

ALLEGATO C alla delibera n. 96/25/CONS

ESITI DELLA CONSULTAZIONE PUBBLICA DI CUI ALLA DELIBERA N. 61/24/CONS

1 Sommario

<i>I. IL PROCEDIMENTO</i>	1
<i>II. CONSIDERAZIONI GENERALI</i>	2
<i>III. OBBLIGHI E AMBITO SOGGETTIVO E OGGETTIVO DELLE LINEE GUIDA</i>	6
<i>IV. MODALITA' DI REALIZZAZIONE DEI SISTEMI DI AGE ASSURANCE</i>	10
<i>V. SULLA LIBERTA' DI SCELTA DEI SISTEMI DI VERIFICA DELL'ETA' DA PARTE DEI SOGGETTI REGOLAMENTATI</i>	18
<i>VI. SULLE TEMATICHE RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI</i>	19
<i>VII. SULL'INTERVENTO DI SOGGETTI TERZI INDIPENDENTI</i>	22
<i>VIII. SUL TEMA DELLA SICUREZZA DEI SISTEMI</i>	25
<i>IX. SUI CRITERI DI PRECISIONE ED EFFICACIA</i>	27
<i>X. SUI CRITERI DI ACCESSIBILITA', FACILITA' D'USO E NON DISCRIMINAZIONE</i>	28
<i>XI. SUL CRITERIO DI TRASPARENZA</i>	29
<i>XII. SUL TEMA DELLA FORMAZIONE E INFORMAZIONE</i>	30

I. IL PROCEDIMENTO

Con la delibera n. 61/24/CONS, del 6 marzo 2024, l'Autorità ha avviato la consultazione pubblica di cui all'art. 1, comma 4, della delibera n. 9/24/CONS volta all'adozione di un provvedimento sulle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159.

Alla consultazione hanno partecipato con propri contributi i seguenti soggetti: Meta Ireland (di seguito denominata **META**), [**OMISSIS** - un fornitore di piattaforma video sharing], WebGroup

Czech Republic¹ (di seguito denominata **WEBGROUP**), Aylo holdings² (di seguito denominata **AYLO**), [**OMISSIS** - un operatore di comunicazioni elettroniche (di seguito denominato **un operatore**)] , Garante per l'infanzia e l'adolescenza (di seguito denominato **GARANTE PER L'INFANZIA**), Consiglio nazionale degli utenti (di seguito denominato **CNU**), Movimento italiano genitori (di seguito denominato **MOIGE**), Altroconsumo, Forum delle associazioni familiari (di seguito denominato **FAF**), Centro Italiano Femminile (di seguito denominato **CIF**), Movimento cristiano lavoratori (di seguito denominato **MCL**), Noi Trento APS (di seguito denominata **NOI TRENTO**).

A seguito della ricezione dei contributi scritti, nel mese di maggio 2024, si sono tenute le audizioni dei partecipanti al procedimento.

Si illustrano di seguito gli esiti della consultazione pubblica.

II. CONSIDERAZIONI GENERALI

A. Osservazioni di soggetti istituzionali, operatori e associazioni

Sulla necessità di efficaci sistemi di verifica dell'età

Il **GARANTE PER L'INFANZIA** rappresenta che la costante e rapida evoluzione del mondo digitale e lo sviluppo di nuove e sempre più coinvolgenti modalità di relazione con i diversi dispositivi e software che ne fanno parte rendono sempre più urgente l'implementazione di un sistema efficace di regolamentazione e tutela dai rischi che ne possono scaturire, soprattutto per i soggetti più vulnerabili. Tale esigenza è resa quanto mai impellente dal crescente e massivo impiego dell'intelligenza artificiale che sta determinando ulteriori trasformazioni dagli esiti difficilmente prevedibili. Ritiene che, sebbene siano stati compiuti apprezzabili progressi nell'introduzione di diversi strumenti e meccanismi volti a proteggere i giovani utenti dalle insidie della rete, molte di queste misure si rivelano ancora del tutto insufficienti. Aggiunge che risulta evidente come la maggior parte dei sistemi di verifica dell'età si basi ancora su metodi facilmente eludibili che comportano una evidente e significativa vulnerabilità dei minori, in quanto potenzialmente esposti a contenuti e servizi molto lesivi per la loro salute fisica e psichica. Pur riconoscendo che il problema risulta molto complesso e di difficile soluzione anche per la mancanza di una standardizzazione e regolamentazione coerente

¹ WebGroup Czech Republic, a.s. è una società, costituita nella Repubblica Ceca, che gestisce il sito web XVideos disponibile all'indirizzo www.xvideos.com. XVideos ospita e mette a disposizione degli utenti video per adulti gratuitamente. Gli utenti possono anche creare un account per caricare i propri contenuti online e ricevere in cambio un compenso. XVideos è un modello di business basato sul traffico Internet e sulla pubblicità e non prevede la vendita di contenuti per adulti.

² Aylo Holding S.à.r.l. è una società di tecnologia e media, proprietaria di un ampio portafoglio di attività di intrattenimento per adulti (Pornhub, YouPorn, Redtube, Brazzers). Le attività principali sono costituite da siti di streaming video gratuiti e su abbonamento. Le principali unità di business di Aylo sono le seguenti: piattaforme di condivisione video (VSP), siti a pagamento, piattaforme di contenuti per modelli e modelle, piattaforme pubblicitarie e piattaforme di videogiochi.³ Per filtering software intende in generale un software installato sul dispositivo in grado di filtrare le pagine web/contenuti per adulti (a livello di browser web come propone la Spagna, o anche a livello di software applicativo di parental control).

nei diversi paesi che può creare disparità e lacune nei sistemi di protezione, rendendo impraticabile l'adozione di soluzioni effettivamente efficaci su scala globale, il GARANTE apprezza che l'Autorità abbia dato attuazione ad una norma cui il Legislatore ha dato rilievo urgente e che si pone l'obiettivo di introdurre un sistema di verifica dell'età capace di impedire l'accesso dei minorenni ai siti ed alle piattaforme di condivisione di immagini e video a carattere pornografico.

