AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

**Allegato A alla delibera n. 96/25/CONS**

# MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI AI FINI DELL'ACCESSO A DETERMINATI SERVIZI FORNITI DAI GESTORI DI SITI WEB E DALLE PIATTAFORME DI CONDIVISIONE DI VIDEO CHE DIFFONDONO IN ITALIA IMMAGINI E VIDEO A CARATTERE PORNOGRAFICO, AI SENSI DELL'ARTICOLO 13 BIS DEL DECRETO LEGGE 5 SETTEMBRE 2023, N. 123 CONVERTITO CON MODIFICAZIONI DALLA LEGGE 13 NOVEMBRE 2023, N. 159

Il presente provvedimento specifica le modalità tecniche e di processo che determinati gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, sono tenuti ad adottare a garanzia della maggiore età degli utenti.

Lo scopo del provvedimento non è quello di certificare soluzioni tecniche, bensì quello di predisporre un quadro dei requisiti tecnici minimi, conforme al quadro giuridico europeo sui servizi online, con il fine specifico di proteggere i minori online dai contenuti a carattere pornografico che possano nuocere alla loro salute e al loro sviluppo fisico, mentale e morale.

Il provvedimento può essere rivisto e aggiornato al fine di tenere conto dello stato dell'arte e, in particolare, al fine di assicurare piena conformità agli orientamenti adottati dalla Commissione europea ai sensi dell'articolo 28 del Regolamento (UE) 2022/2065. Pertanto, il presente provvedimento costituisce una soluzione transitoria come indicato all'articolo 4 del presente provvedimento.

## Art. 1

## INDIVIDUAZIONE DEI SOGGETTI CHE RENDONO DISPONIBILI AL PUBBLICO CONTENUTI A CARATTERE PORNOGRAFICO E AMBITO DI APPLICAZIONE DELLE MODALITÀ TECNICHE E DI PROCESSO PER L'ACCERTAMENTO DELLA MAGGIORE ETÀ DEGLI UTENTI

1. Il presente provvedimento, adottato in attuazione dell'art. 13-bis, comma 3, del Decreto, si applica ai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, stabiliti in Italia o stabiliti in un altro Stato membro. Detti soggetti sono individuati in una lista compilata e aggiornata dall'Autorità, nonché comunicata dalla stessa alla Commissione europea.

2. Al fine di stabilire se un contenuto diffuso da un fornitore stabilito in un altro Stato membro sia diretto al pubblico italiano deve essere soddisfatto almeno uno dei seguenti criteri:

a) l'utilizzo *prevalente* della lingua italiana all'interno del servizio online, da valutare in relazione alla presenza di elementi testuali realizzati in lingua italiana nell'interfaccia utente, nonché alla disponibilità della funzione multilingua che includa la lingua italiana;

b) il raggiungimento da parte del servizio online di un significativo numero medio di utenti unici mensili sul territorio italiano sulla base dei dati forniti da organismi dotati della massima rappresentatività dell'intero settore di riferimento, anche alla luce dei processi di convergenza multimediale, la cui organizzazione risponda altresì a princìpi di terzietà, autonomia e indipendenza;

c) il conseguimento da parte del fornitore del servizio di piattaforma per la condivisione di video di ricavi realizzati in Italia, anche se contabilizzati nei bilanci di società aventi sede all'estero Tali servizi sono individuati in un elenco/lista compilata e aggiornata dall'Autorità che ne cura anche la comunicazione alla Commissione europea;

d) il servizio è promosso o commercializzato anche per gli utenti italiani;

e) il servizio ha un dominio in Italia o fornisce un indirizzo di contatto e/o un numero di telefono in Italia.

3. Qualora sussistano le condizioni di cui al paragrafo 4 dell'articolo 3 della Direttiva 2000/31/CE, l'ambito di applicazione di cui al comma 1 è esteso anche ai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, stabiliti in un altro Stato membro, individuati caso per caso dall'Autorità in conformità alla normativa europea e alla procedura prevista dal citato articolo 3 ai paragrafi 4 e 5.

