alla garanzia dell'età che non soddisfano gli standard stabiliti nella bozza di linee guida. I metodi non affidabili includono:

- autodichiarazione dell'età;
- metodi di pagamento online che non richiedono che una persona abbia 18 anni (carte di debito, Solo o Electron); E
- termini generali, esclusioni di responsabilità o avvertenze.

I servizi non dovrebbero ospitare o consentire contenuti che indirizzino o incoraggino i minori a tentare di eludere i controlli sull'età e sull'accesso.

I. Introduzione alle Linee Guida sugli obblighi di verifica dell'età.

Le Linee guida OFCOM sugli obblighi di verifica dell'età sono funzionali a fare in modo che i fornitori di servizi regolamentati adottino le opportune misure, sui propri sistemi, funzionali a garantire che i minori non siano normalmente in grado di accedere a contenuti pornografici, implementando un processo di verifica dell'età (il termine verifica età va inteso in senso generale e dipende dalla metodologia utilizzata. In alcuni casi la verifica dell'età avviene mediante una stima della stessa. In altri casi mediante una verifica indiretta di credenziali fornite da altri enti, ecc.)

In generale le Linee guida forniscono delle indicazioni sui:

- tipi di sistemi di verifica sull'età che possono ritenersi efficaci e quelli che non lo sono;
- criteri di cui i fornitori di servizi devono tener conto quando progettano o implementano un sistema di verifica dell'età per garantire che sia efficace;
- principi che i fornitori di servizi dovrebbero considerare per garantire che il processo di verifica dell'età sia di facile utilizzo e non impedisca indebitamente agli adulti di accedere a contenuti legali;
- esempi in cui è probabile ritenere che un fornitore di servizi non abbia rispettato gli obblighi di verifica dell'età.

Nel seguito si intenderà per:

• **metodo di verifica dell'età,** il particolare sistema o tecnologia che è alla base di un processo di verifica dell'età; E

• **processo di verifica dell'età,** il processo end-to-end attraverso il quale vengono implementati un metodo di verifica dell'età o una combinazione di metodi per determinare se un utente è o meno un minore.

Indicazioni generali sui tipi di sistemi di verifica dell'età che possono considerarsi efficaci

Gli obblighi di verifica dell'età impongono ai fornitori di servizi di garantire che i minorenni non siano normalmente in grado di accedere a contenuti pornografici, implementando un processo di verifica dell'età che sia efficace nel determinare correttamente se un utente è o meno un minore.

Ciò significa che i fornitori devono implementare controlli di accesso al loro servizio regolamentato in modo che agli utenti che sono stati identificati come minorenni dal processo di verifica dell'età sia poi impedito di accedere a contenuti pornografici (ad esempio negando l'accesso a ulteriori sezioni del servizio). I fornitori di servizi non devono ospitare o consentire contenuti sui loro servizi che indirizzino o incoraggino gli utenti minorenni a eludere il processo di verifica dell'età o i controlli di accesso, ad esempio fornendo informazioni o collegamenti a una rete privata virtuale (VPN).

In linea generale un processo di verifica dell'età può considerarsi efficace se risulta:

• Tecnicamente accurato

• Robusto

• Affidabile

• equo

Esempi di metodi di assicurazione dell'età che secondo OFCOM potrebbero essere molto efficaci sono:

 Open banking

 Abbinamento foto-tessera

 Stima dell'età mediante riconoscimento facciale

 Controlli sull'età degli MNO

 Carte di credito

 Portafogli di identità digitale

 Altri metodi che soddisfano ciascuno dei criteri previsti dalle Linee guida

Esempi di metodi di assicurazione dell'età che non sono in grado di essere efficaci

 Autodichiarazione

 Carte di debito, Solo o Electron

 Altri metodi di pagamento che non richiedono che l'utente abbia più di 18 anni

 Restrizioni contrattuali generali sulla fruizione del servizio da parte dei bambini

Ulteriori caratteristiche di un processo di verifica dell'età sono:

• Accessibilità

• Interoperabilità

OFCOM prende atto del fatto che esiste una vasta gamma di metodi di verifica dell'età che un fornitore di servizi può implementare. Alcuni possono essere sviluppati internamente dal fornitore di servizi; altri possono essere forniti da fornitori di terze parti. Questi metodi funzionano in modi diversi ed è probabile che la tecnologia alla base di essi continui a migliorare nel tempo. Si rileva inoltre che è probabile che in futuro emergano nuovi approcci alla verifica dell'età.

Per tale ragione OFCOM ha adottato un approccio alle Linee guida che non è mirato a fornire un elenco esaustivo di tipi di processi di verifica dell'età che potrebbero essere efficaci nel determinare correttamente se un utente è o meno minorenne. Fornisce, ad ogni modo, degli esempi. Ciò ha lo scopo di garantire, per quanto possibile, che le Linee guida siano a prova di futuro e neutrali dal punto di vista tecnologico.

Tra gli esempi di sistemi di verifica dell'età che possono essere considerati efficaci ve ne sono alcuni consolidati, come la corrispondenza della foto-identificazione (foto-identità), e metodi più innovativi come la stima dell'età del volto.

Spetta a ciascun fornitore di servizi determinare quale tipo di metodo di verifica sull'età è più appropriato per soddisfare i propri obblighi ai sensi della legge e delle presenti Linee guida.

OFCOM è consapevole del fatto che tutti i metodi di verifica dell'età comportano il trattamento di dati personali e, come tali, sono soggetti ai previsti obblighi di legge a cui si rinvia.

Descrizione dei criteri per garantire che il sistema di verifica dell'età sia efficace

OFCOM ha ritenuto ritiene opportuno, in linea con quanto sopra, fornire dei criteri generali che consentano di valutare se un determinato processo possa essere considerato efficace rispetto all'obbiettivo di una verifica dell'età che sia per quanto possibile certa. I criteri che si propongono, e che devono essere soddisfatti contemporaneamente, sono la precisione tecnica, la robustezza, l'affidabilità e l'equità.

Alla luce della evoluzione tecnologica OFCOM ritiene opportuno fornire delle indicazioni sulla misura di ciascuno dei suddetti KPI senza definire, allo stato delle soglie. Ha chiesto, tuttavia, ai rispondenti alla di fornire delle valutazioni sia in relazione ad altri utili KPI sia in relazione alle soglie.

Precisione tecnica

Il criterio dell'accuratezza tecnica si riferisce specificamente a come un metodo di verifica dell'età può determinare correttamente l'età di un utente in ambiente di prova (ad esempio in laboratorio). È stato utilizzato il termine accuratezza "tecnica" per distinguere questo criterio da concetti ulteriori di accuratezza, che possono prendere in considerazione una gamma più ampia di fattori. Un tipico esempio è l'accuratezza tecnica ottenibile nel caso di una stima dell'età in caso di riconoscimento facciale o inferenza del comportamento dell'utente. Alcuni studi forniscono delle metriche per la stima dell'accuratezza. Un esempio è riportato nel documento Age Check Certification Scheme (ACCS) sulle tecnologie di misurazione della garanzia dell'età che ha esaminato diversi parametri per la valutazione della garanzia dell'età.

Robustezza

Il criterio di robustezza descrive il grado in cui un metodo di verifica dell'età può determinare correttamente l'età di un utente in condizioni impreviste o reali. Per soddisfare questo criterio, appare opportuno che i fornitori di servizi adottino le seguenti misure:

a) garantire che i metodi di assicurazione dell'età siano stati sottoposti a test in più ambienti durante lo sviluppo;

c) adottare misure per mitigare i metodi di elusione facilmente accessibili ai minori e laddove sia ragionevole presumere che possano utilizzarli.

I metodi di verifica dell'età dipendenti da input visivi o audio che sono stati testati solo in condizioni di laboratorio potrebbero non funzionare efficacemente nelle condizioni del mondo reale. Condizioni diverse possono essere dovute a scenari intenzionali o non intenzionali.

Gli scenari non intenzionali includono variazioni inattese nell'input. Esempi di circostanze che possono influire sull'efficacia di un controllo dell'età in tali scenari includono:

a) condizioni di illuminazione scarsa/varie;

b) l'uso di telecamere a bassa risoluzione; O,

c) movimento, ad esempio dovuto a un tremore o al movimento naturale di una mano.

Gli scenari intenzionali includono tentativi di eludere il metodo di verifica dell'età (si riconosce che ogni sistema di verifica dell'età possa essere soggetto, anche con successo, a tentativi di elusione).

È necessario quindi che i fornitori di servizi adottino misure volte a garantire che il loro processo di verifica dell'età possa mitigare forme semplici di elusione facilmente accessibili ai minori e che sono consentite dal funzionamento del metodo di verifica dell'età. Si fa riferimento, a titolo esemplificativo, ai casi in cui un minorenne può ottenere l'accesso ai contenuti pornografici utilizzando i dati personali o le forme di identificazione di un adulto o altrimenti impersonificandolo[18].

Affidabilità

Il criterio di affidabilità descrive il grado in cui il risultato dell'età ottenuto da un metodo di verifica dell'età possa essere considerato riproducibile e derivato da prove attendibili.

Ai fini di un sistema di verifica affidabile il fornitore del servizio è tenuto a:

[18] OFCOM, nel proprio documento, ha riportato dei casi di studio a scopo esemplificativo.
Il primo esempio specifico è quello in cui il fornitore di servizi ha implementato un metodo di stima dell'età del volto che richiede solo un'immagine fissa. Tale funzionalità senza ulteriore autenticazione è a rischio di "attacchi di stampa", ovvero quando una fotografia stampata o un'immagine del volto di un utente viene presentata alla fotocamera per tentare di abbinare l'immagine sul documento d'identità con foto. Il rilevamento della vivacità, che conferma l'autenticità di un volto scansionato distinguendolo da immagini o video statici attraverso l'analisi di movimenti facciali sottili (ad esempio, sbattere le palpebre), è un modo in cui un fornitore di servizi può adottare misure per mitigare questo rischio.
Il secondo è quando il fornitore del servizio ha implementato un processo di garanzia dell'età che consente di verificare la loro età utilizzando documenti d'identità falsi o manipolati (ad esempio, dove l'età potrebbe essere alterata utilizzando una penna o una matita su un ID esistente a un'estremità) o forme più avanzate che implicano l'uso improprio di documenti autentici. Il primo è facilmente accessibile ai bambini ed è ragionevole aspettarsi che possano utilizzarlo. Pertanto, laddove un servizio regolamentato utilizza un metodo di corrispondenza dei documenti di identità con foto, è necessario che il fornitore del servizio adotti misure per mitigare i livelli più elementari di documentazione falsa.
In generale nel draft di Linee guida si riconosce che potrebbero esserci altre forme di elusione del processo di verifica dell'età o del processo di controllo dell'accesso nel suo insieme. Per cui occorre che i fornitori di servizi adottino misure per mitigare e astenersi dal promuovere tali forme. Un esempio di potenziale non conformità in questo caso sarebbe il caso in cui il fornitore di servizi incoraggi esplicitamente e deliberatamente gli utenti minorenni a eludere il processo di verifica dell'età e/o i controlli di accesso per gli utenti del Regno Unito, ad esempio fornendo un collegamento e raccomandando l'uso di una VPN per consentire loro di accedere ai contenuti pornografici di fornitori regolamentati.

a) garantire che i metodi di verifica dell'età con un certo grado di varianza (ad esempio, metodi che si basano su modelli statistici o intelligenza artificiale) siano stati adeguatamente testati e che le prestazioni siano misurate e monitorate; E,

b) garantire che le prove utilizzate dal metodo di verifica dell'età provengano da una fonte affidabile.

Equità

Il criterio di equità descrive la misura in cui un metodo di verifica dell'età evita o minimizza errori e risultati discriminatori come, ad esempio, inferiore precisione tecnica per gli utenti di determinate etnie quando si basa sul riconoscimento facciale. Le caratteristiche rilevanti rispetto a tale indicatore includono razza, età, disabilità, sesso e genere.

Al fine di garantire l'equità, è necessario che i fornitori di servizi garantiscano che il metodo di verifica dell'età utilizzato sia stato testato su diversi set di dati. Questo passaggio preliminare risulta necessario per i metodi di verifica dell'età che si basano specificamente sull'apprendimento automatico o sulla modellazione statistica. Infatti, in questo contesto possono verificarsi distorsioni quando i set di dati utilizzati per addestrare un algoritmo non sono sufficientemente diversi.

L'Autorità inglese ritiene inoltre opportuno prevedere che, in aggiunta ai precedenti indicatori, i sistemi di verifica dell'età siano progettati in modo da garantirne accessibilità e interoperabilità.

Accessibilità

A tal fine il sistema di verifica dell'età dovrebbe:

a) essere di facile utilizzo; E

b) funzionare efficacemente per tutti.

Al fine di garantire l'accessibilità il fornitore deve:

a) considerare il potenziale impatto che il metodo o i metodi di verifica dell'età scelti potrebbero avere sulle persone che appartengono a categorie protette;

b) considerare l'offerta di una varietà di metodi di verifica dell'età; E,

c) progettare il percorso dell'utente attraverso il processo di verifica dell'età in modo che sia accessibile a un'ampia gamma di abilità.

Interoperabilità

L'interoperabilità descrive la capacità dei sistemi tecnologici di comunicare tra loro utilizzando formati comuni e standardizzati. Si basa su approcci tecnologici coerenti adottati nei diversi sistemi. Standard, quadri tecnici e altre specifiche sono importanti per raggiungere l'interoperabilità.

Nel contesto della verifica dell'età, l'interoperabilità può comportare il riutilizzo del risultato di un controllo dell'età su più servizi consentendo a diversi fornitori di metodi di verifica dell'età di condividere queste informazioni in linea con le leggi sulla privacy dei dati. I fornitori di servizi possano tenere conto di questo principio rimanendo aggiornati con gli sviluppi in questo ambito e implementando tali soluzioni laddove esistono e sono appropriate per il loro servizio.

I.3 La posizione del CNIL in Francia sull'equilibrio tra tutela dei minori e rispetto della privacy

In Francia la CNIL (il CNIL è un'Autorità amministrativa indipendente, istituita nel 1978 dalla legge sulla protezione dei dati, composta da un collegio di 18 membri e da un gruppo di agenti contrattuali dello Stato) ha analizzato i principali tipi di sistemi di verifica dell'età al fine di chiarire la sua

posizione sul controllo dell'età su Internet, e in particolare sui siti pornografici per i quali tale controllo è obbligatorio. Specifica come questi editori potrebbero adempiere ai loro obblighi legali. Tuttavia, il CNIL rileva che i sistemi attuali possono essere aggirati e invasivi e chiede l'attuazione di modelli più rispettosi della privacy. Di seguito una sintesi di quanto riportato in una recente pubblicazione sul proprio sito proprio sito web.

Informare, sensibilizzare e dare priorità al controllo degli utenti sui dispositivi

In generale, la CNIL ricorda l'importanza di informare e sensibilizzare i minori, i genitori, i funzionari giudiziari e il personale della comunità educativa e della gestione giovanile sulle buone pratiche informatiche, data l'importanza crescente dell'uso degli strumenti digitali nella vita dei cittadini.