Il CNU apprezza l'attenzione di Agcom alla tutela dei diritti e delle legittime esigenze dei minori quali soggetti attivi del processo comunicativo, così come previsto anche dalla Convenzione del Fanciullo, e ritiene che l'avvio della consultazione pubblica sulle modalità di verifica della maggiore età da parte dei gestori di siti web e dei fornitori delle piattaforme di condivisione video potrà contribuire ad evitare l'esposizione dei minori a contenuti inappropriati rispetto alla loro età, contenuti che ne possono minare il benessere psico-fisico. **Rappresenta, pertanto, che la soluzione che l'Autorità ha posto in consultazione, con il parere favorevole del Garante privacy, trova totale adesione da parte del CNU.** Ritiene, altresì, che sia necessaria una definizione delle modalità di verifica dell'età in modo che le stesse risultino chiare, efficaci e verificabili tramite un solido quadro di certificazione e interoperabilità, in quanto i metodi di verifica dell'età online già presenti sul mercato globale comportano, il più delle volte, rischi per la privacy e la sicurezza informatica poiché adottano un trattamento eccessivo dei dati personali come, ad esempio, i dati della carta d'identità, i dati della carta di credito, il riconoscimento facciale, o ancora, l'analisi del comportamento online dell'utente. Questi metodi richiedono una eccessiva proliferazione di dati sensibili che sfuggono al controllo dei titolari e che comportano rischi in termini di sicurezza e trasparenza. Altri metodi di verifica (come, ad esempio, l'autodichiarazione) risultano molto poco efficaci in quanto possono essere facilmente aggirati, altri ancora sono caratterizzati da un elevato margine di errore statistico e, in tal caso, il rischio è che il minore riesca ad avere accesso a contenuti nocivi e inappropriati, senza limitazioni o controlli.

Il **MOIGE** sottolinea, nel perseguimento del superiore interesse dei minori ed al fine di garantire loro la massima tutela anche sulla rete, la rilevanza giuridica del problema dell'accesso dei minori d'età alle piattaforme di social networking ed a tutti i servizi della società dell'informazione, considerato che la fruizione di tali servizi è pur sempre esecuzione di un'attività negoziale in quanto è subordinata alla conclusione di un contratto e delle relative condizioni di utilizzo dei servizi offerti dai fornitori. Rileva, pertanto, un'antinomia all'interno dell'ordinamento giuridico in quanto la normativa consente ai minori, dopo il compimento dei quattordici anni, di utilizzare i servizi di comunicazione elettronica, sebbene per accedere alle piattaforme di social networking sia necessario sottoscrivere vere e proprie clausole contrattuali, accettare i termini di servizio e prestare il proprio consenso al trattamento dei dati personali per le finalità inerenti all'esecuzione del contratto. Infatti, per accedere alle piattaforme dei social network sites è necessario sottoscrivere le condizioni di utilizzo, vere e proprie clausole contrattuali, accettare i termini di servizio e prestare il proprio consenso al trattamento dei dati personali per le finalità inerenti all'esecuzione del contratto. Evidenzia che un minore d'età, per l'ordinamento italiano, non può lecitamente disporre dei propri diritti ed interessi ad es. patrimoniali, poiché l'ordinamento attribuisce la capacità di agire a colui che abbia raggiunto la maggiore età. Eppure, aggiunge, per una sorta di fenomeno dei vasi comunicanti, la condizione soggettiva per la prestazione del consenso al trattamento dei dati personali del Regolamento UE 2016/679 è diventata

di fatto, non di diritto, requisito sufficiente per la conclusione di un contratto di fornitura di servizi, senza alcun consenso del soggetto esercente la responsabilità genitoriale. Pertanto, ritiene che l'appropriazione dei dati personali dei minori mediante l'artificio di differenziare l'età per accedere ai servizi della società dell'informazione rispetto all'età per compiere qualsiasi altra attività giuridica sia illegittima e in violazione di norme imperative dell'ordinamento italiano e di ogni ordinamento che richieda, per l'acquisto della capacità di agire, il compimento dei 18 anni. Per una sorta di fenomeno dei vasi comunicanti la condizione soggettiva per la prestazione del consenso al trattamento dei dati personali ai sensi dell'art. 6, comma 1 lett. a) del Regolamento (UE) 2016/679 è diventata di fatto, anche se non di diritto, condizione soggettiva per la conclusione di un contratto di fornitura di servizi, posto che le possibilità di un effettivo controllo sull'età del contraente-utilizzatore sono limitate, a meno che non vengano con urgenza applicate misure efficaci per la verifica dell'età degli utilizzatori di siti e servizi che esponano contenuti o attività non adatti ai minori. Inoltre, sottolinea che ai sensi dell'art. 17 d. lgs. 70/2003 il prestatore di servizi della società dell'informazione non è tenuto ad un obbligo di sorveglianza sulle informazioni che trasmette o memorizza, per cui la responsabilità civile degli atti commessi dal minore sulla rete ricade sugli esercenti la responsabilità genitoriale: per questo è necessario e urgente che sia restituita ai genitori la reale possibilità di controllo e decisione sull'utilizzazione da parte dei figli minori delle piattaforme di social networking e che sia ripristinata l'età di diciotto anni per esprimere validamente qualsiasi tipo di volontà e di consenso anche per la fornitura di servizi della società dell'informazione. Infine, richiede l'adozione dei sistemi che, con la massima efficacia e sicurezza, garantiscono una specifica espressione di consenso da parte degli esercenti la responsabilità genitoriale per l'accesso a piattaforme che forniscono servizi di comunicazione o mettano a disposizione contenuti audio e video.