4. L'Autorità ritiene che le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti che si adottano con il presente provvedimento siano altamente raccomandate, in quanto efficaci, idonee, proporzionali e funzionali, per il loro stesso utilizzo anche da parte di altri soggetti rispetto a quelli indicati nella lista di cui al comma 1 e con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori quali ad esempio le categorie previste dalla delibera 9/23/CONS.

## Art. 2

## DEFINIZIONI

**Decreto:** il Decreto-legge 123/2023 come convertito dalla legge 13 novembre 2023, n. 159.

**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 **l'autodichiarazione, la verifica dell'età e** la **stima dell'età**.

**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.

**Prova dell'età**: oggetto di tipo fisico (es. scratch card) o digitale (es. documento elettronico, file, stringa alfanumerica, transazione elettronica, etc.) che consente di stabilire, sulla base di processi e protocolli codificati e riconosciuti tra le parti, la maggiore età dell'utente che lo utilizza.

**Indicatori di performance**: parametri qualitativi e quantitativi che permettano di misurare l'efficacia di un sistema di *age assurance* 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 specifici indicatori quali, ad esempio, nel caso di sistemi basati sulla stima, *l'errore medio*, la *deviazione standard*, il 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 altro indicatore di performance 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.

## Art. 3

## REQUISITI, SPECIFICHE TECNICHE E INDICATORI DI PERFORMANCE DEI SISTEMI DI *AGE ASSURANCE*

1. L'Autorità adotta un approccio che sia tecnologicamente neutrale, che lasci ai soggetti tenuti alla realizzazione dei processi di *age assurance*, individuati ai sensi dell'articolo 1, una ragionevole libertà di valutazione e scelta, stabilendo tuttavia i principi e requisiti di riferimento.

2. Visti gli esiti della consultazione pubblica e considerato il parere del Garante per la protezione dei dati personali, alla luce delle analisi svolte, anche in ambito europeo, l'Autorità stabilisce che un sistema funzionale per fornire la "Garanzia dell'età" deve rispettare i **requisiti e le specifiche di processo e di sistema** 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. I soggetti di cui all'articolo 1 del presente provvedimento devono utilizzare uno strumento per quanto possibile non invasivo per raggiungere l'obiettivo prefissato.
- In base al principio di *accountability* di cui agli artt. 5(2) e 24 del Regolamento (UE) 20761679 ("GDPR"), è opportuno che siano i soggetti di cui all'articolo 1 a scegliere gli strumenti di garanzia 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 considera anche l'impatto dello strumento utilizzato sui "diritti delle persone" da considerare come diritti e libertà fondamentali.

ii. **Protezione dei dati personali:**

- I sistemi di *age assurance* implementati devono essere conformi 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.). I metodi prescelti per la verifica dell'età dovranno essere, in particolare, rispettosi 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 garanzia 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 di cui all'articolo 1 del presente provvedimento che implementano i processi di garanzia 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.
- 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.
- I soggetti di cui all'articolo 1 del presente provvedimento e le terze parti coinvolte nel processo di garanzia dell'età e nei processi ad esso correlati (es. manutenzione dei sistemi, gestione o fatturazione del servizio, etc.) non devono effettuare alcuna profilazione degli utenti e, in particolare, i meccanismi di garanzia dell'età implementati non devono consentire ai soggetti interessati di raccogliere l'identità, l'età, la data di nascita o altre informazioni di carattere personale degli utenti.
- L'Autorità non ritiene conformi, rispetto al tema della privacy, 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*).

**Visto il parere del Garante per la protezione dei dati personali e le relative considerazioni in relazione al possibile utilizzo di ID digitali forniti in ambito pubblico**, nell'ambito delle possibili soluzioni da implementare e ferma restando la necessità di preservare la libertà di valutazione e scelta della tecnologia da parte dei soggetti di cui all'articolo 1 del presente provvedimento, si rappresenta quanto segue.

