AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Allegato B alla delibera n. 61/24/CONS

CONSULTAZIONE PUBBLICA DI CUI AL COMMA 4 DELLA DELIBERA N. 9/24/CONS PER L'APPROVAZIONE DI UN PROVVEDIMENTO CHE DISCIPLINA LE MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI AI SENSI DELLA LEGGE 13 NOVEMBRE 2023, N. 159

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.

Facial age estimation
world leading accuracy results

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. **YouTub**e 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).

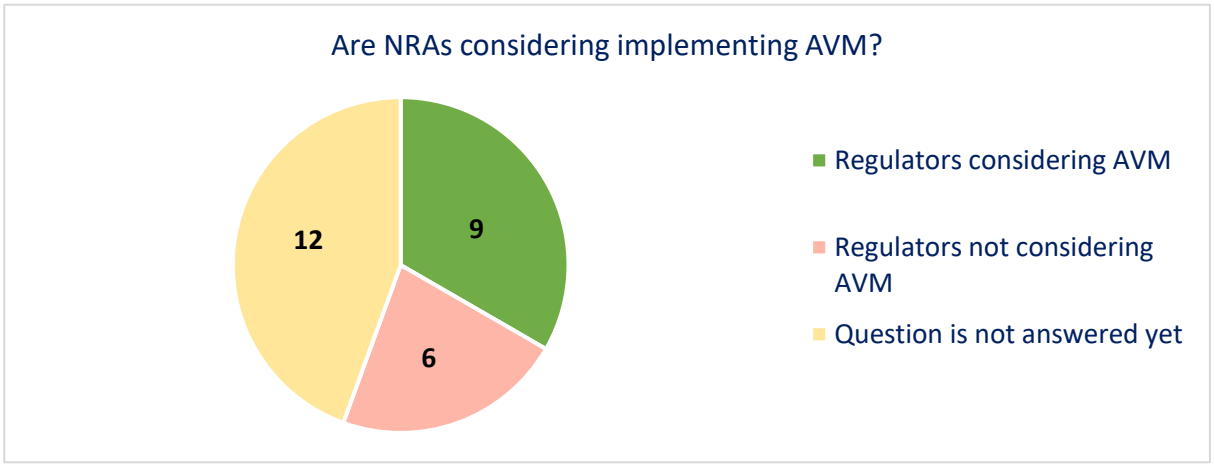
Anche l'ERGA riconosce che identificare e implementare meccanismi efficienti per impedire ai bambini di accedere a contenuti dannosi, e in particolare a contenuti pornografici, solleva una serie di sfide, sia in termini di efficienza (poiché alcuni di questi meccanismi possono essere facilmente aggirati) 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).

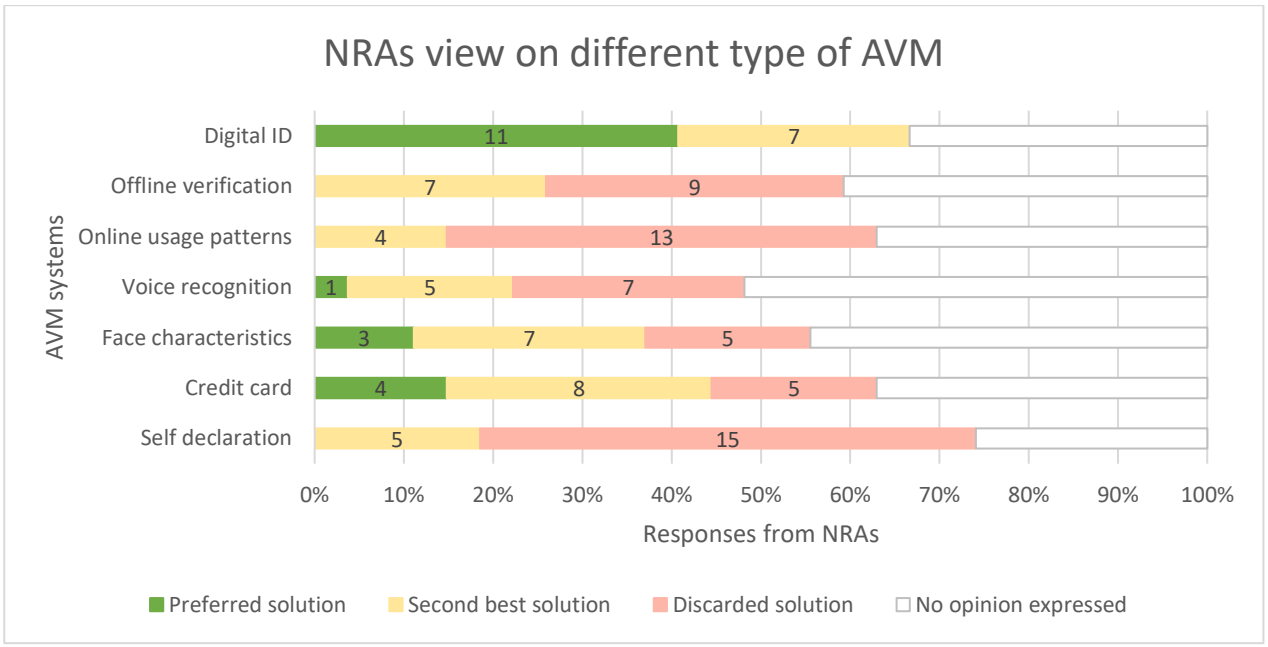
Avuto particolare riguardo alla implementazione di meccanismi di verifica dell'età negli stati membri dell'ERGA per limitare l'accesso dei minori ai contenuti pornografici, 12 ANR hanno risposto di non avere ancora una specifica posizione.