NOITRENTO supporta l'esigenza di una reale *age verification* per la consultazione dei siti che richiedono una maggiore età.

Il **MCL** rappresenta che i metodi di verifica on line dell'età utilizzati fino ad ora non sono stati in grado di tutelare i minori dai contenuti che possono danneggiare e compromettere il loro sviluppo e benessere fisico, psichico e morale, e ritiene pertanto urgente individuare ed attivare nuovi meccanismi che garantiscano un elevato livello di protezione e, nel rispetto della privacy, non permettano ai minori di accedere a contenuti e attività che danneggiano irreparabilmente il loro sviluppo armonico ed integrale. Chiede, inoltre, che la presente consultazione pubblica non sia un'iniziativa episodica, ma attivi un sistema di protezione costantemente monitorato e aggiornato in grado di coinvolgere e supportare le famiglie.

Il **CIF** conferma di approvare in toto il provvedimento che disciplina le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti.

ALTROCONSUMO ritiene utile aggiungere le definizioni di "prova dell'età" e di "soggetto certificatore". Evidenzia che il principio di proporzionalità deve funzionare da bilanciante nella ponderazione dei diritti e delle libertà da salvaguardare, quali la libertà di espressione e il diritto alla privacy, e che i sistemi di verifica devono operare per eccesso di garanzia dato che è meglio tutelare

“erroneamente” un maggiore, che omettere tutela nei confronti di un minore. Per queste evenienze, propone di prevedere dei sistemi di “correzione” *ex post* nel caso venga bloccata la fruizione di un sito o di contenuti da parte di un maggiorenne.

Il FAF, nell'accogliere con favore l'apertura della consultazione pubblica sulle modalità tecniche e di processo che i soggetti individuati dalla norma sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, ritiene necessario agire su più fronti. Infatti, oltre al filtro di parental control predisposto dagli operatori, ritiene che anche i siti che diffondono materiale video inteso per un pubblico di adulti, come Pornhub e molti altri simili, dovrebbero predisporre adeguate forme di verifica dell'età.

Sulla necessità di un approccio armonizzato a livello europeo

META, pur comprendendo che l'obiettivo della legge è quello di impedire l'accesso a contenuti pornografici (dunque non direttamente applicabili a Meta), ritiene che l'accesso a contenuti inappropriati o destinati ad un pubblico adulto dovrebbe essere considerato nell'ambito di un quadro più ampio e articolato; piuttosto che puntare all'introduzione di svariati metodi di *age assurance* adottati da soggetti diversi che, oltre a generare un quadro di riferimento frammentario ed inefficace, potrebbero provocare rischi significativi rispetto alla minimizzazione dei dati. Inoltre, al fine di garantire la loro efficacia, reputa necessario che queste soluzioni siano discusse a livello europeo, oltre che discusse a livello di settore. Allo stesso modo, ritiene fondamentale che tutte le app siano soggette agli stessi standard in modo da assicurare un approccio coerente ed efficace alla tutela dei giovani. La collaborazione dell'intero settore sul tema permetterebbe di garantire esperienze sicure e adatte all'età, prevenendo allo stesso modo la migrazione dei giovani su app meno sicure di quelle che hanno investito in sicurezza ed esperienze adatte all'età. Infine, reputa che bisogna adottare un approccio multilivello alla verifica dell'età, che preveda la possibilità per gli utenti di scegliere un meccanismo di *age assurance* basato sulla fattibilità e sulle preferenze, così da garantire equità e obiettività del processo.

B. Valutazioni dell'Autorità

L'Autorità prende atto del fatto che sussiste sia da parte dei soggetti istituzionali che dei privati la consapevolezza della necessità di un efficace sistema di verifica dell'età e che la soluzione proposta dall'Autorità risulti idonea a contemperare le esigenze di efficacia e tutela dei dati personali. Ritiene, inoltre, condivisibile che il tema dell'accesso a contenuti inappropriati o destinati ad un pubblico adulto debba essere considerato nell'ambito di un contesto internazionale o, quantomeno, europeo al fine di evitare un quadro di riferimento frammentario e di garantire l'efficacia delle soluzioni. Si condivide altresì sulla necessità che tutte le app siano soggette agli stessi standard minimi in modo da assicurare un approccio coerente ed efficace alla tutela dei giovani. L'Autorità, pertanto, con le presenti specifiche tecniche adotta un approccio *future proof*, che sia allo stesso tempo rispettoso dei requisiti del decreto-legge 123/2023 (come convertito in legge) e, allo stesso tempo, in grado di includere ed essere conforme alle future previsioni comunitarie in materia di sistemi per la verifica dell'età e le decisioni che saranno assunte in tale ambito.

III. **OBBLIGHI E AMBITO SOGGETTIVO E OGGETTIVO DELLE LINEE GUIDA**

A. Osservazioni di soggetti istituzionali, operatori e associazioni

Il **GARANTE PER L'INFANZIA** auspica che si possa consentire di **estendere tale protezione anche ad altri contenuti gravemente lesivi** della salute fisica e psichica di bambini e adolescenti, come quelli di istigazione all'odio, alla violenza ed altre pratiche scorrette e dannose, anche se non ricompresi nelle finalità della consultazione.