L'utilizzo di banche dati pubbliche o di un sistema di autenticazione potrebbe teoricamente risultare conforme alle modalità tecniche e di processo qui indicate solo a condizione che per il suo funzionamento non fosse prevista la registrazione degli utilizzi sui server degli enti Statali e di società private, non essendo consentita **la messa a disposizione di tali soggetti di un elenco di collegamenti di natura puramente privata e di presunti orientamenti sessuali.**

Come illustrato nella sezione I.8 dell'Allegato B al presente provvedimento, il sistema SPID, ad esempio, non risulta, ai fini dell'attuazione delle disposizioni di cui all'art.13-*bis* della legge 13 novembre 2023, n. 123, **pienamente conforme alle specifiche tecniche AGCOM di seguito**

**indicate (essenzialmente nella parte in cui è prescritto il c.d. doppio anonimato),** nel momento in cui si trasferisce all'*Identity Provider* la richiesta di autenticazione del *Service Provider*, che contiene il nome a dominio del sito visitato. Infatti, tale sistema di autenticazione SPID consente all'*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'*Identity Provider*[1].

Rispetto al livello di protezione dei propri dati personali adeguato al rischio e, in generale, assicurare che il processo di verifica e di autenticazione sia conforme alla normativa in materia di protezione dei dati personali, giova comunque evidenziare l'utilità dei livelli di sicurezza offerti dai Gestori dell'identità digitale, che, va ricordato, sono soggetti terzi essi stessi (sia nei riguardi del soggetto regolamentato, sia rispetto a "Enti statali" e gestori di "banche dati pubbliche") e in possesso di determinati requisiti soggettivi e oggettivi stabiliti dalla normativa di settore, selezionati sulla base di specifiche procedure di qualificazione e sottoposti a vigilanza da parte dell'Agenzia per l'Italia Digitale (AGID)[2].

Si evidenzia, pertanto, la possibilità, con un sistema pubblico, di poter disporre in breve tempo di un insieme di *Identity Provider* certificati e di una rete di connessioni e accordi (basati su obblighi normativi esistenti), in grado di fornire, all'utente e per il tramite di questo alla piattaforma, la cosiddetta prova dell'età.

Quanto detto vale sia per la modalità di verifica dell'età collegate a sistemi di verifica dell'età non basati su applicativi installati nel terminale utente sia per quelli basati su applicativi installati nel terminale utente (cosiddetti *digital wallet*), fermo restando la necessità di preservare la libertà di scelta dell'utente in merito all'utilizzo di uno o dell'altro sistema, anche considerando la potenziale invasività dell'installazione di determinate app sul proprio dispositivo personale.

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

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

I seguenti criteri costituiscono una base minima di requisiti applicabili a tutti i sistemi di verifica dell'età coperti dal presente provvedimento.

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

Il fornitore di sistemi di verifica dell'età deve essere giuridicamente e tecnicamente indipendente dai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico contemplato dal presente provvedimento; deve altresì garantire che i soggetti mirati interessati che diffondono contenuti pornografici, non abbiano in nessun caso accesso ai dati utilizzati per verificare l'età dell'utente.

---

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

Nella documentazione tecnica della modalità *Single Sign On di SPID* (disponibile al'url https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#esempio-di-authnrequest) è tuttavia previsto lo scambio di messaggi contenenti **metadati** dal *Service_provider* allo *User_agent* e dall'*Identity_provider* allo *User_agent*, tra i quali l'URL del Service Provider ossia l'indirizzo del sito visitato dall'utente, a cui inviare il messaggio di risposta alla richiesta di autenticazione.

[2] Ad esempio, solo per la componente di "certificazione" il sistema SPID è basato, fin dall'origine, su un processo di accreditamento e vigilanza dei soggetti che la svolgono.

**Riservatezza per quanto riguarda i servizi che diffondono contenuti pornografici**

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

In particolare, l'implementazione di soluzioni di verifica dell'età non deve consentire ai soggetti mirati interessati di raccogliere l'identità, l'età, la data di nascita o altre informazioni di carattere personale di tali utenti.

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

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

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

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

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

Un sistema di verifica dell'età che utilizza il "doppio anonimato", ossia basato sull'intervento di un soggetto terzo indipendente (sezione seguente iii), non deve consentire ai soggetti mirati interessati di riconoscere un utente che ha già utilizzato il sistema sulla base dei dati generati dal processo di verifica dell'età.