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

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), 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:

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.*

In aggiunta, in base al comma 7 dell'art.42 del TUSMA:

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;

[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.

Più recentemente 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* (di seguito DSA) 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. Inoltre, all'articolo 35, paragrafo 1, lettera j), del DSA, prevede che i fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi adottano misure di attenuazione dei rischi sistemici, tra cui *"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"*

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, nonchè 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.*

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 dovrà, in esito alla consultazione, acquisire 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.

Attività in ambito EU:

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.

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.

III. 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.

IV. Valutazioni dell'Autorità sulle modalità tecniche e di processo che i soggetti indicati dal Decreto sono tenuti ad adottare a garanzia della maggiore età degli utenti

Di seguito si riportano le analisi e le valutazioni dell'Autorità in merito ai requisiti che i sistemi di verifica dell'età degli utenti che accedono a contenuti nocivi devono rispettare e rispetto ai quali si chiede ai soggetti interessati di inviare un proprio contributo.

DEFINIZIONI

L'Autorità ritiene preliminarmente opportuno, anche in considerazione delle attività, seppur preliminari, svolte in ambito comunitario, tener conto delle seguenti definizioni utili ai fini delle valutazioni di seguito svolte. Si intenderà, pertanto, nel seguito per:

Garanzia dell'età (di seguito anche ***Age assurance*****)** l'insieme dei metodi, sistemi e processi 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**.

Autodichiarazione (di seguito anche *Self-desclaration*) si riferisce all'insieme di processi in cui un utente inserisce una data o seleziona una casella di un form, anche online, per dichiarare di essere sopra/sotto una determinata età, senza fornire altre prove.

Stima dell'età (di seguito anche ***Age estimation*****)** si riferisce ai metodi che stabiliscono che con una certa probabilità 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 o con altri utenti della stessa età, metriche derivate dall'analisi dei movimenti del corpo, il riconoscimento facciale, o l'analisi delle capacità o conoscenze. Nei metodi utilizzati per una stima dell'età rientrano anche quelli effettuati mediante algoritmi e il ricorso a tecnologie basate sull'intelligenza artificiale.

Verifica dell'età (di seguito anche ***Age verification*****)** fa riferimento a quei sistemi che si basano su identificatori rigidi (fisici) e/o fonti di identificazione verificate, che forniscono un elevato grado di certezza nel determinare l'età di un utente.

Servizio regolamentato: la diffusione e/o la pubblicazione, in Italia, di immagini e video a carattere pornografico tramite siti web e VSP soggetta all'obbligo di verifica dell'età dell'utente. La definizione è generalizzabile nel caso in cui il sistema di garanzia dell'età si intenda applicato anche a ulteriori tipologie di contenuti riservati ad utenti maggiorenni.

Soggetto regolamentato: i gestori di siti web e i fornitori delle piattaforme di condivisione video che distribuiscono in Italia immagini e video a carattere pornografico da considerarsi soggette all'obbligo di verifica dell'età. Questa definizione è generalizzabile laddove il sistema di garanzia venga adottato anche da fornitori di ulteriori contenuti riservati a utenti maggiorenni.

Domanda n. 1: Si richiede ai rispondenti di fornire proprie considerazioni in relazione alle definizioni riportate, specificando se sia necessario o meno aggiungerne altre al fine di inquadrare al meglio la tematica.

REQUISITI GENERALI E INDICATORI DI PERFORMANCE DEI SISTEMI DI AGE ASSURANCE

L'Autorità ritiene ragionevole seguire un approccio che sia tecnologicamente neutrale, che lasci ai soggetti tenuti alla realizzazione dei processi di *age assurance* una ragionevole libertà di valutazione e scelta, stabilendo tuttavia i principi e requisiti che devono essere soddisfatti dai sistemi messi in campo.

L'Autorità ritiene, anche alla luce delle preliminari analisi svolte, principalmente in ambito comunitario, che un sistema funzionale per l'"assicurazione dell'età" debba rispettare una serie di **requisiti generali** di seguito descritti

i. **Proporzionalità:**

- Trattasi di un requisito generale, di carattere primario, che fa riferimento alla ricerca del giusto equilibrio tra i mezzi utilizzati per raggiungere l'obiettivo prefissato, nel caso di specie la verifica dell'età, e il suo impatto sulla limitazione dei diritti delle persone. Il soggetto tenuto, ai sensi della legge, a realizzare il sistema di controllo dell'età per l'accesso ai contenuti, mediante *age assurance*, deve utilizzare uno strumento per quanto possibile non invasivo per raggiungere l'obiettivo prefissato.
- In base al principio di *accountobility* di cui agli artt. 5(2) e 24 del Regolamento (UE) 20761679 ("GDPR"), è opportuno che siano i "soggetti regolamentati" a scegliere gli strumenti di verifica dell'età da implementare nel proprio servizio e a dimostrare l'efficacia dello strumento utilizzato secondo i principi e requisiti fissati dall'Autorità, nonché la conformità del medesimo strumento ai principi e alle regole in materia di protezione dei dati, in particolare, quello di proporzionalità. ln tale contesto il documento propone di considerare anche l'impatto dello strumento utilizzato sui "diritti delle persone" da considerare come diritti e libertà fondamentali.