Pertanto, nell'ambito dei suoi lavori sui diritti digitali dei minori, la CNIL ha pubblicato nell'agosto 2021 raccomandazioni generali in cui indica i requisiti stabiliti per verificare l'età del minore e il consenso dei genitori nel rispetto della loro vita privata, in particolare, per rispettare gli obblighi del GDPR e della legge sull'accesso dei minori ai social network. La Raccomandazione n. 7, in particolare, chiede che **i sistemi di verifica dell'età siano strutturati attorno a sei pilastri: minimizzazione, proporzionalità, robustezza, semplicità, standardizzazione e intervento di terzi.**

Il CNIL, infine, tende a privilegiare l'utilizzo di dispositivi sotto il controllo degli utenti piuttosto che soluzioni centralizzate o imposte: in quest'ottica, la logica del controllo parentale, che lascia alla responsabilità delle famiglie di limitare l'accesso ai contenuti sensibili, sembra la più rispettosa dei diritti degli individui. Questa logica ha però un limite: **la legge prevede che, in alcuni casi, siano gli editori di siti (ad esempio, siti pornografici) a farsi carico degli obblighi di verifica dell'età**.

La moltiplicazione degli obblighi giuridici per la verifica dell'età online

La legge francese e alcune normative europee subordinano la fornitura di determinati servizi o beni a condizioni di età, che impongono ai siti in questione di verificare l'età del cliente: acquisto di alcolici, giochi d'azzardo e scommesse online, alcuni servizi bancari, ecc.

Per il caso particolare dei siti che diffondono contenuti pornografici, la legge del 30 luglio 2020 volta a tutelare le vittime di violenza domestica ha riaffermato gli obblighi in materia di verifica dell'età, codificati nell'articolo 227-24 del codice penale. Il fatto di diffondere un "messaggio pornografico" suscettibile di essere visto da minorenni è quindi penalmente punibile**; la legge specifica che il controllo dell'età non può derivare da una semplice dichiarazione da parte dell'internauta di avere almeno diciotto anni.**

Il presidente dell'Autorità di regolamentazione delle comunicazioni audiovisive e digitali (**Arcom**), nell'ambito dei poteri che gli sono stati affidati, **ha intimato, nel dicembre 2021, a diversi siti pornografici di istituire un controllo efficace dell'età degli internauti**.

Il 3 giugno 2021 **il CNIL ha emesso un parere sul progetto di decreto che precisa, per l'applicazione della legge del 30 luglio 2020, gli obblighi dei siti che diffondono contenuti pornografici**. In tale occasione ha definito alcuni principi fondamentali per conciliare la tutela della privacy e la tutela dei minori mediante l'implementazione di sistemi di verifica dell'età online per i siti pornografici:

- **nessuna raccolta diretta di documenti di identità da parte dell'editore del sito pornografico;**

- **nessuna stima dell'età basata sulla cronologia di navigazione dell'utente Internet sul web;**
- **nessun trattamento di dati biometrici al fine di identificare o autenticare in modo univoco una persona fisica (ad esempio, confrontando, tramite tecnologia di riconoscimento facciale, una fotografia riportata su un documento di identità con un autoritratto o un selfie).**

Il CNIL raccomanda inoltre, più in generale, il ricorso a un terzo indipendente di fiducia destinato a impedire la trasmissione diretta di dati identificativi relativi all'utente al sito o all'applicazione che offre contenuto pornografico. Attraverso le sue raccomandazioni, il CNIL persegue il duplice obiettivo di impedire ai minori di consultare contenuti inadatti alla loro età, riducendo al minimo i dati raccolti sugli utenti di Internet dagli editori di siti pornografici.

In questo contesto, il CNIL ha emesso numerose raccomandazioni e avvertimenti.

Raccomandazioni e avvertimenti del CNIL sulla verifica dell'età online

La necessità di regolamentare, a breve termine, le soluzioni di verifica dell'età coinvolgendo una terza parte di fiducia

Criteri di controllo dell'età che sollevano questioni importanti

Nell'ambito del ricorso a un soggetto terzo di fiducia, raccomandato dal CNIL nel suo parere del 3 giugno 2021, la verifica dell'età si divide in pratica in due operazioni distinte:

- Da un lato**, l'emissione di una prova dell'età**: l'istituzione di un sistema destinato a convalidare le informazioni sull'età della persona, rilasciando una prova dell'età accompagnata da un livello di confidenza. Questa prova può essere rilasciata da diversi soggetti che conoscono l'utente di Internet, siano essi **fornitori di servizi specializzati nella fornitura di identità digitale o un'organizzazione che conosce l'utente di Internet in un altro contesto** (un commerciante, una banca, un'amministrazione, ecc.). In questo documento vengono analizzate diverse soluzioni.
- D'altro canto, **la trasmissione di tale prova certificata dell'età al sito visitato** affinché quest'ultimo dia accesso o meno al contenuto richiesto (si ricorda che, come indicato nella nota PEReN, un terzo passo consiste nell'analizzare la prova dell'età presentato e fornire o meno l'accesso al contenuto richiesto).

Questi due aspetti comportano importanti questioni di protezione dei dati e di privacy per preservare in particolare la possibilità di utilizzare Internet senza rivelare la propria identità o dati direttamente identificativi. **Affidare queste funzioni a soggetti diversi rende possibile una triplice tutela della privacy**:

- Il soggetto che **fornisce la prova dell'età conosce l'identità dell'internauta ma non sa quale sito sta consultando**;
- Il soggetto che trasmette la prova dell'età al sito può conoscere il sito o il servizio che l'internauta sta consultando ma non conosce la sua identità (nella soluzione "ideale" sviluppata dal CNIL, la prova dell'età passa attraverso l'utente, ciò che consente la compartimentazione tra gli attori);
- il sito o il servizio conosce l'età dell'utente Internet (o solo la sua maggiore età) e sa che sta consultando questo sito, ma non conosce la sua identità e, in alcuni casi, il servizio di verifica dell'età utilizzato.

Un verificatore indipendente di terze parti per proteggere al meglio i dati delle persone

Al fine di preservare la fiducia tra tutte le parti interessate e un elevato livello di protezione dei dati, il CNIL raccomanda pertanto che i siti soggetti all'obbligo di verifica dell'età non effettuino personalmente operazioni di verifica dell'età, ma si affidino piuttosto a soluzioni di terzi verificate in modo indipendente per validità.

Il lavoro della Commissione Europea si muove in questa direzione, come mostra la comunicazione dal titolo "Nuova strategia europea per un Internet più a misura di bambino" (PDF), in particolare nel contesto della proposta relativa a un'identità digitale europea.

Valutazione necessaria della prova di fornitori di età di terze parti

Inoltre, sembra anche necessario, in generale, che i fornitori di prove dell'età siano soggetti a una valutazione da parte di terzi, soprattutto quando adottano un approccio basato sull'analisi automatica o statistica.

A tal fine, e in considerazione della sensibilità dei dati raccolti e della natura invasiva dei sistemi di verifica dell'età e più in generale del trattamento delle informazioni legate all'identità, la creazione di un'etichettatura specifica o la certificazione di questi soggetti terzi potrebbe contribuire a garantire la conformità dei dispositivi al GDPR (rispetto dei principi di minimizzazione, sicurezza dei dati raccolti e finalità).

Una verifica necessariamente imperfetta

Per quanto riguarda i processi di verifica offerti sul mercato, il CNIL sottolinea che attualmente tutte le soluzioni proposte possono essere facilmente aggirate. Infatti, l'utilizzo di una semplice VPN che localizza l'utente Internet in un paese che non richiede una verifica dell'età di questo tipo può consentire a un minore di eludere un sistema di verifica dell'età applicato in Francia, o di eludere il blocco di un sito web che non rispetta con i suoi obblighi legali. Allo stesso modo, è difficile certificare che la persona che utilizza la prova dell'età sia quella che l'ha ottenuta.

Così, nel Regno Unito, dove tali misure sono state prese in considerazione da tempo, il 23% dei minori afferma di poter aggirare le misure di blocco e alcuni editori di contenuti pornografici offrono già servizi VPN. Se l'uso delle VPN deve essere oggetto di una certa vigilanza, va sottolineato che queste tecnologie sono anche uno degli elementi essenziali della sicurezza degli scambi su Internet, utilizzato da molte aziende ma anche dai privati che desiderano proteggere la propria navigazione dal tracciamento effettuato da soggetti pubblici o privati.

Analisi delle soluzioni esistenti

Il CNIL ha analizzato diverse soluzioni esistenti che consentono di verificare l'età degli utenti online, verificando se presentano le seguenti proprietà: **verifica sufficientemente affidabile, copertura completa della popolazione nonché rispetto della protezione dei dati e della privacy delle persone e della loro sicurezza**.

Il CNIL constata che attualmente non esiste alcuna soluzione che soddisfi in modo soddisfacente queste tre esigenze. Invita pertanto le autorità pubbliche e gli attori del settore a sviluppare nuove soluzioni, seguendo le raccomandazioni sopra sviluppate. La CNIL ritiene urgente che vengano proposti e controllati rapidamente sistemi più efficaci, affidabili e rispettosi della vita privata. L'articolo 3 del decreto n. 2021-1306 del 7 ottobre 2021 affida ad ARCOM il compito di sviluppare

linee guida che descrivano in dettaglio l'affidabilità dei processi tecnici che i siti web devono implementare per impedire l'accesso da parte di minori.

Tuttavia, esistono già misure per migliorare il livello di protezione dei minori, in particolare dei più giovani. Diverse soluzioni sono descritte di seguito, in ordine decrescente di maturità dal punto di vista della CNIL. In attesa dell'istituzione di un controllo adeguato e solo per un periodo transitorio, la CNIL ritiene che alcune di queste soluzioni possano consentire di rafforzare la protezione dei minori, a condizione che siano garantiti della loro attuazione e in particolare dei rischi aggiuntivi generati dal loro utilizzo.

1. Verifica dell'età tramite convalida della carta di pagamento

La verifica dell'età tramite carta di pagamento ha il vantaggio di basarsi solo su infrastrutture già implementate e collaudate. Viene pertanto preso in considerazione, anche se questo tipo di verifica può essere aggirato (poiché i minorenni potrebbero essere in possesso di carte di pagamento che consentono loro di effettuare acquisti su Internet) e non accessibile a tutti (poiché gli adulti potrebbero non possedere tale carta, a causa di differenze nell'accesso alla carta di credito a seconda del reddito). Questa soluzione è già implementata da un certo numero di fornitori e si basa sul controllo della validità della carta e non su un pagamento, anche se alcuni propongono un micropagamento, immediatamente cancellato.

Un sistema del genere permette in particolare di tutelare i più giovani (all'incirca fino all'ingresso nella scuola secondaria), che non possono disporre di una carta bancaria che consenta loro di effettuare un pagamento on-line.

Da un lato, questo sistema di verifica dell'età non dovrebbe, in linea di principio, essere attuato direttamente dal titolare del trattamento (ovvero il sito web consultato) ma piuttosto da un terzo indipendente. D'altro canto, i sistemi messi in atto dovrebbero garantire la sicurezza della verifica, al fine di prevenire i rischi di phishing ad essa associati. È quindi importante assicurarsi che le informazioni di pagamento siano inserite correttamente sui siti attendibili. Nel caso in cui si preferisca questa soluzione, sarebbe auspicabile che gli editori dei siti e i fornitori di soluzioni lanciassero parallelamente una campagna di sensibilizzazione sui rischi del phishing, tenendo conto in particolare di questa nuova pratica. L'accesso gratuito deve restare tale: l'utilizzo di questo sistema non deve comportare alcun costo per l'utente.

2. Verifica dell'età mediante stima basata sull'analisi facciale

Alcuni processi di stima dell'età si basano sull'analisi facciale, senza però mirare all'identificazione della persona. Tuttavia, è necessario che chi contesta l'esito della verifica disponga di un altro metodo di verifica.

L'utilizzo di tali sistemi, per il loro aspetto intrusivo (accesso alla telecamera del dispositivo dell'utente durante una prima registrazione presso terzi, o un controllo a campione da parte di questi stessi terzi che potrebbe essere fonte di ricatto tramite webcam quando si richiede l'accesso a un sito pornografico), nonché il margine di errore insito in qualsiasi valutazione statistica, dovrebbero essere imperativamente subordinati al rispetto di requisiti sull'affidabilità e sulle prestazioni verificati in modo indipendente da un Ente terzo.

Secondo il CNIL, dovrebbe essere privilegiata una stima dell'età effettuata localmente sul terminale dell'utente al fine di ridurre al minimo il rischio di fuga di dati. In assenza di tale requisito, questo metodo non dovrebbe essere utilizzato.

3. Il sistema di verifica offline

Il metodo di verifica offline che sembra avere più successo è la commercializzazione solo per gli adulti di “scratch-cards” tipo “gratta e vinci” che consentono loro di recuperare un identificatore e una password che fornirebbe l'accesso a contenuti soggetti a limiti di età. Queste carte verrebbero offerte in determinati punti vendita, ad esempio supermercati o tabaccherie, dove i loro dipendenti già effettuano operazioni di controllo dell'età nell'ambito della vendita di alcolici, sigarette e giochi d'azzardo.

Tuttavia, questa modalità non può essere utilizzata esclusivamente per la consultazione di siti pornografici, in quanto potrebbe risultare stigmatizzante per l'interessato. Dovrebbero essere incluse tutte le attività soggette a limiti di età e questo modello dovrebbe essere promosso da una comunità diversificata di editori (acquisti di prodotti regolamentati, pornografia, ecc.). I limiti di un tale sistema sarebbero gli stessi dell'acquisto di sigarette o alcolici, vale a dire la frode mediante rivendita di carte su un mercato parallelo.

Prerequisiti: questa modalità richiede una governance specifica, con un'autorità che pubblica le carte e gestisce i sistemi di autenticazione.

4. Verifica dell'età mediante analisi dei documenti di identità

La verifica dell'età può essere effettuata da una terza parte responsabile della raccolta e dell'analisi di un documento di identità fornito dall'utente. Tale sistema può essere facilmente aggirato utilizzando il documento di identità di un'altra persona se è necessaria solo la copia del documento (possibilità di utilizzare un documento di un altro adulto, anche all'interno dello stesso nucleo familiare). Questo sistema è quindi inaffidabile e irrispettoso dei dati personali, perché richiede, per funzionare, la raccolta e il trattamento di documenti ufficiali di identità.

Alcuni sistemi verificano l'identità della persona confrontando la fotografia del documento di identità fornito con un test di “live detector”, vale a dire la cattura di una fotografia o di un video ripreso dalla persona dell'utente al momento della verifica dell'età richiesta, al fine di verificare che l'utente sia effettivamente la persona che dichiara di essere e contrastare possibili elusioni del dispositivo. Questo processo è molto più affidabile e viene utilizzato anche per la verifica dell'identità secondo lo standard ANSSI PVID.