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

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

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

Il requisito della *Riservatezza rafforzata*, che si aggiunge a quello della *Riservatezza*[3] di cui sopra, prevede un sistema di verifica dell'età che utilizzi il modello del "doppio anonimato", in cui non si deve consentire ai fornitori di prove dell'età di sapere per quale servizio viene eseguita la verifica dell'età. In particolare, nel processo di verifica dell'età che utilizza il "doppio anonimato", ai soggetti che forniscono la prova dell'età non deve essere comunicata l'informazione relativa al sito web/piattaforma a cui l'utente vuole accedere.

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

Un sistema di verifica dell'età che utilizza il "doppio anonimato" non deve consentire a nessun altro soggetto terzo coinvolto nel processo di riconoscere un utente che ha già utilizzato il sistema. Ad

[3] Si ricorda che il requisito della *Riservatezza*, per quanto riguarda i servizi che diffondono contenuti pornografici, prevede che i dati personali, che consentono all'utente di verificare la propria età con un servizio oggetto del presente regolamento, non devono essere trattati. In particolare, l'implementazione di soluzioni di verifica dell'età non deve consentire ai servizi oggetto del regolamento di raccogliere l'identità, l'età, la data di nascita o altre informazioni di carattere personale di tali utenti.

esempio, un soggetto terzo che assicura la trasmissione della prova dell'età o ne certifica la validità non deve poter sapere se ha già elaborato la prova dello stesso utente.

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

In linea generale l'Autorità ritiene conforme alle presenti specifiche tecniche un sistema di verifica dell'età che prevede due passaggi logicamente separati: identificazione e autenticazione della persona identificata per ciascuna sessione di utilizzo del servizio regolamentato.

SISTEMI DI VERIFICA DELL'ETA' NON BASATI SU APPLICATIVI INSTALLATI NEL TERMINALE UTENTE

- In tal caso, un processo di verifica dell'età, in grado di fornire il necessario grado di tutela dei dati personali, deve essere diviso 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 o soggetto che ha identificato l'utente di Internet in un altro contesto. **Il soggetto che fornisce la "prova dell'età" non è conoscenza dell'utilizzo che l'utente ne farà.**

    L'Autorità ritiene opportuno che i gestori di siti web e le piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico 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 giuridicamente e tecnicamente 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. L'Autorità ritiene necessario 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). Come sopra detto, nel caso di sistemi pubblici, i Gestori dell'identità digitale sono essi stessi "soggetti terzi" (sia nei riguardi del soggetto regolamentato, sia rispetto a "Enti statali" e gestori di "banche dati pubbliche") e sono in possesso di determinati requisiti soggettivi e oggettivi stabiliti dalla normativa di settore, nonché selezionati sulla base di specifiche procedure di qualificazione e sottoposti a vigilanza da parte dell'Agenzia per l'Italia Digitale (AGID).
  - In secondo luogo, è prevista 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, non si ritiene conforme in quanto comporta che lo stesso soggetto che rilascia la prova dell'età sarà a conoscenza del particolare sito o piattaforma visitata dall'utente. **Viceversa, il modello proposto dall'Autorità, 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**).

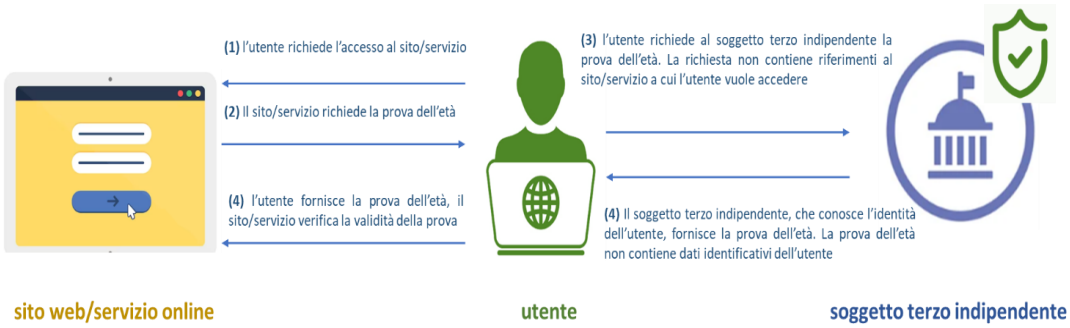
- Di seguito un esempio del processo suddetto:

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 che utilizzano la cifratura a chiave pubblica e privata per gestire la certificazione e la verifica come di seguito descritto[4]:
    a) per accedere ai contenuti, il sito o piattaforma video richiede all'utente di verificare la sua età e invia un oggetto (es. un file o una stringa alfanumerica) denominato "età da provare". **Tale oggetto non contiene nessun riferimento al sito web, piattaforma di video sharing o contenuto a cui l'utente vuole fare accesso.**
    b) l'utente richiede al soggetto terzo di fornire la prova dell'età, certificando l'oggetto denominato "età da provare". Il soggetto terzo certifica l'oggetto "età da provare" crittografandolo con chiave privata e generando così un nuovo oggetto denominato "prova dell'età". Tale certificazione non contiene nessun dato sull'identità dell'utente o sulla sua età anagrafica.
    c) l'utente invia la "prova dell'età" al sito o piattaforma a cui vuole accedere. Il sito o piattaforma applica la decrittografia con chiave pubblica alla "prova dell'età" per risalire al contenuto dell'oggetto, dopodiché verifica che tale contenuto sia valido e coerente con quello inizialmente inviato all'utente ed effettua i necessari controlli volti ad evitare il rischio di riutilizzo o di creazione fraudolenta delle certificazioni.

[4] 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.

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.

3) il gestore di siti web o la piattaforma di condivisione di video che diffondono in Italia immagini e video a carattere pornografico ottiene una prova della maggiore età dell'utente e, pur conoscendo necessariamente il particolare contenuto online consultato dall'utente, non ha alcuna informazione circa la sua identità.




- L'Autorità evidenzia l'importanza che la "prova dell'età" contenga solo l'informazione della maggiore età dell'utente e, pertanto, non includa riferimenti alla sua identità o all'età anagrafica.

SISTEMI DI *AGE ASSURANCE* BASATI SULL'USO DI APPLICATIVI

- Il soggetto terzo che fornisce la prova dell'età mette a disposizione dell'utente un'APP per la certificazione e la generazione della "prova dell'età" (es. **APP del portafoglio di identità digitale, oppure APP per la gestione dell'identità digitale,** etc.). In tal caso, con riferimento al punto (a) di cui sopra, l'oggetto "età da provare", presentato dal sito web/piattaforma di video *sharing* all'utente, può anche essere ottenuto tramite un QR Code[5]. L'utente, inquadrando il QR Code attraverso la fotocamera del proprio smartphone, accede, tramite un link, a un servizio (presente nella piattaforma/sito web) deputato all'autenticazione e utilizzerà l'APP per inviare la "prova dell'età", direttamente dal proprio dispositivo e senza l'intervento di alcun servizio web esterno, in modo che sia garantita la riservatezza dell'informazione relativa al sito/piattaforma/contenuto visitato e che tale informazione non venga divulgata a soggetti esterni, ma venga gestita esclusivamente all'interno del dispositivo utente.

- Ai sensi dell'art.12-ter comma 3 del "Regolamento del Parlamento europeo e del Consiglio che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea", le piattaforme *online* di dimensioni molto grandi, come definite dal DSA, che impongono agli utenti di autenticarsi per accedere ai servizi online, dovranno **accettare anche l'uso dei portafogli europei di identità digitale (EU digital wallet)**, rigorosamente su richiesta volontaria dell'utente, anche per quanto riguarda gli

[5] QR Code è la contrazione di ""Quick Response Code", ovvero un codice a barre matriciale a risposta rapida. Si tratta di un simbolo che restituisce, ogni qualvolta viene inquadrato dalla fotocamera di uno smartphone, dati e informazioni all'utente.

attributi minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione, come la 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*.

v. **Precisione ed efficacia:**

- Il sistema di *age assurance* deve essere efficace 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 indicatori di performance quali, ad esempio, nel caso di sistemi basati sulla stima, *l'errore medio*, la *deviazione*