ALTROCONSUMO ritiene che i **sistemi di garanzia delineati possano trovare applicazione con riferimento ai contenuti soggetti a parental control di cui alla delibera 9/23/CONS** e cioè, a titolo non esaustivo: contenuti per adulti, gioco d'azzardo, scommesse, contenuti relativi ad armi, droga, violenza, odio e discriminazione, promozione di pratiche che possono danneggiare la salute alla luce di consolidate conoscenze mediche, sette.

META si raccomanda di limitare le definizioni riportate nel testo ai soli soggetti definiti dall'articolo 13 bis del decreto-legge n. 123 del 15 settembre 2023. In particolare, ritiene che **le definizioni di "servizio regolamentato" e "soggetto regolamentato" debbano comprendere esclusivamente i servizi e i soggetti che facilitano l'accesso a contenuti pornografici**, così come definiti dall'articolo 13 bis del decreto-legge 15 settembre 2023, n. 123, evitando un'applicazione generalizzata a ulteriori tipologie di servizi che offrono contenuti riservati a utenti adulti.

AYLO ritiene che nelle definizioni **dovrebbero rientrare non solo le piattaforme di condivisione video, ma tutti i siti web e i social media che sono anche solo in grado di condividere contenuti sessualmente espliciti**. Infatti, evidenzia che se i sistemi di verifica dell'età venissero implementati solo su piattaforme specifiche che diffondono contenuti sessualmente espliciti, come è avvenuto in altre giurisdizioni, quasi nessun utente (a prescindere dall'età) continuerebbe a visitare tale sito e gli utenti passerebbero semplicemente ad altri e numerosi siti sprovvisti di sistemi di verifica e di stima dell'età, i quali, probabilmente, sarebbero meno ossequiosi della legge e soggetti a misure di affidabilità e sicurezza e di moderazione dei contenuti notevolmente inferiori. Pertanto, ritiene che l'effettiva protezione dei minori sarebbe nulla, poiché gli utenti si sposterebbero semplicemente sui siti meno protetti e non ossequiosi della legge. Inoltre, evidenzia che gli utenti che dovessero decidere di non spostarsi su altri siti, utilizzerebbero altri metodi per aggirare i requisiti di protezione dell'età, qualunque sia la forma adottata nello specifico. Sul tema, AYLO rappresenta che esistono centinaia di migliaia di siti classificati come siti per adulti e che i siti web di contenuti per adulti più grandi e più visitati sono, in realtà, quelli che hanno maggiori probabilità di rispettare la legge, in quanto capaci di investire più risorse nei processi di affidabilità e sicurezza e di moderazione, limitando così la disponibilità e la potenziale esposizione dei visitatori a materiale illegale, osceno o dannoso. Pertanto, mentre gli operatori di siti web più responsabili potranno conformarsi a tale legislazione, gli altri non lo faranno (e non lo hanno fatto sinora nei Paesi dove è stata fatta una regolamentazione) e ciò comporta un sostanziale aumento del rischio per gli utenti di essere esposti a materiale potenzialmente

dannoso su siti web privi di controlli adeguati. Ad esempio, negli Stati americani in cui AYLO ha introdotto la verifica dell'età e la stima dell'età o ha rimosso l'accesso alle proprie piattaforme, si è assistito a un'impennata delle ricerche di altri siti per adulti, spesso non regolamentati, con processi di affidabilità, sicurezza o moderazione ridotti o inesistenti, nonché a ricerche di reti private virtuali (VPN).

In particolare, AYLO ha rappresentato il caso dello stato della Louisiana (USA) dove, nel 2023 a seguito dell'adozione di una norma che obbligava i siti web/piattaforme che forniscono contenuti pornografici, a effettuare la verifica dell'età tramite carta di identità elettronica, si è riscontrato una diminuzione degli accessi alla propria piattaforma dell'80% e sono aumentate, al tempo stesso, le ricerche di siti alternativi, metodi di elusione dei controlli e di utilizzo delle VPN.

Alla luce di quanto rappresentato, ritiene fondamentale che - al fine di proteggere i minori dai contenuti destinati agli adulti online nel modo più completo ed efficace - l'ambito di applicazione di tali obblighi debba essere sufficientemente ampio da includere tutti i contenuti di questo tipo.

In conclusione, AYLO ritiene che per garantire che i minori siano protetti dai contenuti online destinati agli adulti, il campo di applicazione della nuova legislazione dovrebbe essere sufficientemente ampio da includere tutti i contenuti potenzialmente dannosi, compresi i siti web dei social media che consentono la fruizione di materiale per adulti, sottolineando che una soluzione implementata a livello di dispositivo rappresenterebbe la migliore opzione per bloccare anche altri contenuti non adatti ai minori.

WEBGROUP ritiene che nel caso in cui venga introdotto un ampio requisito che stabilisca meccanismi di *age verification* per tutti i contenuti audiovisivi dei VSP ritenuti dannosi, **tali requisiti dovrebbero essere conformi al diritto dell'Unione europea e, in particolare, alla legge del Paese d'origine**, come sancito dalla Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, quale il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico). Tali requisiti dovrebbero inoltre rispettare il principio di proporzionalità in termini di utilizzo dei mezzi meno restrittivi possibili per raggiungere gli obiettivi di politica pubblica e dovrebbero garantire un adeguato bilanciamento tra la protezione dei minori e i diritti fondamentali in gioco.

[OMISSIS - Un fornitore di piattaforma video sharing] ritiene che la **norma non si applicherebbe a [OMISSIS - Un fornitore di piattaforma video sharing]** in quanto **fornitore stabilito in paese terzo** oltre che in relazione al fatto che la società non permette agli utenti la diffusione di contenuti pornografici tramite le proprie piattaforme; tuttavia, condivide la necessità di stabilire meccanismi per proteggere i minori dai contenuti rivolti agli adulti. Aggiunge che lo **sviluppo di un quadro europeo di *age assurance* sia la strada giusta da seguire** e, pertanto, tali sforzi dovrebbero essere presi in considerazione anche ai fini del provvedimento oggetto di consultazione.