Tuttavia, poiché comporta il trattamento di dati biometrici, il suo utilizzo dovrebbe essere particolarmente regolamentato e in linea di principio, in applicazione del GDPR, essere previsto da una specifica norma giuridica o basarsi sul libero consenso delle persone.

Prerequisiti: come per lo standard PVID, è necessario istituire un organismo di certificazione (o etichettatura) che permetta di verificare che ci siano le garanzie necessarie per la raccolta e l'analisi dei documenti di identità.

5. L'utilizzo degli strumenti offerti dallo Stato per verificare identità ed età

L'utilizzo di banche dati pubbliche o di un sistema di autenticazione come FranceConnect potrebbe teoricamente consentire di dimostrare l’età per accedere a determinati siti o servizi online. Tuttavia, FranceConnect non è stato progettato con questo scopo, ma con il desiderio di semplificare le procedure amministrative: il suo stesso funzionamento si basa sulla registrazione degli utilizzi sui server dello Stato. Questa modalità non appare quindi soddisfacente, poiché porterebbe lo Stato a

disporre di un elenco di collegamenti di natura puramente privata. Inoltre, per quanto riguarda la consultazione di siti pornografici, l'utilizzo di questi dispositivi comporterebbe il rischio di associare un'identità ufficiale a informazioni intime e ad un presunto orientamento sessuale.

D'altro canto, come spiegato sopra, si potrebbe prendere in considerazione la connessione di un servizio di gestione degli attributi gestito da un terzo di fiducia ai sistemi di identità dello Stato.

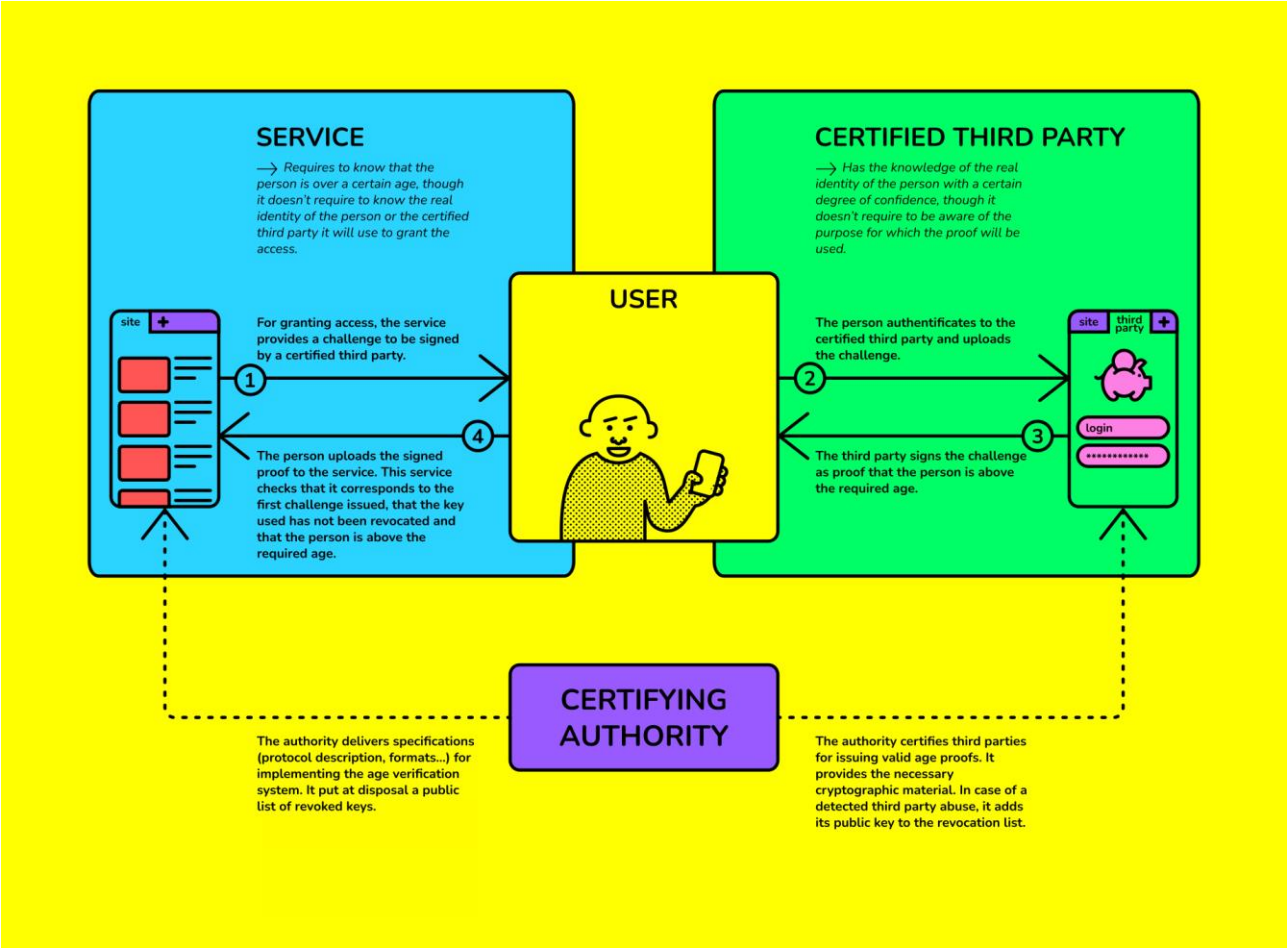
Prerequisiti: è necessario avvalersi di soggetti terzi di fiducia che colleghino i servizi di gestione degli attributi ai sistemi di identità dello Stato.

6. Sistemi inferenziali di verifica dell'età

Esistono tre varianti principali di questo tipo di analisi: la prima appare difficilmente compatibile con la protezione dei dati, mentre la seconda solleva questioni di affidabilità. Il terzo, che solleva anch'esso importanti interrogativi, può essere utilizzato solo da un numero limitato di servizi che già raccolgono molti dati di navigazione.

- Importazione della cronologia di navigazione Internet dell'individuo: questo metodo appare troppo invadente per il semplice scopo di controllo dell'età.
- Analisi della "maturità" tramite questionario: questo metodo sembra poter evitare il trasferimento di dati personali. Tuttavia, questo metodo sembra essere relativamente affidabile e la possibilità di elusione (condivisione delle risposte online) è significativa, così come i pregiudizi che potrebbero essere associati ad esso. Ad esempio, una parte della popolazione potrebbe essere discriminata in base alle proprie competenze (lettura, comprensione), al proprio livello di conoscenza della lingua, ai propri riferimenti culturali, ecc. Questo metodo dovrebbe quindi essere evitato.
- Analisi della navigazione sui servizi specifici dell'editore del sito (in particolare le grandi piattaforme digitali). Il riutilizzo dei dati per la creazione di modelli di inferenza (o deduzione) dell'età sembra possibile, fatti salvi i seguenti punti:
    - in linea di principio questo metodo non dovrebbe portare ad una decisione automatizzata, ma ad una prima stima che, in caso di sospetto mancato rispetto del requisito dell'età, può portare ad uno scambio con l'utente di Internet;
    - non devono essere raccolti dati aggiuntivi al solo scopo di costruire il modello (vengono utilizzati solo i dati già raccolti);
    - i dati prodotti sui servizi della piattaforma devono essere distinti dai dati raccolti tracciando la navigazione dell'utente su altri siti (ad esempio, mediante l'autenticazione sulla piattaforma, mediante l'installazione di un meccanismo per tracciare l'accesso a determinate pagine web, ecc.);
    - il sistema di inferenza dovrebbe essere valutato da una terza parte indipendente, al fine di limitare i rischi.

Il Laboratorio di Innovazione Digitale della CNIL (LINC), ha dimostrato la fattibilità di un sistema basato su un protocollo sicuro, che si basa su un processo implementato in crittografia che consente alle persone identificate di dimostrare che una situazione è vera senza dover rivelare altre informazioni. Si è visto che è possibile, attraverso un sistema di terze parti, garantire la tutela dell'identità dell'individuo e il principio di minimizzazione dei dati, pur mantenendo un elevato livello di garanzia sull'accuratezza dei dati trasmessi. Si presuppone tuttavia che i terzi utilizzati siano completamente indipendenti dagli editori.



I.4 La consultazione pubblica del regolatore francese Arcom

In Francia, in applicazione delle disposizioni dell'articolo 227-24 del codice penale, introdotto dalla legge n. 92-684 del 22 luglio 1992, è vietato esporre i minori a contenuti pornografici. L'articolo 23 della legge n. 2020-936 del 30 luglio 2020, volta a tutelare le vittime di violenza domestica, ha affidato all'Autorità di regolamentazione delle comunicazioni audiovisive e digitali (Arcom) la prerogativa di diffidare i servizi di comunicazione al pubblico non conformi a tale obbligo penale, nonché il deferimento al giudice allo scopo di bloccare i siti che non rispettano la suddetta diffida.

Il disegno di legge Francese denominato PJL SREN, volto alla messa in sicurezza e alla regolamentazione dello spazio digitale, prevede di attribuire ad Arcom il potere di bloccare amministrativamente i servizi di comunicazione pubblica online con responsabilità editoriale e i servizi delle piattaforme di condivisione di video che diffondono contenuti pornografici accessibili ai minorenni dopo essere stati condannati a conformarsi all'articolo 227-24 del codice penale. Tale potere, esercitato nell'ambito di una speciale procedura posta sotto il controllo del giudice amministrativo, integrerebbe i poteri altrimenti riconosciuti al giudice giudiziario in questa materia.

Inoltre, il disegno di legge prevede che **Arcom adotti un quadro, previa consultazione della Commissione nazionale per l'informatica e le libertà (CNIL), al fine di determinare i requisiti tecnici minimi applicabili ai sistemi di verifica dell'età predisposti per l'accesso ai servizi che diffondono contenuti pornografici.** Il mancato rispetto dei requisiti comporta una sanzione pecuniaria, previa diffida da parte di Arcom.

In data 11 aprile 2024, Arcom ha pubblicato la **Consultazione pubblica sul progetto di un quadro che determina i requisiti tecnici minimi applicabili ai sistemi di verifica dell'età messi in atto per l'accesso a contenuti pornografici online**, in previsione dell'adozione del disegno di legge PJL SREN.

Il testo sottoposto a consultazione prevede un insieme di requisiti minimi obbligatori e di requisiti opzionali come di seguito descritti.

Robustezza della soluzione

La tutela dei minori deve risultare come impostazione predefinita, a partire dalla visualizzazione della prima pagina di un servizio di comunicazione pubblica online che consenta la diffusione di contenuto pornografico. I servizi online che trasmettono contenuti pornografici sono tenuti a visualizzare uno schermo che non contenga contenuti pornografici "purché non sia stata verificata l'età dell'utente".

I servizi online che trasmettono contenuti pornografici devono garantire che nessun utente acceda a contenuti pornografici finché non abbia dimostrato la maggiore età, ad esempio, oscurando completamente la home page del servizio.

Gli editori possono segnalare la natura pornografica del loro servizio. Per fare ciò, possono fare affidamento su un meccanismo di autodichiarazione (ad esempio etichettando ogni pagina web come "riservata ad adulti"), consentendo ai sistemi di controllo parentale di essere consapevoli dell'età minima richiesta per accedere ai contenuti del sito.

Efficacia della soluzione

La soluzione tecnica di verifica dell'età implementata dai servizi che distribuiscono contenuti pornografici deve consentire di distinguere chiaramente gli utenti minorenni da quelli adulti.

Limitazione della possibilità di elusione

I servizi che diffondono contenuti pornografici devono fare del loro meglio, in conformità con gli elevati standard di diligenza professionale del settore, per limitare le possibilità di elusione delle soluzioni tecniche che implementano. I sistemi di verifica dell'età non devono consentire la condivisione della prova dell'età con altre persone. Infine, il sistema deve essere robusto contro i rischi di attacchi, come *deepfake*, *spoofing*, ecc.

Ad esempio, per quanto riguarda le soluzioni basate sulla stima dell'età mediante l'analisi delle caratteristiche facciali, i servizi che trasmettono contenuti pornografici devono garantire che le soluzioni contengano un meccanismo per il riconoscimento degli organismi viventi, la cui efficacia sia conforme allo stato della tecnica. Il rilevamento deve essere effettuato con una qualità dell'immagine sufficiente e consentire di escludere qualsiasi processo di diversione che possa essere utilizzato da minori per apparire artificialmente come adulti, in particolare mediante l'uso di foto, video registrati o addirittura maschere. Invece, per quanto riguarda le soluzioni tecniche per generare la prova dell'età sulla base della presentazione di un documento di identità fisica, i servizi interessati che distribuiscono contenuti pornografici devono verificare: (i) che il documento sia reale, e che non si tratti di una semplice copia; (ii) che l'utente è titolare del documento di identità fornito. Tale verifica può essere effettuata in particolare mediante il riconoscimento dei lineamenti del volto mediante un meccanismo di rilevamento vivente, alle condizioni sopra indicate.

Verifica dell'età ogni volta che viene consultato il servizio

La verifica dell'età deve avvenire ad ogni consultazione di un servizio che diffonde contenuti pornografici. Dopo che la consultazione del servizio viene interrotta, deve scattare una nuova verifica dell'età in caso di nuovo accesso a contenuti pornografici.

Il rispetto di tale criterio lascia impregiudicata la possibilità, per l'utente, di utilizzare prove dell'età riutilizzabili o da lui stesso rigenerate, previa presenza di un secondo fattore di autenticazione. Ciò può essere fatto collegando l'utilizzo della prova riutilizzabile al terminale della persona interessata, come nel caso dei portafogli digitali. Inoltre, il sistema di verifica non deve consentire che questa prova venga condivisa con un'altra persona o con un altro servizio.

A esempio, in caso di un dispositivo condiviso tra un adulto e un minore, è opportuno evitare che il periodo di validità della verifica dell'età consenta la visione di contenuti pornografici senza ulteriore verifica. La validità di una verifica dell'età deve quindi cessare nel momento in cui l'utente esce dal servizio, ovvero quando termina la sessione, quando l'utente esce dal browser o quando il sistema operativo entra in stand-by e, comunque, dopo un periodo di un'ora di inattività.

Uso di un account utente

L'implementazione di una soluzione di verifica dell'età non deve richiedere la creazione di un account utente sul servizio in questione che renda disponibili contenuti pornografici. Inoltre, la prova dell'età non può essere memorizzata in un account utente su tale servizio. In ogni caso, l'obbligo di verifica dell'età si applica ad ogni accesso, con o senza account utente.

Non discriminazione

Le soluzioni adottate dai servizi mirati che diffondono contenuti pornografici non devono avere l'effetto di discriminare determinati gruppi di popolazione, in particolare per i motivi stabiliti dall'articolo 21 della Carta dei diritti fondamentali dell'Unione europea. Pertanto, l'efficacia della soluzione tecnica di verifica dell'età deve essere la stessa indipendentemente dalle caratteristiche fisiche dell'utente. Per quanto riguarda i sistemi per la generazione di prove dell'età basati sul *machine learning* o su modelli statistici, i fornitori di servizi possono, ad esempio, testare la loro soluzione su diversi database per garantire la conformità a questo requisito.