Domanda n. 2: Si ritiene opportuno che ciascun soggetto regolamentato decida in merito ai sistemi di verifica dell'età da implementare nel proprio servizio secondo i principi e requisiti fissati dall'Autorità?
Domanda n. 3: Si richiede ai rispondenti di fornire proprie valutazioni in merito al principio di proporzionalità e di come reputano che questo possa essere applicato ai sistemi di *age assurance*.

ii. **Protezione dei dati personali:**

- Il sistema deve essere conforme alle norme e principi di protezione dei dati stabiliti dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 - GDPR (minimizzazione dei dati, accuratezza, limitazione della conservazione, ecc.). Il metodo prescelto per la verifica dell'età dovrà essere, in particolare, rispettoso del principio di minimizzazione dei dati (art. 5 del GDPR) e dei principi di data protection by design e by default (art. 25 del GDPR).
- I processi di verifica dell'età comportano il trattamento e la gestione di dati personali come, ad esempio, i dati riportati sui documenti di identità, l'immagine fotografica dell'utente, le informazioni del titolare della carta di credito, etc. Pertanto, al fine di garantire la protezione della privacy degli utenti, i soggetti regolamentati che implementano i processi di verifica dell'età devono assicurare che il trattamento dei dati personali avvenga nel rispetto degli obblighi previsti dal GDPR, fornendo opportuna informativa agli utenti e assicurando che siano raccolti solo ed esclusivamente i dati personali necessari in ragione dello scopo.
- L'Autorità osserva che la logica del *controllo parentale*, di cui alla delibera n. 9/23/CONS, che limita l'accesso ai contenuti mediante strumenti di filtro a livello di rete e applicativi, limita l'accesso ai contenuti sensibili senza richiedere la fornitura di dati sensibili.
- L'Autorità osserva inoltre che, rispetto al tema della privacy, appaiono risultare suscettibili di attente riflessioni e cautele quei sistemi che si basano su:

- raccolta diretta di documenti di identità da parte dell'editore del sito pornografico;
- stima dell'età basata sulla cronologia di navigazione dell'utente Internet sul web;
- trattamento di dati biometrici al fine di identificare o autenticare 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),
- utilizzo di ID digitali come lo SPID forniti in ambito pubblico; l'utilizzo di banche dati pubbliche o di un sistema di autenticazione come lo 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 è prevista la registrazione degli utilizzi sui server degli enti Statali, lo stesso disporrebbe di un elenco di collegamenti di natura puramente privata e di presunti orientamenti orientamento sessuale.

Domanda n. 4: Si richiede ai rispondenti di fornire proprie valutazioni in relazione alle tematiche connesse alla privacy, anche avuto riguardo all'elenco di sistemi oggi usati per la *age assurance* e descritti in questo documento.

iii. **Intervento di soggetti terzi indipendenti:**

- Si è rilevato che la verifica dell'età per un utilizzo ripetuto in genere consiste in due passaggi: identificazione una tantum e autenticazione 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 processo gli può consentire l'accesso a un numero qualsiasi di offerte diverse.
- Pertanto, un processo di verifica dell'età, in grado di fornire un certo grado di tutela dei dati personali, si potrebbe dividere in pratica in tre fasi distinte:
  - in primo luogo, l'emissione di una "prova dell'età", con un certo livello di confidenza, a **seguito della identificazione.** 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 ha identificato l'utente di Internet in un altro contesto (un commerciante – es. tabacchi nel modello "scratch card" -, una banca, un'amministrazione, ecc.). Il soggetto che fornisce la "prova dell'età" non è conoscenza dell'utilizzo che l'utente ne farà.

    L'Autorità ritiene opportuno che i siti e le piattaforme soggette 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. Quindi il soggetto che fornisce un servizio di *age assurance*, secondo il processo di cui sopra, dovrà essere indipendente dal fornitore dei contenuti (sito web o piattaforma di video sharing) per le ragioni che seguono.

    Il ricorso a un soggetto terzo indipendente fidato (o certificato) evita la trasmissione diretta di dati identificativi dell'utente al sito o alla piattaforma che offre contenuti pornografici. Affidare queste funzioni a soggetti diversi rende possibile una massima tutela dei dati personali grazie ad un processo che garantisca la compartimentazione degli attori ossia tra utente, fornitore del contenuto e soggetto che certifica la maggiore età.