[OMISSIS - Un fornitore di piattaforma video sharing] ritiene che, al fine di tutelare adeguatamente i minori online, gli strumenti di *age assurance* debbano essere: (i) proporzionati; (ii) rispettosi dei diritti di protezione dei dati personali dell'utente e della *user experience*; e (iii) semplici ed efficaci. Concorda con l'Autorità che è fondamentale che qualsiasi iniziativa adottata in questo ambito sia proporzionata. Da ciò deriva che le misure di *age assurance* dovrebbero limitare l'accesso da parte dei minori ai contenuti senza ledere i loro dati personali e diritti fondamentali mediante

strumenti di tutela eccessivamente restrittivi. In tale contesto, ritiene utile notare anche che **l'art. 28 del DSA prevede che piattaforme online debbano adottare misure "adeguate e proporzionate" al fine di garantire la protezione dei minori online ma non dispone alcun obbligo a dotarsi di strumenti di *age assurance* - la cui adozione rimane nella libera iniziativa dei fornitori.** Infatti, l'*age assurance* rappresenta solo una delle soluzioni disponibili ai fini della tutela dei minori online e può essere progettata in modi diversi, a seconda delle caratteristiche specifiche del servizio considerato di volta in volta. A tale riguardo, ai sensi **dell'art. 35(1)(j) del DSA**, l'*age assurance* potrebbe essere considerata una potenziale misura di mitigazione del rischio per le Very Large Online Platforms (VLOPs), anche in riferimento ai rischi identificati nell'art. 34 del DSA (che comprende anche i rischi per i minori).

[OMISSIS – Un operatore] sostiene che gli obblighi e le responsabilità per l'implementazione delle modalità di *age verification* saranno da riferirsi esclusivamente alle categorie di soggetti individuati dalla normativa, e non anche ai soggetti che non offrono contenuti o piattaforme di condivisione di video come i fornitori di servizi di comunicazione elettronica. **Ritiene che quest'ultimi, non avendo alcuna connessione con detti servizi, dovranno ritenersi al di fuori della categoria dei soggetti regolamentati ai fini della presente consultazione.**

Allo stesso tempo, ritiene che gli Operatori di comunicazione elettronica non debbano essere obbligati a fornire tale prestazione e dunque ad evadere le richieste di verifica dell'età. Nell'ottica di non ribaltare sui soggetti terzi indipendenti un obbligo in capo ai siti web e alle piattaforme, ritiene che **l'Operatore debba mantenere una discrezionalità nella fornitura di tale servizio di *Age Verification* ai soggetti regolamentati.** Infatti, non ritiene proporzionale la previsione che l'Operatore debba soddisfare ciascuna richiesta di verifica dell'età da parte dei siti, in maniera obbligatoria. Evidenzia che non si può non tenere in considerazione l'eccezionale numerosità delle richieste che il soggetto chiamato ad eseguire tecnicamente l'attività di verifica dovrebbe evadere e gli investimenti che si rendono necessari, in particolar modo a fronte di una possibile espansione dell'ambito applicativo della proposta di regolamento.

B. Valutazioni dell'Autorità

L'Autorità rileva che il GARANTE PER L'INFANZIA auspica che si possa consentire di estendere il sistema di verifica dell'età proposto a protezione dei minori anche ad altri contenuti gravemente lesivi della salute fisica e psichica di bambini e adolescenti, come quelli di istigazione all'odio, alla violenza ed altre pratiche scorrette e dannose, anche se non ricompresi nelle finalità della consultazione. Dello stesso avviso ALTROCONSUMO ritiene che i sistemi di garanzia delineati possano trovare applicazione con riferimento ai contenuti soggetti a *parental control* di cui alla delibera 9/23/CONS. Su fronte opposto META e AYLO che ritengono che **le definizioni di "servizio regolamentato" e "soggetto regolamentato" debbano comprendere esclusivamente i servizi e i soggetti che facilitano l'accesso a contenuti pornografici.** WEBGROUP ritiene che nel caso in cui venga introdotto un ampio requisito che stabilisca meccanismi di *age verification* per tutti i contenuti audiovisivi dei VSP ritenuti dannosi, **tali requisiti dovrebbero essere conformi al diritto dell'Unione europea e, in particolare, alla legge del Paese d'origine.** Anche [OMISSIS - Un

fornitore di piattaforma video sharing] ritiene che la norma non si applicherebbe a lui in quanto fornitore stabilito in paese terzo e che lo sviluppo di un quadro europeo di *age assurance* sia la strada giusta da seguire; se del caso, in linea con l'art. 35(1)(j) del DSA, l'*age assurance* potrebbe essere considerata una potenziale misura di mitigazione del rischio per le Very Large Online Platforms (VLOPs), anche in riferimento ai rischi identificati nell'art. 34 del DSA (che comprende anche i rischi per i minori).

Con riferimento all'osservazione di META, AYLO e WEBGROUP, per quanto riguarda la sussistenza dell'obbligo e l'ambito soggettivo di applicazione, l'Autorità, considerato anche quanto proposto dal GARANTE PER L'INFANZIA e dall'associazione dei consumatori, ritiene opportuno chiarire, viste le osservazioni di alcuni soggetti intervenuti nella consultazione pubblica, che la disciplina delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti, che con la presente delibera si approva in attuazione dell'art. 13-bis del decreto-legge n. 123/2023 convertito, con modificazioni, dalla legge n. 159/2023, deve essere adottata dai gestori di siti web e dai fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico ovunque stabilite.