È infatti essenziale che i sistemi di controllo dell'età limitino i pregiudizi discriminatori, che generano anche errori tali da metterne in discussione sia l'affidabilità che l'accettabilità.

I servizi online che diffondono contenuti pornografici sono invitati a integrare eventuali pregiudizi discriminatori, suddivisi in base ai pertinenti motivi di discriminazione, nella valutazione della performance del loro sistema di verifica dell'età, ma anche durante gli audit.

Protezione dei dati personali

I sistemi di verifica dell'età nel loro complesso devono rispettare la normativa vigente in materia di tutela dei dati personali e della privacy, compresi i principi di minimizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita (articoli 5 e 25 del GDPR).

I fornitori di tali sistemi devono prestare particolare attenzione ai seguenti principi:

- esattezza, proporzionalità e minimizzazione dei dati raccolti;
- informazioni per l'utente concise, trasparenti, comprensibili e facilmente accessibili;
- adeguati periodi di conservazione dei dati;
- possibilità per gli interessati di esercitare i propri diritti e cioè il diritto di accesso, il diritto di opposizione, il diritto di rettifica, il diritto di limitazione di trattamento, il diritto alla cancellazione, il diritto alla portabilità;
- sicurezza all'avanguardia dei sistemi informativi utilizzati nel trattamento dei dati personali.

Nel 2022, la CNIL ha pubblicato un esempio di un meccanismo di verifica dell'età rispettoso della vita privata per la trasmissione di un attributo di identità (in questo caso la prova dell'età). Questo meccanismo, conosciuto da allora con il nome di "doppio anonimato" o "doppia riservatezza", è stato oggetto di sviluppi e sperimentazioni da parte di diversi attori pubblici e privati, consentendo di

confermarne la fattibilità tecnica e la capacità di rispondere all'esigenza per la tutela della privacy inerente ai meccanismi di verifica dell'età online. Corrisponde inoltre agli obiettivi generalmente fissati per i sistemi di identità digitale, compresa la gestione degli attributi. Tuttavia, questo meccanismo, sebbene denominato "doppio anonimato", non è del tutto "anonimo" ai sensi del GDPR, ma garantisce comunque un'elevata riservatezza.

I servizi di comunicazione pubblica online che mettono a disposizione contenuti pornografici devono offrire ai propri utenti almeno un sistema di verifica dell'età che rispetti le norme di tutela della privacy in "doppio anonimato", garantendo che tale sistema possa essere utilizzato dalla grande maggioranza dei suoi utenti.

Tale requisito entrerà in vigore alla fine del periodo transitorio previsto dalla regolamentazione, fatti salvi i requisiti minimi indicati di seguito. Pertanto, fino a tale data, i sistemi di verifica dell'età devono rispettare i requisiti minimi di base forniti di seguito per garantire un livello accettabile di protezione dei dati personali dei propri utenti.

Requisiti minimi applicabili a tutti i sistemi di verifica dell'età

I seguenti criteri costituiscono una base minima di requisiti applicabili a tutti i sistemi di verifica dell'età coperti dalla proposta di regolamentazione.

Indipendenza del fornitore del sistema di verifica dell'età dai servizi mirati che diffondono contenuti pornografici

Il fornitore di sistemi di verifica dell'età deve essere giuridicamente e tecnicamente indipendente da qualsiasi servizio di comunicazione pubblica online contemplato dal regolamento e garantire che i servizi interessati che diffondono contenuti pornografici non abbiano in nessun caso accesso ai dati utilizzati per verificare l'età dell'utente.

Riservatezza per quanto riguarda i servizi che diffondono contenuti pornografici

I dati personali, che consentono all'utente di verificare la propria età con un servizio di comunicazione oggetto della presente proposta di regolamento, non devono essere trattati.

In particolare, l'implementazione di soluzioni di verifica dell'età non deve consentire ai servizi di comunicazione oggetto del regolamento di raccogliere l'identità, l'età, la data di nascita o altre informazioni di carattere personale di tali utenti.

Riservatezza per quanto riguarda i fornitori che generano la prova dell'età

Laddove il sistema di verifica dell'età non consenta all'utente di ottenere un'identità digitale o una prova dell'età riutilizzabile, i dati personali forniti dall'utente per ottenere la verifica dell'età, non devono essere conservati dal fornitore del servizio di prova dell'età. Inoltre, questo tipo di sistema non dovrebbe richiedere la raccolta di documenti di identità ufficiali.

Riservatezza nei confronti di eventuali altre terze parti coinvolte nel processo di verifica dell'età

Laddove nel processo di verifica dell'età siano coinvolti soggetti terzi diversi dai fornitori di prova dell'età, ad esempio per la gestione della prova o della fatturazione del servizio, tali soggetti terzi non dovranno conservare i dati personali del personale degli utenti del sistema, ad eccezione dell'archiviazione della prova su richiesta dell'utente.

Misure per salvaguardare i diritti e le libertà delle persone mediante verificatori dell'età

Nel determinare se un utente può accedere o meno a un servizio di comunicazione pubblica online sulla base delle prove presentategli, il servizio interessato che diffonde contenuto pornografico prende

una decisione automatizzata ai sensi dell'articolo 22 del GDPR. Infatti, rifiutando l'accesso a un servizio, tale decisione è idonea a produrre effetti giuridici sugli interessati, o quanto meno, a produrre effetti significativi che colpiscono in modo analogo alcuni soggetti.

Il CNIL ritiene che tale decisione possa basarsi sull'eccezione prevista al paragrafo 2.b. dell'articolo 22 del GDPR, nella misura in cui il servizio in questione che diffonde contenuto pornografico è soggetto all'obbligo di verifica dell'età previsto dall'articolo 227-24 del codice penale e, in definitiva, dalle disposizioni del PJL SREN. L'articolo 22.2.b del GDPR richiede che misure adeguate per salvaguardare i diritti, le libertà e gli interessi legittimi dell'interessato siano previste dalle disposizioni che autorizzano tale decisione automatizzata.

Al fine di preservare i requisiti di privacy che mirano a limitare la capacità dei servizi di identificare le persone, tali misure devono essere messe in atto non dal servizio in questione che diffonde contenuti pornografici, ma dal fornitore della soluzione tecnica per la verifica dell'età, indipendentemente dal fornitore dell'attributo o l'emittente della prova. Tali misure devono consentire agli utenti, in caso di errore, di contestare il risultato dell'analisi delle loro caratteristiche al fine di ottenere la prova dell'età. Per esercitare tali rimedi, i fornitori di soluzioni di verifica dell'età dovrebbero offrire agli utenti la possibilità di utilizzare diversi fornitori di attributi o, a seconda della soluzione, diversi emittenti di prove.

Il servizio in questione che diffonde contenuti pornografici è comunque tenuto a rispettare gli obblighi di informazione imposti dal GDPR e deve avvisare gli utenti della possibilità di ricorrere al fornitore della soluzione di verifica dell'età.

In ogni caso, i fornitori di attributi devono anche consentire alle persone di rettificare i propri dati ai sensi dell'articolo 16 del GDPR.

Riservatezza rafforzata per quanto riguarda i servizi mirati che diffondono contenuti pornografici

Un sistema di verifica dell'età che utilizza il "doppio anonimato" non deve consentire ai servizi di comunicazione oggetto del regolamento di riconoscere un utente che ha già utilizzato il sistema sulla base dei dati generati dal processo di verifica dell'età.

L'uso di sistemi di verifica dell'età che utilizzano il "doppio anonimato" non dovrebbe consentire a questi servizi di conoscere o dedurre la fonte o il metodo per ottenere prove dell'età coinvolte nel processo di verifica dell'età di un utente.

Un sistema di verifica dell'età che rispetti il "doppio anonimato" non dovrebbe consentire a questi servizi di riconoscere che due prove di maggiore età provengono dalla stessa fonte di prova dell'età.

Riservatezza rafforzata nei confronti dei soggetti che forniscono prova dell'età

Un sistema di verifica dell'età che utilizza il "doppio anonimato" non deve consentire ai fornitori di prove dell'età di sapere per quale servizio viene eseguita la verifica dell'età.

Maggiore riservatezza nei confronti di eventuali altri terzi coinvolti nel processo di verifica dell'età

Un sistema di verifica dell'età che utilizza il "doppio anonimato" non deve consentire a nessun altro soggetto terzo coinvolto nel processo di riconoscere un utente che ha già utilizzato il sistema. Ad esempio, un soggetto terzo che assicura la trasmissione della prova dell'età o ne certifica la validità non deve poter sapere se ha già elaborato la prova dello stesso utente.

Disponibilità e copertura della popolazione degli utenti

I servizi di comunicazione regolamentati devono garantire che i loro utenti dispongano di almeno due diversi metodi per generare prova dell'età consentendo di ottenere la prova dell'età attraverso un sistema di verifica dell'età di “doppio anonimato”. In pratica, un fornitore di servizi che offra una soluzione di doppio anonimato deve combinare almeno due metodi per ottenere la prova dell'età (ad esempio, una soluzione basata sui documenti di identità e una soluzione basata sulla stima dell'età).

I servizi di comunicazione coperti da questa norma devono garantire che un sistema di verifica dell’età “doppio anonimato” sia disponibile per almeno l’80% della popolazione adulta residente in Francia.

Informazione esplicita del livello di tutela della privacy degli utenti

Ogni soluzione di verifica dell’età deve essere esplicitamente associata al proprio livello di protezione della privacy, in modo che le soluzioni che soddisfano gli standard di “doppio anonimato” siano visualizzate in modo chiaro e leggibile. In ogni caso non devono essere confuse o evidenziate altre soluzioni al fine di indurre in errore l'utente a favore di soluzioni meno tutelanti della privacy.

Qualora un soggetto terzo che partecipa al processo di verifica dell'età venga a conoscenza del servizio per il quale viene effettuata la verifica dell'età, l'utente dovrà essere chiaramente informato.

Per i sistemi di verifica dell'età che rispettano il principio del "doppio anonimato", l'utente deve essere chiaramente informato che questa soluzione garantisce che il fornitore della verifica dell'età non possa conoscere il servizio per il quale viene effettuata tale verifica.

Requisiti non obbligatori e buone pratiche

I seguenti criteri non sono attualmente richiesti obbligatoriamente per i sistemi di verifica dell’età, ma costituiscono un insieme di buone pratiche verso cui dovrebbero mirare le soluzioni di verifica dell’età.

Possibilità per l'utente di generare autonomamente una prova dell'età in modo confidenziale:

- l'utente può generare una prova dell'età localmente, senza informare l'emittente iniziale dei propri attributi di età, né un'altra terza parte;
- l'utente può generare una prova dell'età tramite un servizio online che può essere utilizzato senza avere alcun accesso ai propri dati personali.

Riservatezza dei sistemi di verifica dell'età nel loro insieme:

- il sistema si basa su zero prove di conoscenza;
- il sistema si basa su tecniche di crittografia con proprietà di resistenza agli attacchi più complessi, anche futuri

Soluzioni derogatorie di generazione di prove accettate in via temporanea

Il regolatore francese prevede che, per un periodo transitorio di sei mesi dalla pubblicazione del regolamento, destinato a consentire ai servizi ad essa soggetti di individuare e implementare una soluzione di verifica dell'età che soddisfi tutti i criteri determinati, le soluzioni che utilizzano la carta bancaria saranno ritenute conformi alle caratteristiche tecniche del quadro, fatto salvo il rispetto delle seguenti condizioni.

Una soluzione che utilizza le carte bancarie costituirebbe una prima modalità di filtraggio di una parte dei minori.

Il filtraggio può essere effettuato sia sotto forma di pagamento di 0 euro, sia tramite semplice autenticazione (senza pagamento).

Questi sistemi di verifica:

- non devono essere implementai direttamente dai servizi mirati che distribuiscono contenuti pornografici, ma da un terzo indipendente dal servizio;
- devono garantire la sicurezza della verifica, al fine di prevenire i rischi di phishing ad essa associati. È quindi importante assicurarsi che le informazioni di pagamento siano inserite correttamente sui siti attendibili. A questo proposito, sarebbe auspicabile che i servizi mirati che diffondono contenuti pornografici e i fornitori di soluzioni lanciassero una campagna coordinata di sensibilizzazione sui rischi del phishing, tenendo conto in particolare di questa nuova pratica;
- devono consentire almeno di assicurare l'esistenza e la validità della carta, escludendo una semplice verifica della congruenza del numero della carta;
- implementano l'autenticazione forte prevista dalla Direttiva Europea (UE) 2015/2366 relativa ai servizi di pagamento (c.d. "DSP2"), ad esempio affidandosi al protocollo 3-D Secure, nella sua seconda versione in vigore, per garantire che l'utente del servizio è il titolare della carta mediante autenticazione a due fattori.

Al termine di questo periodo transitorio Arcom preciserà nuovamente le condizioni alle quali la verifica dell'età tramite carta bancaria potrà continuare ad essere accettata.

I.4 La consultazione pubblica del regolatore spagnolo

L'Autorità di regolamentazione spagnola (CNMC) ha avviato una *Consultazione pubblica sui criteri per garantire l'adeguatezza dei sistemi di verifica dell'età sui servizi di piattaforme di condivisione video per contenuti dannosi per i minori.*

Nel contesto normativo nazionale la legge spagnola 13/2022 del 7 luglio sulla comunicazione audiovisiva generale (*Ley General de Comunicación Audiovisual*; di seguito LGCA) ha esteso l'ambito soggettivo dei soggetti regolamentati, i fornitori di servizi di media audiovisivi, anche i fornitori di servizi di piattaforme per la condivisione di video. Lo scopo di questa estensione è garantire la protezione dei minori dai contenuti dannosi, nonché proteggere gli utenti in generale dai contenuti che incitano alla violenza, all'odio o alla commissione di un crimine, in particolare il terrorismo.

L'articolo 89 della LGCA impone una serie di obblighi a questi nuovi agenti, **incluso l'obbligo di implementare sistemi di verifica dell'età per l'accesso alle loro piattaforme**, come misura gold standard per proteggere i minori dai contenuti audiovisivi dannosi.

La consultazione in parola si pone l'obiettivo di garantire che l'attuazione di questo nuova norma sia quanto più efficace possibile.

Il regolatore osserva che l'esistenza di VSP (Video sharing platform) liberamente accessibili e senza restrizioni volti a diffondere contenuti che per loro natura sono dannosi per i minori, come la violenza o la pornografia, è una questione di preoccupazione sociale. Soprattutto quando la fruizione di questo tipo di contenuti è resa accessibile ai minori, poiché può alterare la loro capacità di comprensione e compromettere il loro sviluppo fisico, mentale o morale. In questo contesto, evidenzia che lo sviluppo del nuovo quadro normativo europeo sull'audiovisivo ha incluso l'obbligo per i VSP di stabilire misure che garantiscano la protezione dei minori e, in particolare, misure per impedire ai minori l'accesso a contenuti particolarmente dannosi. Questi obblighi sono stati recepiti nel diritto spagnolo attraverso la LGCA del 7 luglio 2022.