- In secondo luogo, la fornitura di tale prova certificata dell'età all'utente o direttamente al sito o alla piattaforma visitata affinché questi dia accesso o meno al contenuto richiesto. Il provider del sito o della piattaforma non viene in possesso di dati sulla identità dell'utente. Il caso in cui il soggetto che fornisce la "prova dell'età" la trasmette direttamente al sito o piattaforma, comporta che lo stesso soggetto che rilascia la prova dell'età sarà a conoscenza del particolare sito o piattaforma visitate dall'utente. Pertanto, il modello che prevede la comunicazione della prova dell'età solo all'utente che poi la presenterà al sito o piattaforma visitata, fornisce la massima garanzia per la protezione dei dati. Infatti, in questo caso, il soggetto che rilascia la prova dell'età non conosce il particolare sito o piattaforma che vuole visitare l'utente e al tempo stesso il sito o piattaforma visitata non conoscerà l'identità dell'utente. Inoltre, nel caso in cui il soggetto che si occupa di fornire la "prova dell'età" sia un privato non già soggetto a specifici obblighi di legge in materia di identificazione, come ad esempio un fornitore di servizi di "age assurance", è opportuno che questo sia certificato da un'apposita Autorità al fine di avere garanzie sul sistema di identificazione usato.
- un terzo passo, implementato dal sito o dalla piattaforma visitata dall'utente, consiste nell'analizzare la prova dell'età presentata e fornire o meno l'accesso al contenuto richiesto (**autenticazione**).

- Di seguito un esempio del processo suddetto:

1) il soggetto che fornisce la "prova dell'età", ad esempio una banca, un operatore telefonico, un ente pubblico o soggetto privato (anche un commerciante) presso cui l'utente è stato identificato con certezza per altri servizi o ai fini dell'accesso a contenuti e servizi per adulti, conosce l'identità dell'internauta ma non conosce quale sito/servizio online sta consultando;
2) su richiesta dell'utente, il soggetto terzo fornisce "la prova dell'età" (sorta di certificazione) che viene consegnata all'utente (nel caso, ad esempio, di scratch card), o inviata all'utente (nel caso di processo telematico). Tale "prova dell'età" non contiene alcun dato che identifica l'utente o che consente di ricondurre all'utente. Ad esempio, nel caso di fornitura telematica della "prova d'età", è possibile ipotizzare sistemi di certificazione a chiave pubblica e privata per gestire la certificazione e la verifica come di seguito descritto[6]:
    a) il sito o piattaforma video richiede all'utente di verificare la sua età e invia un file denominato "età da provare". Tale file non contiene nessun riferimento al sito o contenuto a cui l'utente vuole fare accesso.
    b) l'utente richiede al soggetto terzo di fornire la prova dell'età certificando il file denominato "età da provare". Il soggetto terzo certifica il file crittografandolo con chiave privata e generando così un file denominato "prova dell'età". Tale certificazione non contiene nessun dato sull'identità dell'utente.
    c) l'utente invia il file "prova dell'età" al sito o piattaforma a cui vuole accedere. Il sito o piattaforma applica la decrittografia con chiave pubblica per risalire al

[6] La crittografia asimmetrica è una forma di sistema crittografico in cui due chiavi diverse eseguono la crittografia e la decrittografia. Queste due chiavi sono la chiave pubblica e la chiave privata. Ogni partecipante ha una coppia di chiavi pubbliche e private. La chiave pubblica è accessibile a tutti gli altri partecipanti. Tuttavia, la chiave privata è accessibile solo dal suo proprietario. Il mittente utilizza la chiave pubblica del destinatario per crittografare il messaggio. Quando un messaggio raggiunge il destinatario, utilizza la sua chiave privata per decifrare il messaggio.

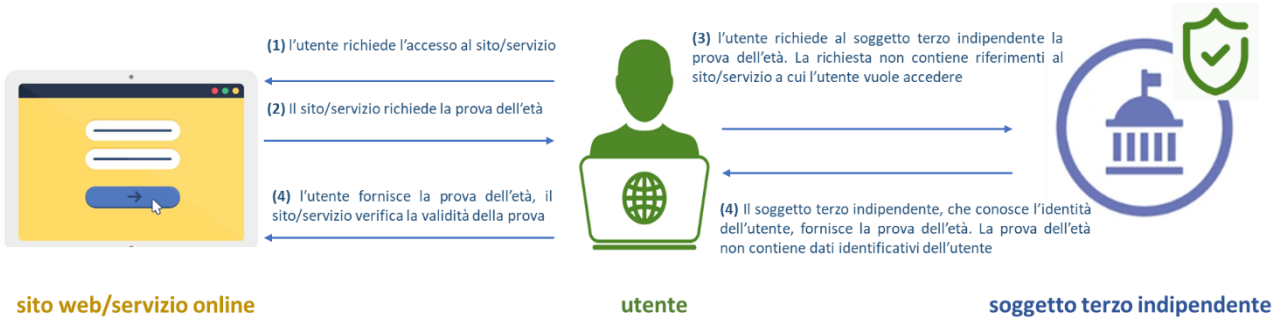
contenuto del file, dopodiché verifica che il contenuto sia coerente con quello inizialmente inviato all'utente.

Tale applicazione presuppone l'esistenza di una Certification Authority che si occupa di generare, condividere, revocare e gestire i certificati e le chiavi di crittografia.