*standard*, il 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 altro indicatore di performance 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 garanzia dell'età basata su Autodichiarazione non viene considerata un metodo efficace per determinare correttamente l'età di un utente.
- Il sistema di garanzia dell'età deve risultare neutrale o indipendente dal dispositivo di accesso o dal sistema operativo utilizzato dall'utente.
- I gestori di siti web e le piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico devono garantire che nessun utente acceda a contenuti pornografici finché non abbia dimostrato la maggiore età ossia finché il processo di garanzia dell'età non sia completato.
- Il processo di *age assurance* deve avvenire ad ogni consultazione di un determinato sito web o determinata piattaforma di *video sharing* che diffonde contenuti pornografici. Dopo che la consultazione del servizio viene interrotta, deve scattare una nuova verifica dell'età in caso di nuovo accesso a contenuti pornografici.
- La validità di una verifica dell'età deve quindi cessare nel momento in cui l'utente esce da un determinato servizio, ovvero quando termina la sessione, quando l'utente esce dal browser o quando il sistema operativo entra in stand-by e, comunque, dopo un periodo di 45 minuti di effettiva inattività al fine di evitare la visione di contenuti pornografici senza ulteriore verifica nel caso di un dispositivo condiviso tra un adulto e un minore.

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

- I sistemi di garanzia dell'età devono 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.

- I sistemi di garanzia dell'età devono risultare accessibili. 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 (es. utenti affetti da disabilità). Pertanto, i gestori di siti web e le piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico 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.
- Sarebbe opportuno rendere disponibili più soluzioni per la garanzia dell'età, dando la possibilità agli utenti di scegliere quale utilizzare in base alle proprie caratteristiche e necessità.
- La verifica dell'età non deve richiedere la creazione di un account utente del servizio offerto dal soggetto regolamentato. Inoltre, la prova dell'età non può essere memorizzata in un account utente su tale servizio. In ogni caso, l'obbligo di verifica dell'età si applica ad ogni accesso, con o senza account utente.

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 garanzia dell'età.
- Il criterio in questione fa riferimento alla capacità del sistema di garanzia dell'età di evitare o minimizzare pregiudizi non intenzionali e risultati discriminatori nei confronti degli utenti. Pertanto, ove applicabile, i gestori di siti web e le piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico 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.

viii. **Formazione e informazione:**

- L'Autorità evidenzia l'importanza di informare e di 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.

x. **Gestione dei reclami:**

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

xi. **Monitoraggio:**

- Al fine di garantire un elevato livello di tutela dei minori, l'Autorità valuterà caso per caso ed in concreto le soluzioni tecniche di verifica dell'età una volta attuate e in condizioni reali di funzionamento. Ai soggetti di cui all'articolo 1 è chiesto di garantire che le soluzioni messe in atto siano sistematicamente in grado di soddisfare i requisiti indicati nel presente provvedimento, adattando, se del caso, i loro principi e parametri operativi.

**xii. Vigilanza e cooperazione:**

- Fermo quanto previsto agli artt. 1 e 4 del presente provvedimento, l'Autorità coopera strettamente con la Commissione e con i Coordinatori nazionali dei servizi digitali designati negli altri Stati membri, in base al principio del paese di origine e, presta assistenza reciproca ai fini dell'applicazione coerente ed efficiente del presente provvedimento, anche mediante scambio di informazioni e ogni altra misura necessaria, attivando le pertinenti procedure di cooperazione tra Stati membri mediante il sistema IMI, anche avvalendosi delle indicazioni fornite dal *Memorandum of Understanding.*

## Art. 4

## ENTRATA IN VIGORE E CLAUSOLA DI RIVEDIBILITÀ

1. Ai sensi dell'art. 13-bis del Decreto, i gestori di siti web e le piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico si dotano di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni indicate entro sei mesi dalla data di pubblicazione del presente provvedimento.

2. Ferme le condizioni e le procedure previste all'articolo 1, comma 3, le disposizioni del presente provvedimento si applicano anche con riferimento ai gestori di siti web e alle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico e a prescindere dallo Stato membro di stabilimento, tre mesi dopo la pubblicazione della lista di cui all'articolo 1 del presente provvedimento.

3. A decorrere dalla data di entrata in vigore degli orientamenti adottati ai sensi dell'articolo 28 del Regolamento (UE) 2022/2065, l'Autorità, laddove necessario, si impegna a modificare ed adeguare il presente provvedimento alla normativa europea sopravvenuta con riferimento ai soggetti stabiliti in altri Stati membri.