In questo contesto la consultazione si pone l'obiettivo di indicare gli elementi minimi ed essenziali che i sistemi di verifica dell'età devono avere per essere considerati conformi all'obiettivo stabilito nella LGCA

Sulla portata materiale dell'obbligo di istituire e gestire sistemi di verifica dell'età per impedire l'accesso dei minori

La LGCA menziona due casi in cui sarebbero applicabili i sistemi di verifica dell'età.

Da un lato, l'articolo 89.1.e) della LGCA prevede che i VSP debbano "Istituire e gestire sistemi di verifica dell'età degli utenti rispetto ai contenuti che possono compromettere lo sviluppo fisico, mentale o morale dei minori che, in ogni caso, impediscono ai minori dall'accesso ai contenuti audiovisivi più dannosi, come la violenza gratuita e la pornografia." Ritenuto che la pubblicità offerta da questi fornitori incoraggia comportamenti altrettanto dannosi per i minori, poiché in molti casi si riferisce a siti pornografici, farmaci di dubbia provenienza, videogiochi violenti o sessualmente espliciti, siti di incontri o numeri di telefono di contatto diretto per servizi sessuali, ritiene giustificato che l'obbligo di istituire e gestire sistemi di verifica dell'età si applichi a tutti i contenuti audiovisivi, comprese le comunicazioni commerciali gestite dai VSP soggetti all'articolo 89, paragrafo 1, lettera e).

I. Sugli elementi minimi dei sistemi di verifica dell'età che impediscono l'accesso dei minori

Sulla base dell'analisi dei diversi servizi di verifica dell'età, nonché dell'esperienza della Francia e della Germania, il regolatore propone una serie di elementi minimi che i diversi sistemi di verifica dell'età devono soddisfare affinché possano considerarsi conformi alla legge.

- Il sistema di verifica dell'età implementato dal VSP deve garantire, in ogni momento, che la persona che accede ai contenuti dannosi sia maggiorenne.

  Considerato che l'accesso a questo tipo di servizi tende ad essere ricorrente, sarà necessario garantire che la persona che in prima istanza accredita la maggiore età sia anche l'unica che potrà utilizzare tale accreditamento per accedere in futuro al servizio.

  In altre parole, il sistema di verifica deve garantire che chi vuole accedere ai contenuti sia realmente la persona identificata come maggiorenne, evitando possibili casi di furto di identità o violazione del sistema.

  L'identificazione e l'autenticazione possono essere effettuate sulla base di **documenti di identità o certificati digitali.** In alcuni casi è possibile una registrazione preventiva, dove è prevista l'identificazione dell'età dell'iscritto, e il successivo controllo che tale persona (precedentemente identificata) sia quella che si sta autenticando per accedere al servizio.

  I meccanismi di verifica dell'età si articoleranno in due fasi: la prima corrisponde all'identificazione univoca della persona, la seconda ad un'autenticazione che confermi che è la persona precedentemente identificata ad accedere al servizio per adulti in ogni utilizzo successivo.

- Il primo passo dell'identificazione univoca riguarda la necessaria identificazione personale con verifica dell'età.

  Per raccogliere dati identificativi e di verifica dell'età, è stato tradizionalmente necessario effettuare un controllo *faccia a faccia* e utilizzare documenti d'identità ufficiali (carta

d'identità nazionale, carta di soggiorno, passaporto), confrontando la fotografia o l'impronta digitale.

Tuttavia, il progresso tecnologico osservato nella formulazione di questo tipo di soluzioni sembra rendere **superflua la necessità del controllo faccia a faccia quando si utilizzano meccanismi di identità digitale** a condizione che tale verifica eviti il rischio di falsificazione ed elusione.

In ogni caso, spetta al fornitore decidere quali meccanismi di verifica dell'età implementare per il proprio servizio e, in ultima analisi, spetta a ciascun utente scegliere tra le possibilità che gli vengono offerte.

Il regolatore ritiene ragionevole **scartare come inadeguate alcune soluzioni come la semplice presentazione o l'invio di una copia del documento di identità, nonché l'identificazione e la verifica dell'età mediante presentazione di una fotografia**, poiché queste non presentano garanzie adeguate.

Per concludere è necessario poi garantire che le chiavi di accesso vengano trasmesse solo alla persona identificata.

- La seconda fase di autenticazione consiste nel garantire che solo la persona rispettivamente identificata e di età verificata abbia accesso al servizio in questione.

  A tal fine, l'autenticazione deve avvenire all'inizio di ogni processo di utilizzo o login e l'accesso ai contenuti deve dipendere da un elemento di autenticazione assegnato individualmente. Inoltre, poiché nella maggior parte delle soluzioni, dopo l'identificazione univoca, l'utente, riconosciuto maggiorenne e quindi autorizzato riceve una forma di "password" per tutti i successivi processi di utilizzo, occorre impedire la possibilità di cedere le autorizzazioni di accesso a terzi non autorizzati. La divulgazione o la moltiplicazione delle password può essere impedita mediante misure tecniche che rendano difficile la moltiplicazione delle autorizzazioni di accesso, ma anche informando l'utente dei rischi personali derivanti dall'uso non autorizzato della propria password.

Il sistema deve essere robusto e accurato per evitare possibili furti d'identità.

Indipendentemente dal tipo di identificazione effettuata, è essenziale che gli elementi di giudizio applicati consentano di garantire che la persona identificata sia maggiorenne.

Neutralità tecnologica

Considerate le diverse modalità di accesso a contenuti pornografici, violenti e altri dannosi, il sistema di verifica dell'età dovrebbe poter essere utilizzato su qualsiasi dispositivo tecnologico e sistema operativo, in modo tale che i minori non possano eludere o aggirare i controlli e accedere ai contenuti.

II. Le soluzioni tecnologiche disponibili per la verifica dell'età

Il regolatore ritiene che la semplice dichiarazione di essere maggiorenne senza alcuna verifica successiva non fornisca un livello di sicurezza adeguato a impedire ai minori di accedere a tali contenuti. Attualmente sul mercato esistono soluzioni di verifica dell'età che potrebbero essere efficaci. La validità di una soluzione tecnologica per la verifica dell'età dipende dall'affidabilità con cui impedisce ai minori di accedere ai contenuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali. Le soluzioni tecniche possono essere sostanzialmente raggruppate in

due tipologie. Di seguito verranno illustrate le principali caratteristiche di ciascuno, specificando, ove opportuno, i possibili svantaggi di ciascuno.

A. Verifica dell'età mediante carta d'identità o certificato digitale da questa derivante

- La verifica dell'età può essere effettuata controllando un **documento di identità** fisica tradizionale, un documento di identità fisica elettronica, oppure un documento di identità digitale. Questi documenti potrebbero essere, ad esempio, carte d'identità, passaporti, certificati di residenza (cittadini UE), carte di soggiorno (cittadini extra-UE) o un supporto di identità digitale o virtuale non basato su un documento fisico.
- Analogamente, in alternativa all'identità vera e propria, è possibile prevedere **l'utilizzo di credenziali di raggiungimento della maggiore età,** come quelle previste dal Regolamento eIDAS, di prossima adozione, basate sull'**identità digitale**. In questo modo, tale età legale può essere autonomamente accreditata senza la necessità di divulgare ulteriori informazioni sull'utente, nel rispetto del principio di minimizzazione, e preservando l'anonimato dell'utente.

  Per quanto riguarda l'autenticazione, potrebbero essere utilizzate procedure *faccia a faccia* o a distanza basate su chiavi, impronte digitali o fotografia della persona.

  Alcune soluzioni di autenticazione prevedono l'avvicinamento del volto alla fotocamera del dispositivo con cui si richiede la verifica dell'età, per garantire che non venga utilizzata una fotografia.

  Nelle soluzioni faccia a faccia, i maggiorenni **possono ottenere carte per soli adulti, tramite le quali ottengono un nome utente e una password** che consentirebbero loro di accedere a contenuti soggetti a limiti di età. Tali carte verrebbero offerte in determinati punti vendita, come supermercati o tabaccherie, il cui personale è a conoscenza dei controlli sull'età relativi alla vendita di alcolici o sigarette. Lo svantaggio principale è che una misura del genere introdotta solo per la visione di siti pornografici o violenti potrebbe stigmatizzare l'interessato e scoraggiarne la fruizione. Un altro svantaggio sarebbe la rivendita delle carte su un mercato parallelo.

  Ognuno di questi meccanismi potrebbe essere implementato tramite app, per i più comuni sistemi operativi per smartphone, che facilitano l'identificazione e l'autenticazione. Questa struttura potrebbe essere una caratteristica **dei portafogli di identità digitali**.

  Come notato sopra, spetta in ultima analisi all'utente scegliere l'uno o l'altro meccanismo.

B. Verifica dell'età tramite carta bancaria

Nelle soluzioni esistenti di questo tipo, gli utenti inseriscono il proprio nome e i dettagli della carta bancaria (numero della carta, data di scadenza, codice CVC) e questi dati vengono confrontati con un database di pagamento per verificare che la carta sia valida. Potrebbe trattarsi di un semplice controllo che il numero fornito sia nel formato corretto, una richiesta di pre-autorizzazione di un pagamento o un micro-pagamento per ottenere il massimo livello di certezza.

In generale, questo sistema tutela i minori più piccoli (sotto i 10-12 anni) che non possiedono una carta bancaria che consenta loro di effettuare un pagamento online e che hanno meno probabilità di utilizzare carte di terzi. Lo svantaggio di questa soluzione è che offre un livello di sicurezza inferiore, in quanto i minorenni potrebbero essere in possesso di carte bancarie che consentono loro di effettuare acquisti su Internet. Un altro svantaggio è che le carte

bancarie potrebbero non essere accessibili a tutti poiché solitamente sono legate ad un determinato reddito.

III. Sulle organizzazioni che potrebbero effettuare la verifica dell'età

La verifica dell'età può essere effettuata dal fornitore stesso o da una terza parte indipendente. Quest'ultimo caso presenta alcuni vantaggi per il fornitore, come l'esternalizzazione di un servizio che può essere complesso da eseguire, ma soprattutto non scoraggia l'utilizzo dei servizi da parte degli adulti che sono più riluttanti a fornire i propri dati ai VSP.

In questo senso, le organizzazioni indipendenti di verifica dell'età possono essere utilizzate anche per acquistare alcolici o tabacco o per consentire il gioco d'azzardo online. Inoltre, oltre agli esempi sopra riportati per la prova dell'età legale, i verificatori di terze parti sono ampiamente utilizzati dalle società di telecomunicazioni e dalle organizzazioni bancarie per convalidare i dati dei propri clienti prima di stipulare contratti online.

In questo modo, il terzo che fornisce la prova dell'età conosce l'identità o l'attributo di età dell'internauta, ma non sa quale sito sta visitando, e il titolare del servizio sa che l'utente è maggiorenne, ma non conosce nessun'altra informazione personale o relativa all'identità dell'utente. E' necessario chiarire che l'utente deve sapere se il terzo è indipendente dal titolare del servizio al quale chiede l'accesso e vigilare sui possibili legami economici tra i terzi e i titolari dei servizi.

IV. Su ulteriori aspetti da soddisfare mediante la verifica dell'età

Occorre considerare ulteriori aspetti legati alla sicurezza dei meccanismi di verifica dell'età, come l'esistenza di backdoor, la durata massima di una sessione o il limite di tempo per considerare l'inattività. Un ulteriore aspetto da tenere in considerazione tra tutte le possibilità disponibili sul mercato per la verifica dell'età è scegliere un servizio che raccolga adeguatamente i dati sull'età nel modo meno invasivo possibile, rispettando la privacy delle persone.

V. Sintesi dei contributi alla consultazione pubblica

La Commissione Nazionale dei Mercati e della Concorrenza (CNMC), ad aprile 2024 ha pubblicato una sintesi dei contributi[19] alla consultazione pubblica sui sistemi di verifica dell'età utilizzati dalle piattaforme video in Spagna per impedire ai minori l'accesso a contenuti dannosi (INF/DTSA/329/23). La CNMC, conformemente alla Legge Generale della Comunicazione Audiovisiva, ha la competenza per valutare che i sistemi utilizzati dalle piattaforme video stabilite in Spagna impediscano ai minori di 18 anni di accedere a contenuti dannosi - pornografia e violenza gratuita - al momento della verifica dell'età dei suoi utenti.

Nel processo di consultazione pubblica sono pervenuti 35 contributi praticamente da tutti gli attori legati a questo settore: associazioni di utenti, media, agenti audiovisivi, fornitori di sistemi di verifica dell'età, verificatori o piattaforme di scambio video (PIV).

Ambito del divieto di accesso

Tutte le risposte concordano sul fatto che i sistemi di verifica dell'età (SVE) devono coprire sia i contenuti che la relativa pubblicità, poiché violano anche i diritti dei minori. Per quanto riguarda il tipo di piattaforma che deve disporre dello SVE, la stragrande maggioranza (61,5%) ritiene che lo SVE debba avere la precedenza sui contenuti pornografici, indipendentemente dal fatto che siano

[19] https://www.cnmc.es/prensa/respuestas-cp-verificacion-edad-plataformas-20240417

ospitati su una piattaforma generalista o pornografica e che lo SVE debba essere applicato prima dell'accesso ai contenuti (65 %), indipendentemente dal tipo di piattaforma.

Libertà nella scelta dei sistemi di verifica dell'età

La maggior parte dei contributi (83%) sostiene che dovrebbero esserci diversi SVE e che la piattaforma scelga quale implementare. Questo approccio non solo avvantaggia le piattaforme, che possono scegliere lo SVE che si adatta al loro modello di business, ma risponde anche alle diverse esigenze degli utenti (diversi gradi di conoscenza tecnologica, mancanza di un documento ufficiale o riluttanza a condividerlo).

Sistemi di verifica dell'età disponibili sul mercato

La maggior parte degli agenti opta per una verifica remota o non faccia a faccia (85%) e le due opzioni principali nel settore sono:

1. Verifica tramite documento d'identità e contrasto con foto (selfie)
2. Stima dell'età mediante analisi facciale.

Equilibrio tra idoneità dei sistemi e protezione dei dati

La maggioranza ritiene che la protezione dei dati sia un elemento determinante per l'efficacia dello SVE. L'anonimato nell'accesso ai contenuti è stato evidenziato da diversi agenti e in linea con ciò, il portafoglio digitale europeo (eIDAS2) è stato indicato come ideale per questo processo, poiché consente di convalidare solo la maggiore età senza condividere più dati.

D'altro canto, un numero significativo di agenti sostiene la proposta SVE dell'Agenzia spagnola per la protezione dei dati. Mentre altri agenti sostengono che i sistemi di stima facciale siano adatti a questo processo.