In un processo meno tutelato rispetto alla privacy il soggetto che fornisce la "prova dell'età" può trasmetterla direttamente al sito o alla VSP (nello schema che segue è indicato solo il primo caso);

3) il sito web o il servizio online ottiene una prova dell'età dell'utente (o solo della sua maggiore età) e, pur conoscendo necessariamente il particolare sito/servizio online consultato dall'utente, non ha alcuna informazione circa la sua identità. Nel caso meno garantista la "prova dell'età" è fornita al sito o VSP dal soggetto che ha svolto l'identificazione (in questo caso quest'ultimo è a conoscenza dei siti o piattaforme visitati).

- L'Autorità ritiene opportuno valutare l'opportunità che i fornitori di prove dell'età, quanto non già soggetti a obblighi normativi di identificazione degli utenti, siano soggetti a una valutazione da parte di terzi (ossia che siano quindi in qualche misura certificati).



Domanda n. 5: Si chiede ai rispondenti una valutazione specifica in merito al principio di indipendenza del fornitore dei servizi di *age assurance*.
Domanda n. 6: Si chiede ai rispondenti di descrivere possibili proposte in merito all'implementazione di servizi di *age assurance* basati su soggetti terzi indipendenti, nel rispetto del processo sopra descritto che prevede l'acquisizione di una "prova dell'età".

iv. **Sicurezza:**

- Il sistema di *age assurance* deve tener conto di possibili attacchi informatici rispetto ai quali deve prevedere misure di sicurezza informatica sufficienti a mitigare i rischi (GDPR, proposta Cyber Resilience Act - CRA) e a evitare i tentativi di elusione.

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 *age assurance* 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; occorre prevedere sistemi per ridurre i tentativi di elusione da parte di bot o processi automatizzati; per la valutazione 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.

(c) La possibilità per un individuo di eludere il sistema; ad esempio, un minorenne potrebbe presentare un'immagine di un documento d'identità che non gli appartiene, un documento falsificato (ad esempio una patente di guida falsa, un passaporto falsificato o una registrazione falsificata in una banca dati) o utilizzare, nei casi di riconoscimento facciale, immagini fisse o video; occorre pertanto prevedere tecniche per stabilire la vitalità (liveness) di un individuo. Diventa importante, pertanto, un sistema di rilevamento della cosiddetta liveness, ad esempio come definita dalla norma ISO/IEC 30107;

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

Altre tipologie di attacco possono verificarsi 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;

Per quanto riguarda i dispositivi attualmente offerti sul mercato, diversi regolatori evidenziano che attualmente tutte le soluzioni proposte possono essere in qualche modo aggirate. Ad esempio, l'utilizzo di una VPN, che nasce per garantire sicurezza nell'utilizzo di Internet agli utenti, può allo stesso tempo consentire a un minore di eludere un sistema di verifica dell'età. Il soggetto tenuto, ai sensi della legge, a realizzare il sistema di controllo dell'età per l'accesso ai contenuti, non deve promuovere o fare comunque riferimento a qualsiasi meccanismo di elusione dei sistemi di *age assurance*.

I soggetti regolamentati devono richiedere la verifica dell'età dell'utente quando questo accede al sito/piattaforma oppure prima che il contenuto nocivo per il minore sia visibile. La richiesta di verifica dell'età deve essere ripetuta con frequenza periodica almeno pari, ad esempio, a 3 mesi.

Domanda n. 7: Si chiede ai rispondenti una valutazione specifica in merito al requisito di sicurezza, riportando, ove disponibili, informazioni o prove sulla portata del rischio di sicurezza e/o elusione che interessa i diversi metodi di *age assurance*.
Domanda n. 8: Si chiede ai rispondenti di descrivere possibili ulteriori proposte per mitigare i rischi relativi alla sicurezza e ai metodi di elusione dei sistemi di *age assurance*.
Domanda n. 9: Quali aspetti specifici relativi alle procedure di accesso ai siti web/piattaforme, alla tipologia di utente, alla durata della sessione o alla durata dell'accesso ai contenuti regolamentati dovrebbero essere presi in considerazione nell'implementazione dei sistemi di verifica dell'età?
Domanda n. 10: Con quale frequenza si ritiene che il sistema di assicurazione dell'età debba richiedere il rinnovo della richiesta all'utente?

v. **Precisione ed efficacia:**

- Il sistema di *age assurance* deve essere efficacie in termini di contenimento dell'errore nella determinazione dell'età sia in ambiente di test che in condizioni reali di funzionamento. Il grado di efficacia può essere determinato sulla base di determinati parametri quali, ad esempio, nel caso di sistemi basati sulla stima, l'errore medio, la deviazione standard; in

generale in termini di tasso di Errati OK, cioè il tasso dei falsi positivi, nel consentire l'accesso (inteso come la probabilità che il sistema ammetta l'accesso ai contenuti vietati a un minorenne).

Un parametro utilizzato in alcuni studi è l'errore medio assoluto (una misura della differenza media tra l'età effettiva e quella prevista) che deve rientrare nelle tolleranze accettabili.