Sul punto, l'Autorità ritiene che, alla luce del contesto normativo di riferimento prima richiamato e alle osservazioni formulate dai partecipanti, le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti approvati con questo 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 qui direttamente regolati 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 9/03/CONS.

Nel condividere l'osservazione di AYLO, L'Autorità ritiene ragionevole che nell'ambito oggettivo di applicazione dovrebbero rientrare non solo le piattaforme di condivisione video, ma tutti i siti web e i social media che sono anche solo in grado di condividere contenuti sessualmente espliciti. In relazione all'osservazione secondo cui è probabile che solo i fornitori di siti e piattaforme di grandi dimensioni implementeranno le misure in questione, si ritiene che una adeguata attività di vigilanza, anche per il tramite del sistema di cooperazione previsto dal Regolamento *digital service act*, e adeguati presidi normativi potranno fungere da deterrente. Ai sensi del TUSMA, inoltre, come di seguito chiarito, l'Autorità potrà comunque inibire la circolazione di contenuti nocivi, diffusi da parte di fornitori stabiliti in altri Stati, presso utenti situati nel territorio italiano.

Con riferimento all'osservazione di [OMISSIS – Un operatore], l'Autorità ritiene ragionevole, laddove come soggetti terzi intervengano i privati, che i titolari delle piattaforme di condivisione video e di siti web interagiscano con questi ultimi mediante accordi frutto di negoziazione commerciale.

IV. MODALITA' DI REALIZZAZIONE DEI SISTEMI DI AGE ASSURANCE

A. Osservazioni di soggetti istituzionali, operatori e associazioni

Il **GARANTE PER L'INFANZIA** ritiene che, tra le diverse soluzioni prospettate nella consultazione, conformemente a quanto già proposto nell'ambito del Tavolo tecnico sulla tutela dei diritti dei minori in rete nel contesto dei sodai networks, dei servizi e dei prodotti digitali istituito presso il Ministero della Giustizia con DM 21 giugno 2021 **l'adozione di un sistema basato sull'utilizzo di una identità digitale di tipo SPID consenta di garantire un elevato grado di certezza** nel determinare l'età dell'utente e, al contempo, nel rispetto del principio di proporzionalità, offra le necessarie garanzie di tutela dei dati personali e protezione da contenuti dannosi per i minori. Ciò è in linea con quanto sollecitato dalla Commissione europea con la nuova strategia europea per un'internet migliore per i ragazzi (BIK+), adottata l'11 maggio 2022, che ha invitato gli Stati membri a sostenere strumenti efficaci di verifica dell'età in linea con la normativa europea sull'identità digitale europea recentemente adottata (Regolamento UE del 26 marzo 2024). Inoltre, pur riconoscendo che altre soluzioni consentono di conseguire più agevolmente discreti livelli di protezione, ritiene che la protezione dei minori non può essere limitata all'impiego di sistemi già utilizzati in passato, come il parental control, uno strumento che, sebbene quando attivato risulti molto flessibile ed adeguato ad offrire protezione ai minori in rete, ha incontrato scarsa diffusione, sia nei media tradizionali che nei nuovi media, a causa di uno scarso utilizzo da parte degli adulti di riferimento, spesso a fronte di una certa difficoltà di impiego.

WEBGROUP sottolinea l'importanza di considerare che *l'age verification* possa essere effettuata in maniera più efficiente a livello di dispositivo dell'utente, ad esempio sotto forma di software di filtraggio (APP), anziché a livello di sito web. In tal modo gli utenti hanno il controllo assoluto sulla propria identità ed età e si riduce al minimo la quantità di dati condivisi con i siti web pornografici che resterebbero sul dispositivo. A supporto di ciò, afferma che il **governo australiano** ha recentemente deciso, dopo l'approvazione di una legge che favoriva *l'age verification*, di non implementare più *l'age verification* a causa di uno studio dettagliato che ha confermato numerosi problemi con la tecnologia ad esso collegata. In particolare, il governo australiano sta attualmente collaborando con i rappresentanti dell'industria per sviluppare meccanismi educativi efficaci per i genitori, affinché **utilizzino il software di filtraggio a livello di dispositivo per limitare l'accesso dei bambini a materiale dannoso.**

Come ulteriore esempio, aggiunge che anche la **Spagna ha recentemente lanciato un programma pilota, sviluppato dall'Agenzia nazionale per la protezione dei dati (DPA), che prevede di effettuare *l'age verification* a livello di dispositivo.**

La soluzione prevista dal DPA Spagnolo si basa **sull’etichettatura dei contenuti** (mediante *tag*) da parte dei fornitori di servizi online, che consente di classificare i contenuti come sessuali, violenti e/o razzisti. La limitazione dell'accesso viene eseguita localmente sul dispositivo dell'utente anziché dal fornitore di servizi online o anche da terzi come intermediari. Il sistema si basa su una interazione virtuale che si stabilisce tra il *browser* del PC e un’APP installata nel cellulare dell’utente. In questo modo l'accesso ai contenuti riservati agli adulti tramite il *browser* del PC è gestito da un App di verifica dell'età da installare sul cellulare degli utenti. Il browser del PC, analizzando i *tag* relativi ai contenuti web, richiederà all’utente la verifica dell’età – inquadrando con il cellulare un codice QR presentato dal browser stesso – all'App installata sul cellulare per concedere o rifiutare l'accesso a contenuti specifici precedentemente etichettati, dai siti e piattaforme online, come contenuti per adulti o contenuti inappropriati. Invece, per quanto riguarda l'accesso ai contenuti direttamente da cellulare, trovano applicazione le soluzioni eWallet compatibili con il regolamento eIDAS che lavorano su sistemi di “attribuzione dell'età” per fornire conferma di un'età specifica, rispettando il principio di minimizzazione dei dati. In questo caso, il browser del cellulare richiederà la verifica e interagirà con l’App eWallet, anche questa nel cellulare, che fornisce l'attributo della maggiore età.