Terze parti che potrebbero effettuare la verifica dell'età

Il 92% preferisce che sia una terza entità indipendente. Questa opzione si basa sul fatto che esistono già sul mercato agenti di verifica che svolgono questa funzione in modo sicuro, nel rispetto della protezione dei dati e con trasparenza per l'utente. Inoltre, far eseguire la verifica a una terza parte genera fiducia tra gli utenti.

Strumenti di auto e co-regolamentazione

L'81% capisce che può essere uno strumento molto utile poiché comporta il coinvolgimento del settore, consente maggiore flessibilità e rapidità di adattamento ai cambiamenti e può anche contribuire alla creazione di standard. Al contrario, questo sistema è percepito come lento da costruire.

I.5 La regolamentazione tedesca

L'autorità di regolamentazione tedesca Kommission für Jugendmedienschutz (KJM) nel mese di maggio 2022 ha stabilito criteri[20] per la valutazione dei sistemi di verifica dell'età.

[20] Sito web KJM per i sistemi di verifica dell'età https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme

Questi si basano sul concetto che alcuni contenuti pornografici, dannosi per i minorenni, possono essere distribuiti su Internet solo se il fornitore garantisce che solo gli adulti possano accedervi mediante i cosiddetti sistemi di verifica dell'età (sistemi AV).

I requisiti per tali sistemi AV sono significativamente più elevati rispetto ai requisiti tecnici per l'accesso generico ai contenuti, poiché devono garantire che venga effettuato un controllo dell'età tramite identificazione personale.

La KJM ha quindi sviluppato un **processo di valutazione** con cui analizza e valuta i sistemi di verifica dell'età, su richiesta di aziende o fornitori eventualmente con discussioni o audit in loco. La responsabilità principale per l'implementazione di un sistema di verifica conforme ai criteri spetta tuttavia al fornitore di contenuti. Quest'ultimo deve garantire che nella sua offerta i contenuti pornografici e altri contenuti dannosi per i minori siano accessibili solo agli adulti (gruppi di utenti chiusi).

I dettagli relativi alla griglia di valutazione sono pubblicati nel documento "criteri per la valutazione dei concetti per i sistemi di verifica dell'età"[21].

Secondo i criteri della KJM, la verifica dell'età per i gruppi chiusi di utenti deve essere assicurata attraverso due passaggi strettamente interconnessi:

a) mediante **identificazione almeno una tantum** (verifica dell'età), che generalmente deve avvenire tramite contatto personale. Il presupposto per un controllo affidabile della maggiore età è l'identificazione personale delle persone fisiche, ivi compresa la verifica della loro età. L'identificazione personale è necessaria per evitare il rischio di contraffazione ed elusione.

b) attraverso **l'autenticazione durante i singoli processi di utilizzo**. L'autenticazione serve a garantire che solo la persona identificata e a cui sia stata verificata l'età, possa accedere a gruppi di utenti chiusi e a rendere più difficile il passaggio/trasferimento delle autorizzazioni di accesso a terzi non autorizzati.

Sussistono ulteriori obblighi di sicurezza per i sistemi di verifica dell'età, come ad esempio la protezione nei confronti di *backdoor*, il limite di tempo per una sessione, il timeout dopo un certo periodo di inattività ecc.

La griglia di valutazione KJM consente processi trasparenti per i fornitori, e prevede le seguenti casistiche:

1. **Concetti di verifica dell'età per un utilizzo una tantum (chiave monouso)**

   Come metodo di controllo dell'età, che viene eseguito sempre immediatamente prima di ogni utilizzo o ogni accesso, è accettabile, ad esempio, utilizzare la conferma dell'età tramite la funzione eID della carta di Carta d'identità.

   Inoltre, possono essere sufficienti procedure atte a determinare con un alto grado di probabilità la maggiore età (controllo di plausibilità). Contrariamente ai concetti di verifica affidabile dell'età per un utilizzo ripetuto (vedi di seguito) l'intera procedura deve essere eseguita ogni volta che viene utilizzata.

   Ciò può essere ottenuto ad esempio attraverso una procedura in cui l'utente viene esaminato **tramite una webcam**, a condizione che venga utilizzato solo personale opportunamente addestrato, e venga effettuato un rilevamento efficace *live* e sia garantita una qualità dell'immagine sufficiente. Il rilevamento della vivacità e una qualità dell'immagine sufficiente

[21] Criteri KJM per i sistemi di verifica dell'età pubblicati online al seguente link (in tedesco) https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022__004_.pdf

sono necessari per garantire che sia una persona reale quella seduta davanti alla telecamera e per escludere possibili elusioni, ad esempio l'utilizzo di filmati registrati o il mascheramento. Se l'utente non è chiaramente maggiorenne, dovrà essere effettuato un ulteriore controllo dell'identità. Se il controllo dell'identità viene effettuato tramite webcam, anche in questo caso valgono i requisiti sopra menzionati.

È inoltre necessario garantire che **la carta d'identità** sia controllata da tutti i lati e completamente. Se non è possibile stabilire con certezza che l'utente è maggiorenne, l'accesso potrebbe non essere concesso.

Tuttavia, la mera verifica del codice della carta d'identità o la presentazione di una copia del proprio documento d'identità non sono sufficienti. Anche una copia autenticata del documento d'identità non è sufficiente, poiché conferma solo che un documento corrisponde, ma non identifica una persona.

2. Concetti di verifica dell'età per un utilizzo ripetuto (chiave generale)

La verifica dell'età per un utilizzo ripetuto consiste in due passaggi: identificazione e autenticazione una tantum della persona identificata per ciascuna sessione di utilizzo. Dopo l'identificazione unica, all'utente riconosciuto maggiorenne e quindi autorizzato viene assegnata una sorta di "chiave generale" per tutti i successivi processi di utilizzo. Questo gli dà accesso a un numero qualsiasi di offerte diverse. Rispetto alla precedente "chiave monouso" un controllo dell'età effettuato semplicemente mediante ispezione visiva della persona non soddisfa i requisiti in questo caso.

Il prerequisito per un metodo affidabile di verifica della maggiore età è l'identificazione delle persone fisiche. L'identificazione personale è necessaria per evitare il rischio di contraffazione ed elusione.

I requisiti della KJM per l'**Identificazione** sono specificati come segue:

A. Identificazione della persona fisica: L'identificazione almeno una volta degli interessati deve generalmente avvenire **tramite contatto personale** ossia di un controllo facciale dei presenti (controllo "faccia a faccia") con un confronto dei dati di identificazione ufficiali (carta d'identità, passaporto).

   È anche possibile, a determinate condizioni, ricorrere ad un controllo "in presenza" già avvenuto. È il caso, ad esempio, delle procedure di identificazione mediante dati personali verificati, di età o di nascita, che vengono utilizzati quando si fruisce di determinati servizi o si stipulano determinati contratti (ad es. contratti di telefonia mobile, apertura di conti bancari etc.).

   Si può fare a meno del controllo facciale tra i presenti (controllo "faccia a faccia") se l'identificazione avviene tramite **software confrontando i dati biometrici riportati sul documento di identità** e una foto della persona da identificare, nonché registrando automaticamente i dati sul documento di riconoscimento.

   Si può rinunciare al controllo facciale dei presenti (controllo "faccia a faccia") con il confronto dei dati di identificazione ufficiali (carta d'identità, passaporto) se per il controllo dell'età viene utilizzata una procedura basata sulla determinazione automatizzata dell'età tramite telecamera. Il software formula dichiarazioni sulla probabilità dell'età della persona da identificare in base alle caratteristiche biometriche di un'immagine live della telecamera e raggiunge così il livello di affidabilità di un controllo dell'età personale

B. Raccolta e conservazione dei dati necessari per l'identificazione: I dati personali della persona da identificare necessari per la verifica dell'età dovrebbero essere registrati e conservati nella misura necessaria nel rispetto delle norme sulla protezione dei dati (ad es. data di nascita, nome, indirizzo).

C. Requisiti per i punti di raccolta: I dati identificativi possono essere raccolti su punti diversi (es. sportelli postali, punti vendita vari come negozi di operatori di telefonia mobile, punti lotterie, banche e casse di risparmio, ecc.). In alternativa all'inoltro dei dati al fornitore AVS è anche sufficiente trasmettere solo un riferimento ai dati registrati (luogo di memorizzazione, luogo concreto).

D. Controllo finale dell'età: L'accesso al gruppo chiuso di utenti (attivazione dei dati dell'utente per l'autenticazione) può avvenire solo se il fornitore AVS riceve i dati identificativi o un riferimento agli stessi e ne verifica l'età.

Infine, in merito all'**Autenticazione**, volta a garantire che solo la persona identificata e verificata l'età possa accedere a gruppi di utenti chiusi e a rendere più difficile il trasferimento delle autorizzazioni di accesso a terzi non autorizzati, i requisiti prevedono:

A. Effettuare l'autenticazione all'inizio di ogni processo di utilizzo ("sessione");

B. Protezione dei contenuti mediante una password speciale assegnata individualmente.

I.6 La consultazione pubblica del regolatore irlandese

La "Coimisiún na Meán" (di seguito Commissione) è l'ente regolatore irlandese per la radiodiffusione, i video on demand, la sicurezza online e i media sviluppo si occupa, tra gli altri, della definizione di standard, regole e codici per i diversi tipi di servizi media e relativi servizi online sotto la giurisdizione dell'Irlanda.

L'8 dicembre 2023 la Commissione ha avviato una consultazione pubblica[22] che prevede la proposta di un "Codice di Sicurezza Online" per i servizi e per i fornitori di piattaforme di condivisione video (di seguito "VSPS" o "fornitori VSPS").

Codice di Sicurezza Online proposto dalla Commissione irlandese

Uno dei compiti principali della Commissione è quello di sviluppare un codice di sicurezza online per i servizi forniti dalle piattaforme di condivisione video. Un VSPS è un tipo di servizio online in cui gli utenti possono condividere video e interagire con un'ampia gamma di contenuti e funzionalità social.

In conformità con i suoi poteri statutari e nel rispetto dei suoi doveri statutari, la Commissione ha predisposto una bozza di Codice di Sicurezza Online con lo scopo di garantire che i fornitori di VSPS adottino misure adeguate a proteggere i minori da contenuti dannosi, compresi quelli illegali e contenuti inappropriati per l'età. Si intende inoltre proteggere il pubblico in generale, dai contenuti quale incitamento alla violenza o all'odio, alla provocazione a commettere un reato terroristico, alla diffusione di materiale pedopornografico, reati di razzismo o xenofobia nonché alcuni spot pubblicitari comunicazioni.

Nell'ambito del Codice la Commissione ha specificato alcune definizioni importanti ad inquadrare il contesto in modo che gli obblighi previsti verso i fornitori di VSPS consentano di adottare misure

[22] Disponibile online https://www.cnam.ie/wp-content/uploads/2023/12/Draft_Online_Safety_Code_Consultation_Document_Final.pdf

efficaci per fornire adeguata protezione nei confronti dei possibili danni ai minori, come definiti dalla direttiva AVMS:

Tecniche di verifica dell'età

I fornitori di VSPS sono tenuti ad adottare misure efficaci di verifica o stima dell'età e a stabilire un meccanismo per valutarne l'efficacia.

In alcuni casi è necessaria una solida verifica dell'età (e un meccanismo equivalente per valutarne l'efficacia). I fornitori sono tenuti a riferire sull'efficacia dei meccanismi adottati. **La Commissione ritiene che il Codice debba fare riferimento all'efficacia dei metodi di verifica dell'età, piuttosto che specificarne le tecniche particolari da utilizzare.**

Ciò al fine di offrire ai fornitori VSPS una certa flessibilità nel progettare tecniche appropriate per il loro particolare servizio e nel modificarle man mano che la tecnologia si sviluppa. Inoltre, i fornitori devono essere trasparenti sulle tecniche di verifica dell'età che utilizzano e sui loro obiettivi per quanto riguarda la percentuale di minori che vengono erroneamente valutati come adulti.

Con riferimento alle **tecniche di verifica dell'età,** il Codice di Sicurezza Online elaborato dalla Commissione prevede che fornitori di servizi di piattaforme di condivisione video devono attuare misure efficaci per garantire che i contenuti classificati come non adatti ai bambini non possano normalmente essere visti dai bambini.

Tali misure verranno applicate al momento dell'iscrizione al servizio o a ogni accesso a tali contenuti e possono essere ottenute utilizzando la stima dell'età o la verifica dell'età, a seconda dei casi, o mediante altre misure tecniche.

L'autodichiarazione dell'età da parte degli utenti del servizio non costituisce di per sé una misura efficace.

In particolare, i fornitori di servizi di piattaforme di condivisione video il cui scopo principale del servizio o di una sua sezione è fornire agli adulti l'accesso a:

- contenuti costituiti da pornografia, o

- contenuti costituiti da rappresentazioni realistiche o degli effetti di violenza grave o gratuita o atti di crudeltà,

devono implementare tecniche di verifica approfondita dell'età sia per la registrazione dell'account al servizio o per l'accesso alla sezione del servizio che fornisce l'accesso a tali contenuti, sia ogni volta che si accede a tali contenuti.

In particolare, tali fornitori devono stabilire un meccanismo per descrivere la tecnica di verifica dell'età utilizzata, descrivere il modo in cui le misure vengono utilizzate per limitare l'accesso al/i servizio/i, fissare obiettivi per il numero di minori(in diverse fasce di età determinate dal fornitore di servizi) che vengono erroneamente identificati come adulti attraverso i meccanismi di verifica dell'età del fornitore di servizi e valutare l'accuratezza e l'efficacia dei solidi sistemi di verifica dell'età implementati.

Per quanto riguarda i dati personali il Codice prevede che i fornitori di servizi di piattaforme di condivisione video garantiscono che i dati personali dei minorenni raccolti o altrimenti generati da loro nell'attuazione degli obblighi relativi alla verifica dell'età non siano trattati per scopi commerciali, come marketing diretto, profilazione e pubblicità comportamentale mirata.

La verifica dell'età copre una serie di misure tecniche per stimare o verificare l'età dei bambini e degli utenti, tra cui:

- misure di progettazione tecnica;
- autodichiarazione;
- controllo dell'età mediante token tramite terze parti;
- Sistemi basati sull'intelligenza artificiale e sulla biometria;
- identificatori rigidi come i passaporti.

Il Codice richiede che siano utilizzate tecniche di verifica dell'età efficaci nel garantire che i minori non siano normalmente in grado di accedere ai servizi o alle sezioni degli stessi dedicati ai contenuti per adulti, e ad essere efficaci nel garantire che i minori non siano normalmente in grado di visualizzare contenuti per adulti su altri servizi.

Nessuna tecnica di verifica dell'età sarà efficace al 100%, ma gli operatori dovrebbero ridurre al minimo il tasso di errore quando i minori vengono erroneamente identificati come adulti. Il danno sarà maggiore se l'errore viene commesso nel caso di un minore nella prima adolescenza e minore se l'errore viene commesso nel caso di un minore prossimo all'età adulta.