Il meccanismo di verifica dell'età deve determinare correttamente l'età di un utente in condizioni operative reali, impreviste o reali, garantendo performance adeguate rispetto ai dati ottenuti in laboratorio. Ad esempio, i meccanismi di verifica dell'età devono garantire adeguate performance rispetto a condizioni che modificano la qualità o le caratteristiche dell'input, ad esempio una scarsa illuminazione, sfocatura, luminosità, contrasto o posizionamento dell'utente nell'immagine (per metodi che si basano su un'immagine fotografica del viso, o sulla foto del documento di identità, etc.) o anche risoluzione della videocamera.

Il meccanismo di verifica dell'età deve fornire prestazioni che non variano nel tempo. Ciò potrebbe avvenire nel caso di sistemi basati sulla AI, laddove i dati e le caratteristiche demografiche della popolazione possono cambiare nel tempo determinando un maggiore grado di varianza del meccanismo di verifica dell'età. Ciò a causa del fatto che i dati su cui è stato addestrato il meccanismo diventano meno rappresentativi della popolazione che effettivamente lo utilizza. Tale elemento richiede un continuo monitoraggio del grado di accuratezza del meccanismo utilizzato, apportando le necessarie correzioni.

- La verifica dell'età basata su Autodichiarazione non viene considerata un metodo efficace per determinare correttamente l'età di un utente.
- Il sistema di verifica dell'età dovrebbe risultare neutrale o indipendente dal dispositivo di accesso o dal sistema operativo utilizzato dall'utente.

Domanda n. 11: Si chiede, a tale proposito, ai rispondenti se l'Autorità debba fissare delle metriche relative alla precisione e all'efficacia e se, per ciascuna di esse, debba fissare delle soglie.
Domanda n. 12: Si ritiene che sia più appropriato per la tutela dei minori che il sistema di verifica dell'età sia neutrale o indipendente dal dispositivo di accesso o dal sistema operativo utilizzato o, al contrario, ritiene che vi siano differenze significative in questi elementi che potrebbero consigliare un sistema di verifica dell'età adattato a ciascun dispositivo di accesso o sistema operativo?

vi. **Funzionalità, facilità d'uso e non ostacolo all'accesso ai contenuti in Internet:**

- I sistemi di assicurazione dell'età dovrebbero essere facili da usare e basati sulle capacità e caratteristiche dei minori. La verifica dell'età non dovrebbe limitare l'accesso a Internet ma piuttosto favorirlo, non determinando inutili ostacoli alla fruizione dei servizi e dei contenuti.
- Per accessibilità si intende il criterio secondo cui il sistema di verifica dell'età sia facile da utilizzare per tutti gli utenti, indipendentemente dalle loro caratteristiche (età, genere, etnia, lingua etc.), dal loro livello di informatizzazione o dal fatto che appartengono a un determinato gruppo. Pertanto, i soggetti regolamentati devono garantire che il sistema implementato sia facile da usare e non impedisca indebitamente agli adulti di accedere a contenuti legali. Ciò potrebbe accadere, ad esempio, se il meccanismo risulta troppo difficile da utilizzare, inducendo quindi gli utenti ad abbandonare il processo di verifica e quindi il sito web o la

piattaforma di condivisione video. Inoltre, occorre valutare il potenziale impatto che il sistema, o i sistemi di verifica dell'età implementati possono avere sull'utilizzo da parte di utenti affetti da disabilità, garantendo, ad esempio, che vi sia la possibilità di utilizzare i lettori di schermo per completare con successo il processo di verifica. Infine, sarebbe opportuno rendere disponibili più soluzioni per la verifica dell'età, dando la possibilità agli utenti di scegliere quale utilizzare in base alle proprie caratteristiche e necessità.

Domanda n. 13: Si ritiene che vi siano ulteriori elementi che l'Autorità dovrebbe considerare in merito al criterio di funzionalità, facilità d'uso e non ostacolo all'accesso ai contenuti in Internet previsto per i sistemi di *age assurance*?

vii. **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 il processo di assicurazione dell'età.
- Il criterio in questione fa riferimento alla capacità del sistema di verifica dell'età di evitare o minimizzare pregiudizi non intenzionali e risultati discriminatori nei confronti degli utenti. Pertanto, ove applicabile, i soggetti regolamentati devono garantire che i meccanismi di verifica dell'età siano stati addestrati su diversi dataset, al fine di evitare che vi siano risultati discriminatori per determinati gruppi di utenti, ad esempio un grado inferiore di precisione tecnica per gli utenti di una determinata etnia quando il meccanismo si basa sulla stima dell'età del volto, o anche per evitare che gli utenti minorenni vengano erroneamente identificati come utenti adulti, o che utenti maggiorenni vengano erroneamente identificati come minori.

Domanda n. 14: Si ritiene che vi siano ulteriori elementi che l'Autorità dovrebbe considerare in merito al criterio di inclusività e non discriminazione previsto per i sistemi di *age assurance*?

viii. **Trasparenza:**

- I soggetti economici regolamentati dovrebbero essere trasparenti con gli utenti per quanto riguarda i sistemi e i dati utilizzati e trattati, mediante spiegazioni semplici, chiare e complete oltre che per maggiorenni anche per i minorenni.
- I soggetti economici regolamentati devono rendere disponibili sui propri siti web, i dati relativi alla precisione e all'efficacia dei sistemi di *age assurance* utilizzati, riportando le metriche e i parametri impiegati nella valutazione nonché i risultati ottenuti.