WEBGROUP ritiene che **la soluzione prevista dal DPA spagnolo sia adatta a bilanciare gli obiettivi dei sistemi di *age verification*** (cioè, impedire l'accesso dei minori ai contenuti per adulti) e la protezione dei diritti degli utenti adulti, che includono diritti costituzionalmente protetti come la libertà di espressione e il diritto alla privacy, nonché la sicurezza degli utenti e la sicurezza nazionale. Inoltre, osserva che i minori sono generalmente più a rischio di essere esposti a contenuti per adulti dai siti web dei social media e dai motori di ricerca rispetto ai tradizionali siti web per adulti come XVideos. Ritiene che i motori di ricerca permettano a chiunque di accedere in pochi secondi a una grande quantità di immagini e video per adulti (contenuti che non sono meno espliciti di quelli che si trovano su XVideos). Ad esempio, l’associazione spiega che Facebook ha segnalato ben 73,3 milioni di contenuti espliciti come "nudità infantile e sfruttamento sessuale" solo nei primi nove mesi del 2022 e lo stesso vale per altri siti popolari come Youtube, Twitter (ora X), TikTok, Reddit, Snapchat o LinkedIn, per non parlare di siti web molto meno popolari, ma di facile accesso. Infine, ribadisce che il filtering software, o **software di filtraggio a livello di dispositivo³**, **può essere più efficace nel prevenire l'accesso dei minori a contenuti espliciti online e a un'ampia gamma di contenuti per adulti.**

WEBGROUP ritiene che, se la **procedura di *age verification* viene eseguita a livello di dispositivo tramite software di filtraggio**, senza l'intervento di terzi, il rischio di indipendenza da parte di terzi viene eliminato. Inoltre, ritiene che l’introduzione di una terza parte come depositaria di qualsiasi informazione aggiunga inevitabilmente un ulteriore livello di preoccupazione per la protezione di tali dati. L'*age verification* fatta sul dispositivo bilancia adeguatamente l'interesse del minore con gli altri diritti di tutti gli utenti di Internet, come l'anonimato dell'utente. A questo proposito, ritiene che **quanto implementato oggi dai fornitori di identità digitali (come, ad esempio, l'autorità governativa che concede una carta d'identità elettronica o un certificato) siano sufficienti, e non**

³ Per filtering software intende in generale un software installato sul dispositivo in grado di filtrare le pagine web/contenuti per adulti (a livello di browser web come propone la Spagna, o anche a livello di software applicativo di parental control).

è necessario creare alcun sistema di identità digitale alternativo ai fini dell'*age verification* prima dell'accesso dei minori ai contenuti per adulti.

WEBGROUP ritiene che un sistema di *age verification* a livello di dispositivo garantirebbe che i sistemi siano completamente verificabili e trasparenti, soprattutto alla luce dei rischi elevati che alcuni strumenti *age verification* esistenti comportano. A tale proposito rappresenta che alcuni dei sistemi di *age verification* più diffusi sono realizzati da terze parti, anziché dal sito web stesso, e che l'*age verification* effettuata dai fornitori di contenuti, invece che dagli individui sui loro dispositivi, mette a rischio i diritti e le libertà degli stessi oltre a non essere efficace nel prevenire l'accesso dei minori ai contenuti per adulti, mettendo a rischio la privacy dei visitatori del sito (ad esempio, quando le informazioni di identificazione fornite per la verifica dell'età vengono rivelate da hacker o altro). Inoltre, ritiene ci sia il rischio che l'entità che effettua l'*age verification* possa localizzare i minori o raccogliere i loro dati. Ritiene che l'*age verification* comporti il rischio di ricatto per la sicurezza nazionale quando i dati di accesso vengono compromessi. Aggiunge che l'*age verification* imposta alle piattaforme è altamente inefficace di fronte a una serie di tecnologie economiche e facilmente accessibili, come le reti private virtuali (VPN) nonché inefficace nel geolocalizzare gli individui, con il risultato (soprattutto in prossimità dei confini nazionali) che gli individui non vengono sottoposti alla verifica dell'età perché il fornitore di *age verification* ritiene erroneamente che si trovino al di fuori della regione soggetta ai requisiti e viceversa. **Ritiene che l'età debba essere verificata sul dispositivo personale tramite un'App scelta dall'utente**, evitando di trasmettere o condividere i dati dell'identità personale. Tale App, interposta tra l'identità e la generazione della condizione di utente autorizzato, consente di verificare l'età senza imporre la verifica alle piattaforme, con il vantaggio di evitare tutti i rischi che l'AV imposto alle piattaforme comporta. In via subordinata WEBGROUP ritiene che ogni fornitore dovrebbe essere libero di scegliere i meccanismi di *age verification* ritenuti idonei, e gli utenti dovrebbero essere liberi di scegliere il più conveniente tra i sistemi offerti, fatti salvi, in entrambi i casi, i principi di efficacia e di conformità alla legge. Ritiene che l'Autorità **dovrebbe fornire un elenco di fornitori di servizi AV controllati/certificati**.