Una verifica affidabile dell'età può includere la verifica dell'età **basata su documenti** al momento dell'iscrizione e la verifica dell'età **basata su selfie o somiglianza dal vivo** in base alla visualizzazione di video o sessione. **L'uso di un documento più un selfie dal vivo** al momento della registrazione dell'account sarebbe considerato una valida verifica dell'età; che anche altri metodi, come i selfie dal vivo e la biometria quando si accede ai contenuti, potrebbero essere considerati robusti, purché sia dimostrato che forniscono un livello di protezione equivalente.

I.7 Agenzia Spagnola per la protezione dei dati (AEPD) – age verification

L'agenzia ha definito un decalogo (https://www.aepd.es/guias/decalogue-principles-age-verification-minors-protection.pdf) di principi che i sistemi di verifica dell'età devono rispettare per proteggere i minori da contenuti inappropriati. L'obiettivo è garantire la protezione dei minori, rispettando i principi, i diritti e gli obblighi previsti dal GDPR. Il decalogo include i seguenti principi:

- Nessuna identificazione dell'utente e tracciamento dei minori
- Nessuna informazione sullo "status" di minore
- Garantire l'anonimato
- Verifiche applicabili solo a contenuti inappropriati
- Garantire l'accuratezza delle verifiche
- Nessuna profilazione dell'utente durante la navigazione
- Nessuna traccia e collegamenti delle attività svolte dagli utenti online
- Garantire i diritti fondamentali online
- Definire il framework della governance

Al fine di dimostrare che esistono soluzioni in grado di rispettare il Decalogo, e che queste soluzioni potrebbero essere offerte tramite Internet, l'Agenzia in collaborazione con il General Council of Professional Colleges of Computer Engineering, ha sviluppato delle Proof of Concept (PoC - prove di concetto) che implementano un sistema di verifica basato sul Decalogo. I risultati dimostrano che è possibile una chiara separazione tra gestione dell'identità, verifica dell'età e filtraggio dei contenuti.

Pertanto, si dimostra che i fornitori di identità che attualmente implementano il diritto all'identità personale dei cittadini spagnoli ed europei, sono già sufficienti e che non è necessario costruire sistemi di identità digitale paralleli per accedere a contenuti inappropriati per i minori.

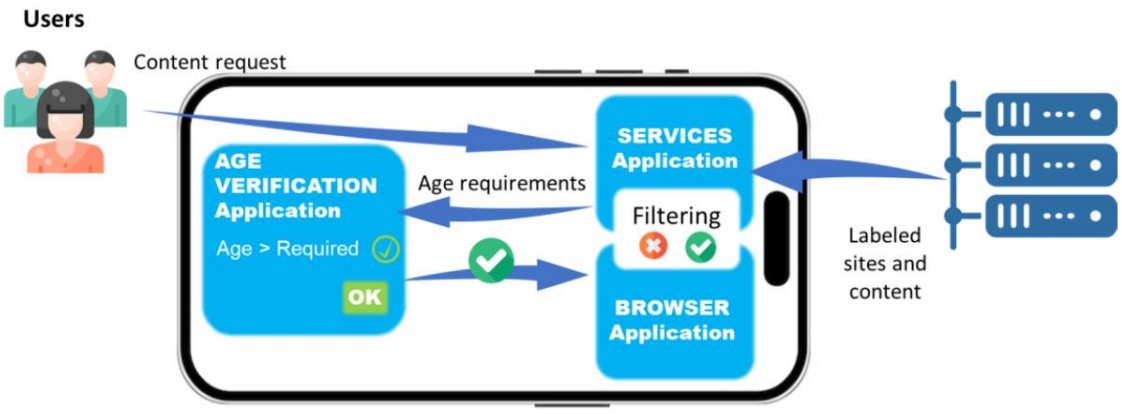
Le prove di concetto si basano anche sul fatto che la protezione contro i contenuti inappropriati può essere effettuata sul dispositivo dell'utente, con le persone che hanno il controllo completo sulla loro identità ed età in modo che i sistemi siano completamente verificabili e trasparenti.

Infine, i PoC dimostrano che la localizzazione, il monitoraggio e la profilazione dei minori su Internet (o degli utenti di Internet in generale) non sono necessari per attuare la protezione dai contenuti inappropriati.

Descrizione del sistema

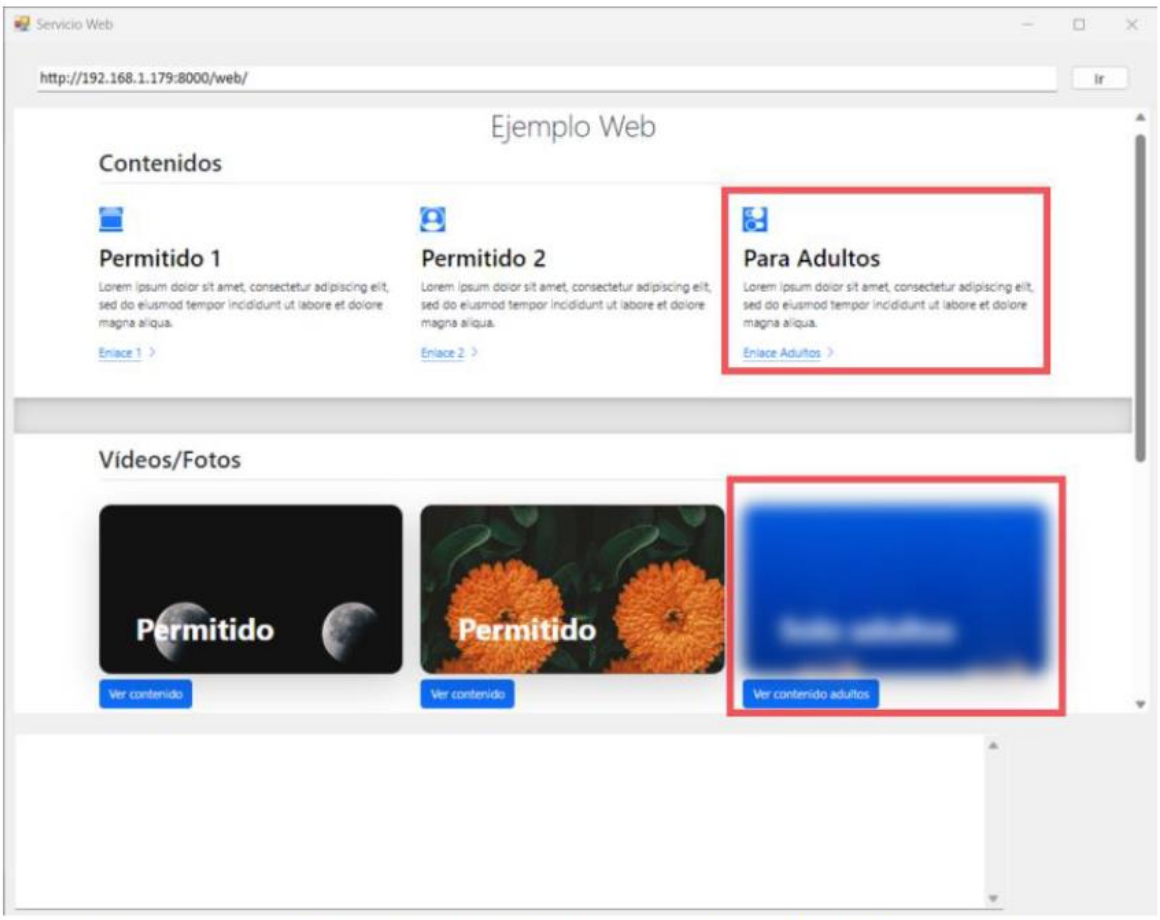
1. Tutti i contenuti sono classificati come “all audience”, “for adults”, “inappropriate for minors”. Negli ultimi due casi i contenuti sono mostrati dal browser internet o da un App di contenuti, solo a seguito della verifica dell’età.
2. Viene implementata un App di verifica dell’età installata sul device dell’utente. L’App di verifica dell’età riceve le richieste di cui al punto (1) ad esempio tramite QR Code mostrato da browaser internet oppure direttamente tramite il portafoglio digitale installato nel cellulare. L’App verifica l’età dell’utente e fornisce al browser l’autorizzazione all’accesso

Di seguito uno schema sintetico:



High-level description of the system implemented in the PoCs

Il browser maschera i contenuti web con etichetta ““for adults”, “inappropriate for minors” come mostrato nell’immagine seguente. Per accedervi viene richiesta la verifica dell’età.

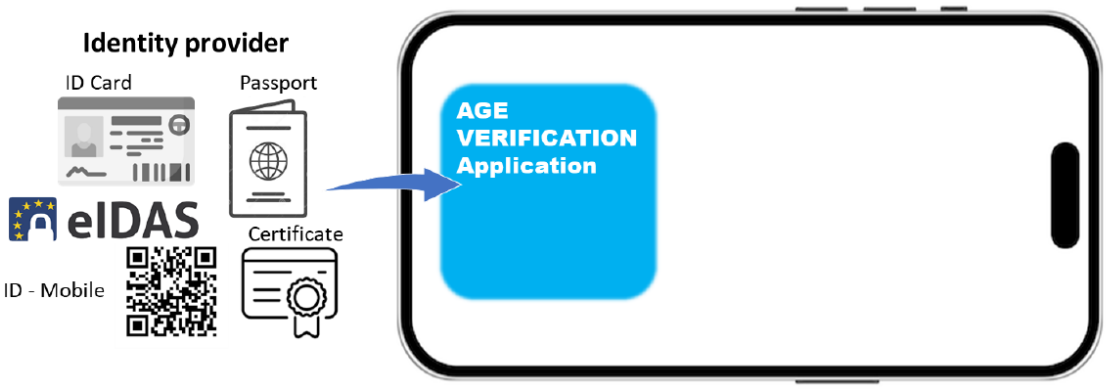


Browser that receives labeled content, but does not display it if it requires age verification

L'App di verifica dell'età funge da intermediario tra diversi provider di identità e l'applicazione che deve verificare l'età per consentire l'accesso a determinati contenuti (il browser, ad esempio oppure l'App del content provider).

I PoC sviluppati si basano sull'utilizzo di codici QR, identità digitali archiviate in portafogli elettronici o documenti di identità fisica. Entrambi i processi, la registrazione in un sistema di gestione dell'identità per utilizzare la verifica dell'identità e dell'età, sono considerati indipendenti.

L'app di verifica dell'età, eseguita solo sul dispositivo personale e fornita da un'entità selezionata dall'utente, impedisce la diffusione dell'identità. Ponendosi tra l'identità e la generazione della condizione "autorizzato all'accesso", questa app consente il controllo in modo che l'identità non venga mai rivelata ai fornitori di contenuti o a terzi.

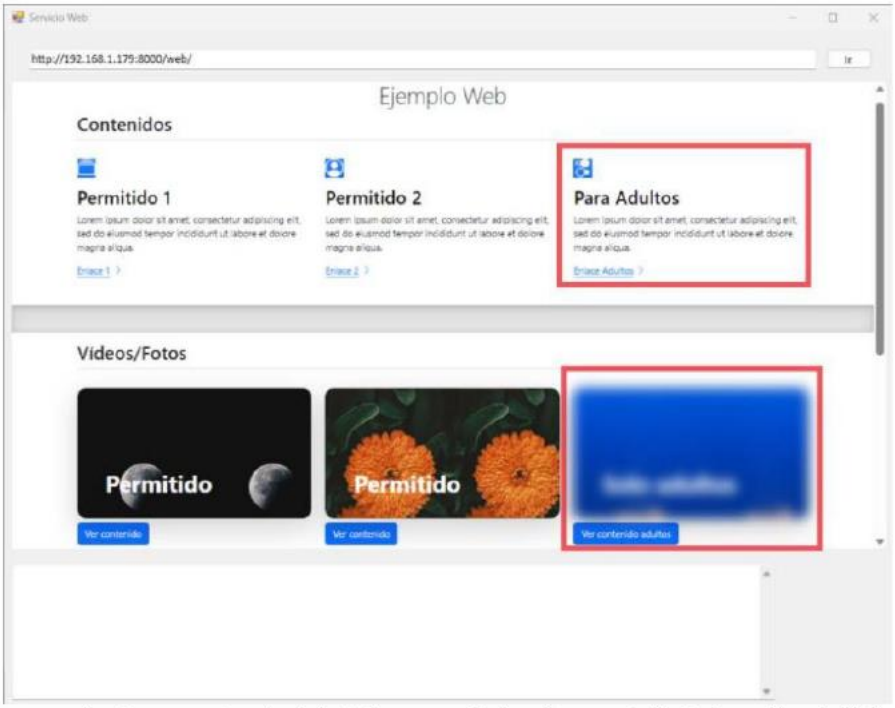


Identity management independent of age verification, which will therefore be anonymous

Esempio di accesso a contenuti dal computer:

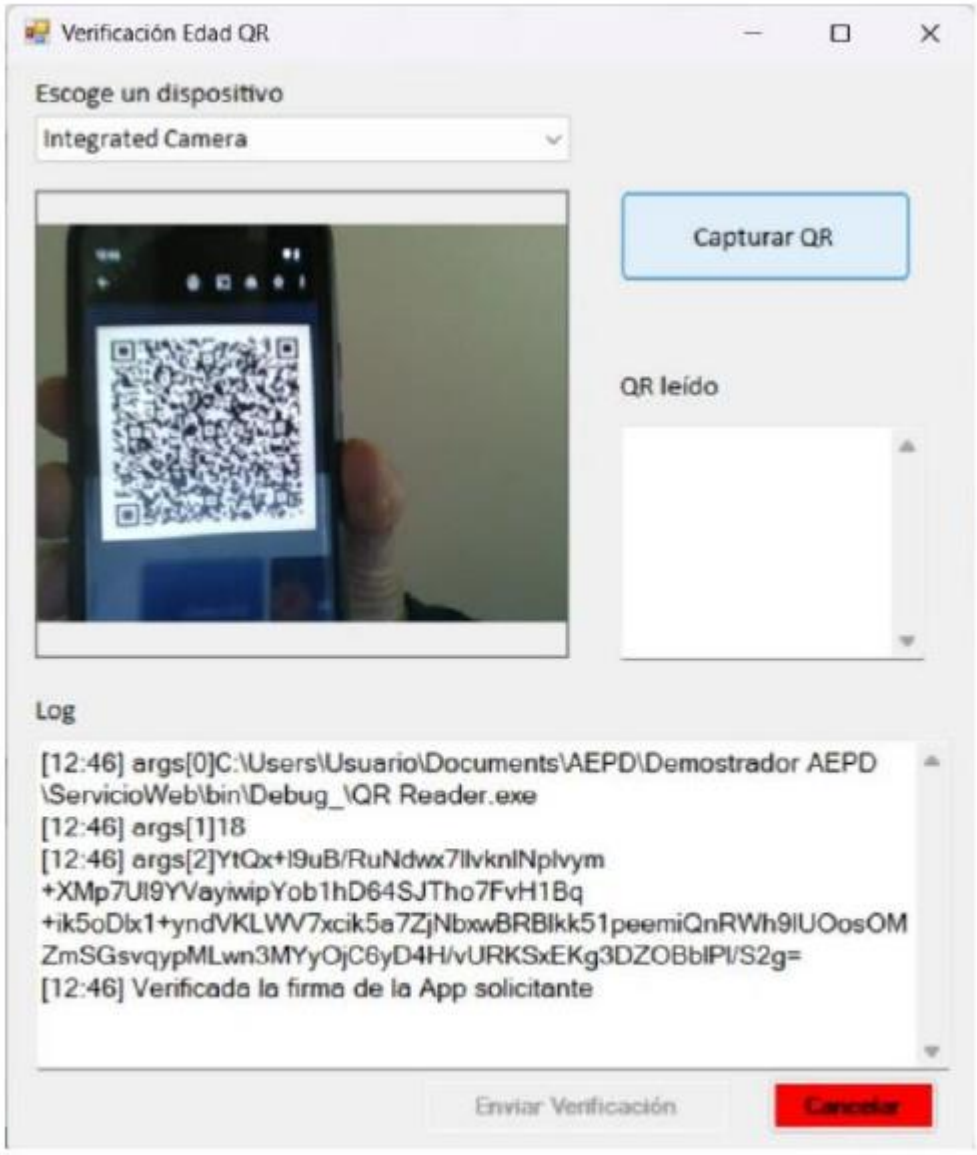
1. L'utente richiede l'accesso al contenuto etichettato “per adulti” dal browser.