Domanda n. 15: Si ritiene che vi siano ulteriori elementi che l'Autorità dovrebbe considerare in merito al criterio di trasparenza?

ix. **Formazione e informazione:**

- L'Autorità ritiene importante informare e sensibilizzare i minori, i genitori, il personale della comunità educativa e della gestione giovanile sulle buone pratiche informatiche, sui rischi

connessi a Internet. Le attività connesse alla implementazione del Parental control hanno evidenziato la centralità di tale aspetto.

Domanda n. 16: Quali canali di formazione e informazione si ritengono utili impiegare per promuovere l'importanza della verifica dell'età, sensibilizzare sulle buone pratiche informatiche e nei confronti dei pericoli e i rischi connessi a Internet?

x. **Gestione dei reclami:**

- Il fornitore dei servizi di *age assurance* deve prevedere un canale per acquisire e gestire, tempestivamente, i reclami in caso di errate decisioni sull'età.

Domanda n. 17: Con riferimento ai suddetti principi si chiede ai rispondenti di fornire specifiche valutazione. Si chiede in particolare una valutazione sull'ammissibilità, tra le tipologie di processi e sistemi, di sistemi che determinano l'età in modo probabilistico, come l'analisi dei comportamenti o il riconoscimento facciale.
Domanda n. 18: Si richiede ai rispondenti di valutare ulteriori principi che l'Autorità dovrebbe prendere in considerazione per i sistemi di *age assurance*.
Domanda n. 19: Con riferimento ai sistemi di verifica dell'età oggi in uso e analizzati in questo documento nell'ambito delle analisi in ambito europeo e nelle consultazioni degli altri Paesi si chiede di indicare, con ordine decrescente di congruità, quali metodologie si ritengono, quantomeno in via provvisoria, applicabili avuto riguardo ai principi sopra enunciati.

OSSERVAZIONI SULL'AMBITO DI APPLICAZIONE

Il presente documento essendo rivolto a dare attuazione all'art. 13-bis, comma 3, della legge 13 novembre 2023, n. 159 si concentra sui servizi che diffondono contenuti a carattere pornografico e, quindi, sui soggetti che hanno come scopo quello di diffondere o pubblicare contenuti a carattere pornografico.

Al riguardo, con il provvedimento n. 88 dell'8 febbraio 2024 con cui il Garante per la protezione dei dati personali, esaminata la bozza di provvedimento previamente trasmessa dall'Autorità, ha espresso parere favorevole all'avvio della consultazione pubblica; sono state altresì formulate delle osservazioni a titolo di collaborazione istituzionale che l'Autorità ha ritenuto opportuno prendere in considerazione nella versione finale del testo che si sottopone a consultazione pubblica.

Tra le osservazioni emerge anche quella secondo cui, la normativa vigente – anche specificamente riferita al ruolo dell'Autorità - richiama più volte l'esigenza di implementare meccanismi di *age verification* stabilendo che i minori hanno diritto ad un livello più elevato di protezione dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale, anche introducendo misure più rigorose nei confronti di ogni servizio della società dell'informazione.

Rileva, a tale proposito, che la Commissione europea sostiene e promuove l'attuazione di norme mirate alla tutela dei minori online e che l'art. 28 del DSA, 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. Inoltre, si osserva che, ai sensi dell'articolo 35, paragrafo 1, lettera j), del DSA i fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca *online* di dimensioni molto grandi adottano misure di attenuazione dei rischi sistemici, tra cui "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".

Va inoltre preso in considerazione quanto previsto dall'art. 8 del GDPR.

Rilevano, inoltre, i poteri specificamente assegnati all'Autorità dagli articoli 41 e 42 del TUSMA, quali, in particolare il comma 7 dell'art. 41 laddove prevede che:

7. 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;.*

Inoltre, i commi 1 e 6 dell'art. 42 prevedono che:

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.***

In base al comma 7 dell'art.42 del TUSMA:

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 tale quadro normativo è peraltro influenzato il documento che si sottopone a consultazione pubblica che, in varie parti, fa riferimenti più ampi all'esigenza di protezione dei minori, come ad es.:

- vi "Funzionalità, facilità d'uso e non ostacolo all'accesso ai contenuti in Internet" laddove si specifica che "i sistemi di assicurazione dell'età dovrebbero essere facili da usare e basati sulle capacità e caratteristiche dei minori. La verifica dell'età non dovrebbe limitare l'accesso a Internet ma piuttosto favorirlo, non determinando inutili ostacoli alla fruizione dei servizi e contenuti";

- vii "inclusività e non discriminazione" laddove si specifica che "le differenze tra i bambini in termini di lingua, abilità, status socioeconomico, ecc. dovrebbero essere prese in considerazione durante il processo di assicurazione dell'età";

- ix "Formazione e informazione" laddove si specifica che l'Autorità ritiene importante informare e sensibilizzare i minori, i genitori, il personale della comunità educativa e della gestione giovanile sulle buone pratiche informatiche, sui rischi connessi a Internet.