2. Il contenuto viene ricevuto con la sua etichetta e la visualizzazione del contenuto sul dispositivo viene preventivamente bloccata (nel PoC il contenuto viene mostrato sfocato). In questo modo lo status di minore non viene rivelato al fornitore di contenuti, il contenuto viene sempre servito.



Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età

3. Il browser richiama l'applicazione di verifica per determinare se l'utente ha l'età appropriata per accedere al contenuto (oltre 14 anni, oltre 18 anni o altre condizioni). L'applicazione di verifica dell'età chiede all'utente di mostrare il proprio codice QR (sul proprio cellulare) vicino alla fotocamera del computer o della console.



Leggere e controllare il QR nell'applicazione di verifica dell'età

3. Si possono verificare due diverse situazioni:

- L'applicazione di verifica dell'età risponde con la condizione “autorizzato all'accesso”, senza rivelare informazioni sull'identità. Il browser rimuove il filtro,

  e l'accesso al contenuto è senza alcun tipo di restrizione.
- L'applicazione di verifica dell'età non risponde con la condizione “autorizzato all'accesso”. Infatti non risponde in alcun modo, quindi dopo un po' il browser smette di attendere una risposta e mantiene il filtro dei contenuti. Ciò può verificarsi perché la persona non ha l'età richiesta (ma non viene rivelato lo status di minorenne), o perché l'applicazione di verifica dell'età non è stata installata, o perché il suo utilizzo non è autorizzato, o il codice QR non è disponibile, o per qualsiasi altra circostanza.

Utilizzo del cellulare

1. L'utente richiede l'accesso al contenuto etichettato “per adulti” dal browser.

2. Il contenuto viene ricevuto con la sua etichetta e la visualizzazione del contenuto sul dispositivo viene preventivamente bloccata (nel PoC il contenuto viene mostrato sfocato). In questo modo lo status di minore non viene rivelato al fornitore di contenuti, il contenuto viene sempre servito.

Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età

4. Il browser richiama l'applicazione di verifica per determinare se l'utente ha l'età appropriata per accedere al contenuto (oltre 14 anni, oltre 18 anni o altre condizioni). L'applicazione di verifica dell'età utilizza le informazioni archiviate nel portafoglio digitale per effettuare i controlli necessari.

L'app di verifica dell'età riceve la richiesta dal browser e comunica con il portafoglio digitale

L'esito della verifica è lo stesso del caso precedente.

I.8 Osservazioni sull'uso di sistemi pubblici

Nell'ambito delle possibili soluzioni da implementare, ferma restando la necessità di preservare la libertà di valutazione e scelta della tecnologia da parte dei soggetti regolamentati, in relazione al possibile utilizzo di ID digitali forniti in ambito pubblico, come ad esempio SPID prospettato nel parere del Garante, si rappresenta quanto segue.

L'utilizzo di banche dati pubbliche o di un sistema di autenticazione come SPID potrebbe teoricamente consentire di dimostrare l'età per accedere a determinati siti o servizi *online*. Tuttavia, trattasi di un sistema nato per semplificare l'accesso ai servizi della PA. Laddove per il suo funzionamento fosse prevista la registrazione degli utilizzi sui server degli enti Statali e di società private, **lo stesso disporrebbe di un elenco di collegamenti di natura puramente privata e di presunti orientamenti sessuali.**

A titolo esemplificativo, il sistema SPID, ad esempio, non risulta, ai fini dell'attuazione delle disposizioni di cui all'art.13-*bis* della legge 13 novembre 2023, n. 123, **pienamente conforme alle specifiche tecniche AGCOM di seguito indicate (essenzialmente nella parte in cui è prescritto il c.d. doppio anonimato),** nel momento in cui si trasferisce all'*Identity Provider* la richiesta di autenticazione del *Service Provider*, che contiene il nome a dominio del sito visitato. Infatti, tale

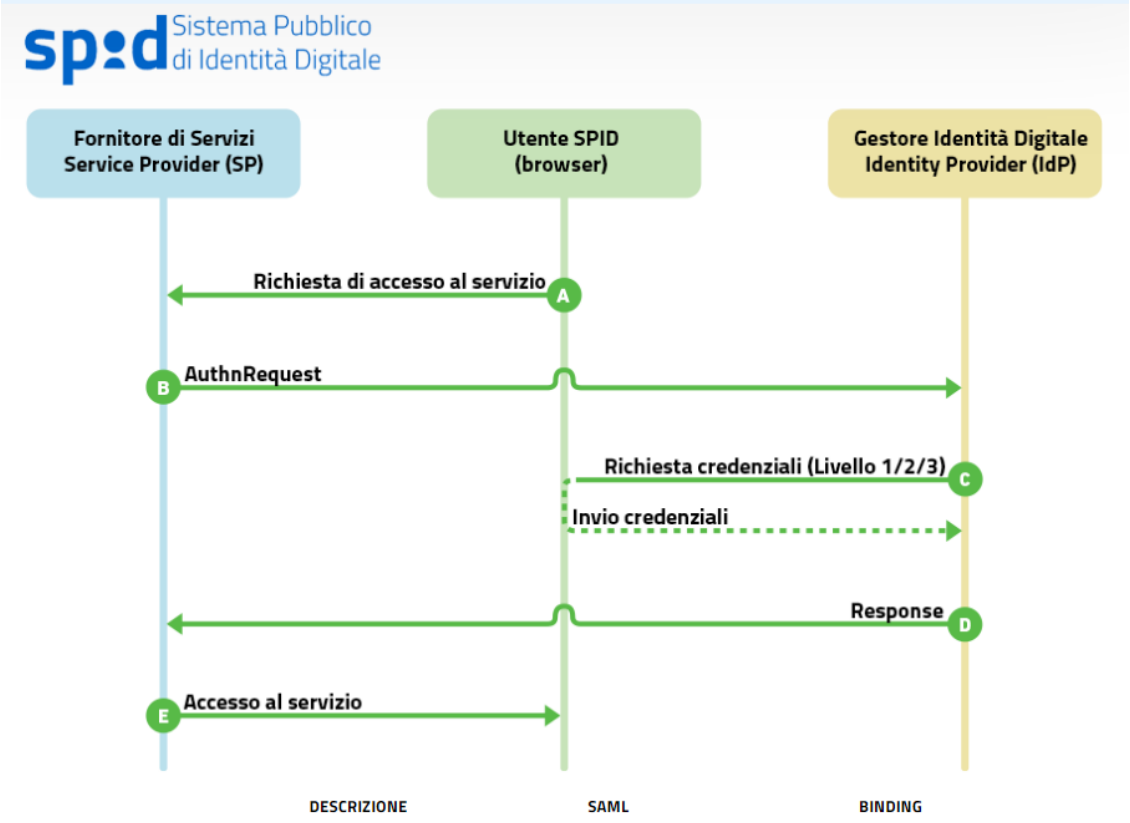
sistema di autenticazione SPID consente all'*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'*Identity Provider*.

La modalità di autenticazione *SPID Single Sign On - SP initiated redirect* consente il disaccoppiamento delle interazioni utente-*service_provider* e utente-*identity_provider.* In tal modo il *Service_provider* non comunica direttamente con l'*identity_provider*, ai fini dell'autenticazione, ma per il tramite dello *User_agent.*

Come illustrato nella documentazione tecnica della modalità *Single Sign On di SPID* [23] è previsto lo scambio di messaggi contenenti metadati dal *Service_provider* allo *User_agent* e dall'*Identity_provider* allo *User_agent*.

Il meccanismo di autenticazione è innescato dalla selezione, da parte dell'utente, del Gestore delle Identità con cui intende effettuare l'accesso; tale selezione avviene all'interno del sito del Fornitore di Servizi mediante un bottone ufficiale «Entra con SPID» da integrarsi nel servizio. Il Fornitore di Servizi prepara di conseguenza una **<AuthnRequest>** da inoltrarsi al Gestore delle Identità, dove l'utente viene reindirizzato per effettuare l'autenticazione. Eseguita l'autenticazione, l'utente torna presso il sito del Fornitore di Servizi con un'asserzione firmata dal Gestore delle Identity contenente gli attributi richiesti (ad es. nome, cognome, codice fiscale) che il Fornitore di Servizi può usare per autorizzare l'utente in base alle proprie *policy* ed erogare il servizio richiesto.

Di seguito uno schema che rappresenta il flusso delle interazioni sopra descritte.



[23] disponibile al'url https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#esempio-di-authnrequest

Il messaggio ***<AuthnRequest>*** è quindi inviato dal *Service Provider*, per tramite dello User Agent, al *SingleSignOnService* dell'Identity Provider ha la funzione di avviare il flusso di autenticazione. Può essere inoltrato da un Service Provider all'*Identity Provider* usando il *binding HTTP-Redirect* o il *binding HTTP-POST*.

Dalla documentazione pubblicata da AGID si evince che tale messaggio ***<AuthnRequest>*** contiene al suo interno l'attributo *"AssertionConsumerServiceURL"* che indica l'URL del *Service Provider* **ossia l'indirizzo del sito visitato dall'utente,** a cui inviare il messaggio di risposta alla richiesta di autenticazione (l'indirizzo deve coincidere con quello del servizio riportato dall'elemento <AssertionConsumingService> presente nei metadata del Service Provider)[24].

Pertanto, tale sistema di autenticazione SPID consente all'*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'*Identity Provider*.

Nella figura seguente è mostrato, più nel dettaglio, il flusso dei messaggi descritti poi in tabella.

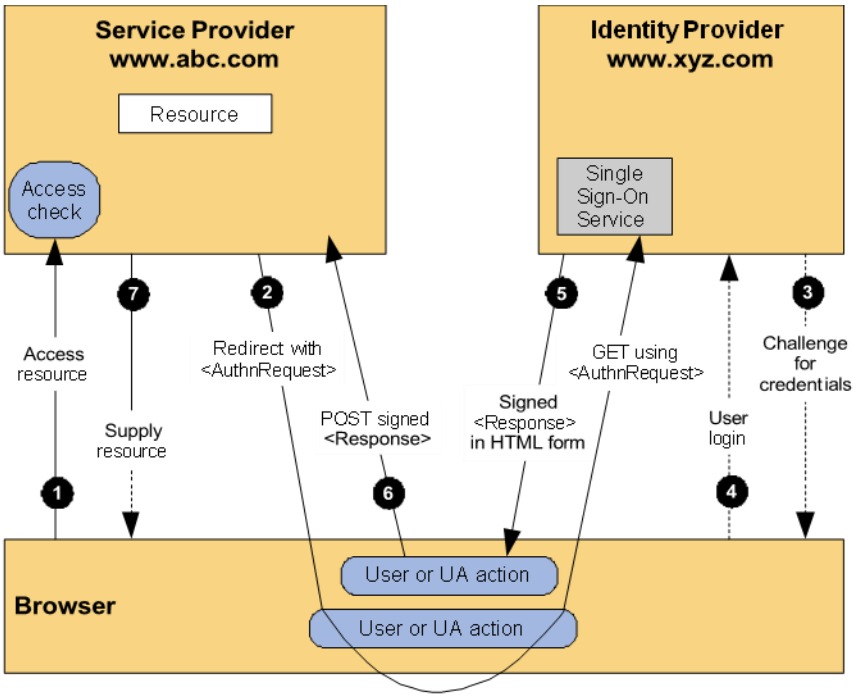


Figura 1 - SSO SP-Initiated Redirect/POST binding

	Descrizione	SAML	Binding
1	Il fruitore utilizzando il browser (User Agent) richiede l'accesso alla risorsa		
2a	Il Service Provider (SP) invia allo User Agent (UA) una richiesta di autenticazione da far pervenire all'Identity Provider (IdP).	AuthnRequest	HTTP Redirect HTTP POST

[24] La risposta inviata dall'Identity Provider al Service Provider può essere trasmessa solo tramite il binding HTTP-POST e deve contenere, in base a dette specifiche, l'attributo Destination, a indicare l'indirizzo (URI reference) del Service Provider a cui è inviata la risposta.

2b	Lo User Agent inoltra la richiesta di autenticazione contattando l'Identity Provider.	AuthnRequest	HTTP Redirect HTTP POST
3	L'Identity Provider esamina la richiesta ricevuta e se necessario esegue una challenge di autenticazione con l'utente.	-	HTTP
4	L'Identity Provider portata a buon fine l'autenticazione effettua lo user login e prepara l'asserzione contenente lo statement di autenticazione dell'utente destinato al Service Provider (più eventuali statement di attributo emessi dall'Identity Provider stesso).	-	-
5	L'Identity Provider restituisce allo User Agent la <Response> SAML contenente l'asserzione preparata al punto precedente.	Response	HTTP POST
6	Lo User Agent inoltra al Service Provider (SP) la <Response> SAML emessa dall'Identity Provider.	Response	HTTP POST

Tabella 1 - SSO SP-Initiated Redirect/POST binding

Si osserva che il passaggio 2b della soprastante tabella non appare conforme alle specifiche tecniche AGCOM (doppio anonimato), di seguito indicate, nel momento in cui si trasferisce all'*Identity Provider* la richiesta di autenticazione del *Service Provider*, che contiene il nome a dominio del sito visitato.

L'Autorità, pertanto, solo laddove soddisfatti i requisiti di cui al regolamento in Allegato A sul doppio anonimato (protezione dei dati personali nei confronti del sito/piattaforma e non conoscenza del sito visitato/piattaforma da parte dell'Identity Provider), ritiene che sistemi pubblici siano utilizzabili.