L'Autorità ritiene pertanto opportuno valutare, nell'ambito della consultazione pubblica di cui si dispone l'avvio, se il sistema di verifica dell'età delineato nel documento posto in consultazione mediante l'indicazione di requisiti generali e di indicatori di *performance* sia efficace, idoneo e funzionale a trovare applicazione, ai sensi del contesto normativo da ultimo richiamato, anche con riferimento ad ulteriori tipologie di contenuti che potrebbero nuocere allo sviluppo fisico, mentale o morale dei minori.

Domanda n. 20: Ciò considerato, si ritiene che il sistema di garanzia dell'età delineato nel presente documento sia funzionale a trovare applicazione, ai sensi del contesto normativo vigente, anche con riferimento ad ulteriori tipologie di contenuti che potrebbero nuocere allo sviluppo fisico, mentale o morale dei minori?

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[7].

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:

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

[7] 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.

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.

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.

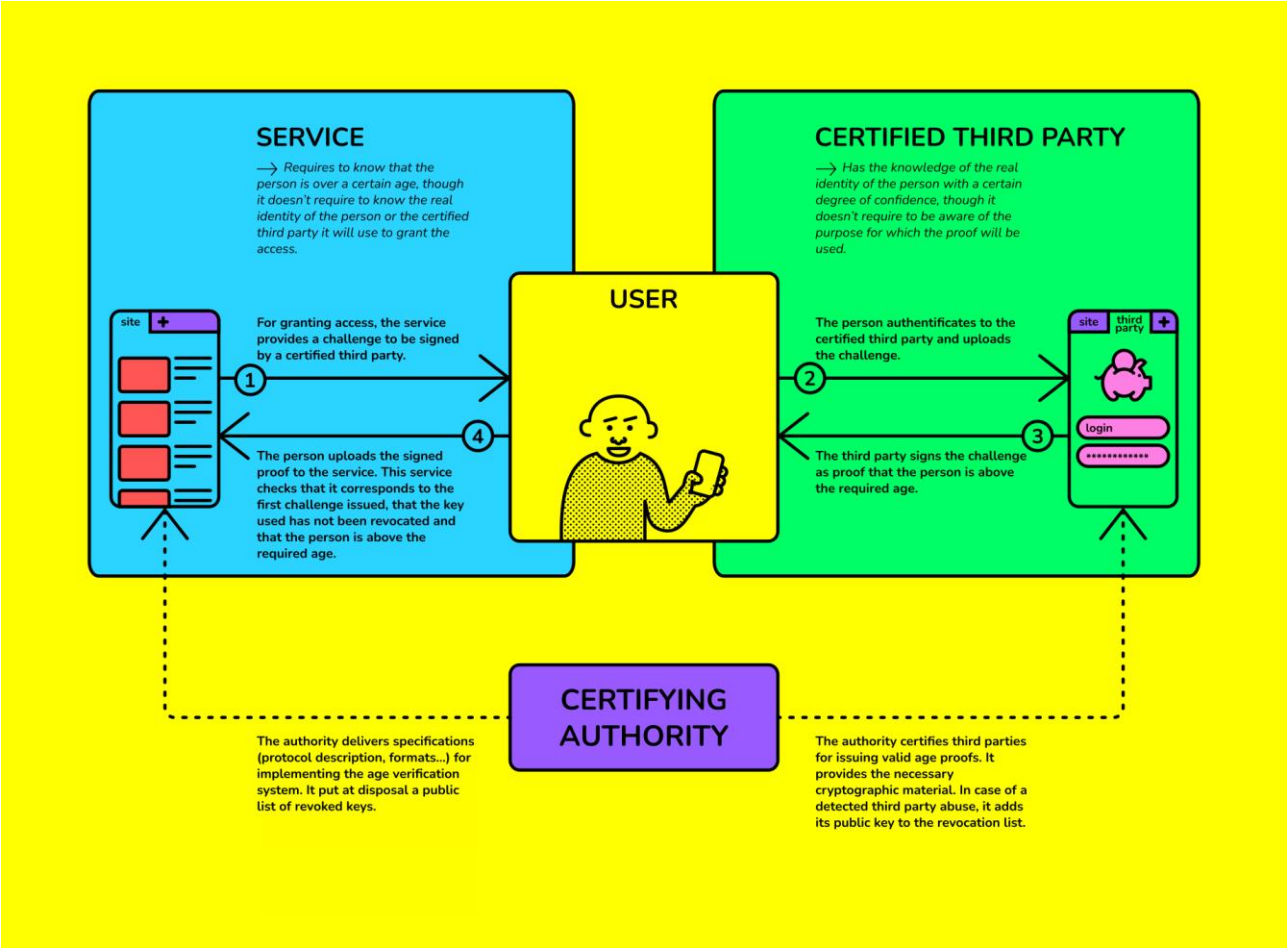
Prerequisiti: è necessario avvalersi di soggetti terzi di fiducia che colleghino i servizi di gestione degli attributi ai sistemi di identità dello Stato.

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 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.

I.5 La regolamentazione tedesca

L'autorità di regolamentazione tedesca Kommission für Jugendmedienschutz (KJM) nel mese di maggio 2022 ha stabilito criteri[8] per la valutazione dei sistemi di verifica dell'età.

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

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

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"[9].

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 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.

[9] 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

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[10] 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 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.

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

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.