WEBGROUP ritiene inoltre che, da un punto di vista di proporzionalità, sia ragionevole **rendere i genitori e i tutor consapevoli, in primo luogo, che i sistemi operativi per computer più diffusi, Microsoft e Apple, includono direttamente funzioni di controllo parentale per impostazione predefinita, senza costi aggiuntivi**. Aggiunge che anche tutti i principali browser, tra cui Google Chrome, Mozilla Firefox, Microsoft Edge e Safari di Apple, dispongono di opzioni di controllo parentale e se i genitori desiderano aggiungere ulteriori funzioni di controllo parentale, possono facilmente acquistare software aggiuntivi come Bark o NetNanny o addirittura scaricare software aggiuntivi gratuiti, come Questodio, Kaspersky Safe Kids, FamilyKeeper e altri. Queste funzioni consentono ai genitori di bloccare l'accesso a materiale sessualmente esplicito sul Web, di impedire ai minori di fornire informazioni personali a sconosciuti via e-mail o nelle chat room, di limitare il tempo di visione dei minori e di mantenere un registro di tutte le attività online su un computer di casa. Aggiunge che i genitori possono anche utilizzare un software di screening che blocca i messaggi contenenti determinate parole, nonché un software di tracciamento e monitoraggio e che possono anche limitare e osservare l'uso di Internet da parte di un minore, semplicemente collocando un computer in uno spazio pubblico all'interno della casa. Tutti questi metodi sono poco costosi (o

gratuiti) e poco invasivi (dal punto di vista del principio di proporzionalità) per ottenere una *age verification* efficace.

WEBGROUP ritiene che allo stato attuale della tecnologia, **il riconoscimento facciale potrebbe non essere tecnicamente sicuro o adeguato**, poiché esiste un ampio margine di errore per quanto riguarda l'età e, inoltre, la raccolta di dati biometrici comporta anche gravi rischi per la privacy degli utenti di Internet.

WEBGROUP ritiene, altresì, necessario aggiungere le definizioni di “controllo parentale”, “filtering” e “verifica dell'età a livello di dispositivo”.

AYLO ritiene che **la vera soluzione per proteggere i minori e gli adulti sia quella di verificare l'età degli utenti nel punto di accesso – ossia nei dispositivi degli utenti⁴ - a livello di sistema operativo** e di negare o consentire l'accesso a materiali e siti web soggetti a restrizioni di età sulla base di tale verifica. Questo approccio richiede la **collaborazione delle aziende produttrici di sistemi operativi** e, con il loro consenso, si avrebbe una riduzione al minimo la trasmissione di dati personali, proteggendo al contempo i minori dai contenuti nocivi agli stessi. Ciò garantirebbe una maggiore facilità di implementazione, poiché i produttori di sistemi operativi sono molti di meno rispetto ai siti web/piattaforma che forniscono contenuti pornografici. Inoltre, si avrebbero maggiori tutele dei dati personali, che non verrebbero gestiti da una moltitudine di siti web, e si garantirebbe una maggiore efficacia della protezione, in quanto l'accesso ai minori sarebbe bloccato verso qualsiasi contenuto pornografico, anche quelli illegali o “estremi”, a prescindere dal fatto che i siti web/piattaforme implementino o meno misure di protezione. Tale soluzione potrebbe essere attuata garantendo che i **produttori dei sistemi operativi blocchino di default i contenuti per adulti**, in modo da proteggere sempre i minori quando accedono ad Internet, e **richiedano la verifica dell'età, a livello di dispositivo, solo quando l'utente richiede l'accesso a contenuti per adulti**.

AYLO evidenzia che, quando la verifica e la stima dell'età vengono effettuate sul dispositivo, gli utenti effettuano tale verifica una sola volta, attraverso il sistema operativo, e non su ogni sito web soggetto a restrizioni di età. In questo modo, si riducono drasticamente i rischi di furto di dati e di privacy e si crea un processo molto semplice da controllare per le autorità di regolamentazione. A parere di **AYLO**, la tecnologia per raggiungere questo obiettivo esiste già oggi, infatti molti dispositivi offrono già **funzioni di controllo parentale gratuite e facili** da usare che possono impedire agli account dei minori di accedere a contenuti per adulti senza rischiare di rivelare dati sensibili dell'utente. Aggiunge che queste funzioni devono semplicemente essere migliorate per garantire un'adeguata verifica o stima dell'età e quindi essere in grado di bloccare i dispositivi per impostazione predefinita, a meno che non siano sbloccate previa verifica o stima dell'età da parte di un adulto sul dispositivo. Infine, ritiene che le soluzioni implementate a livello di dispositivo

⁴ Per verifica dell'età basata su dispositivi **AYLO** intende qualsiasi approccio alla verifica e alla stima dell'età in cui le informazioni personali utilizzate per verificare l'età dell'utente sono condivise di persona presso un rivenditore autorizzato, inserite localmente nel dispositivo dell'utente o memorizzate su una rete controllata dal produttore del dispositivo o dal fornitore del sistema operativo del dispositivo. Attraverso un software di blocco e filtraggio dei contenuti preinstallato, la disabilitazione dei permessi di navigazione sul web o altri mezzi, l'utente non può accedere a contenuti vietati alla sua età su Internet, a meno che non sia stato verificato come avente un'età pari o maggiore. Per essere realizzato, questo approccio richiede la collaborazione degli sviluppatori e dei fornitori di sistemi operativi.

sarebbero le più efficaci dal punto di vista della funzionalità, della facilità d'uso e dell'assenza di impedimenti all'uso, in quanto rimarrebbero circoscritte all'ambiente nel dispositivo, che viene scelto e impostato in base alle esigenze dell'utente, per di più in un ambiente digitale ben conosciuto.

AYLO sostiene che, sebbene un l'approccio di implementare la verifica dell'età a livello di sito web/piattaforma possa funzionare per aziende strutturate ed eticamente orientate come la stessa AYLO, ciò potrebbe portare a una situazione rischiosa in cui siti che non rispettano standard etici o che hanno poca esperienza nel campo, implementerebbero sistemi di verifica dell'età e di stima dell'età inefficaci o non sicuri, facilmente aggirabili o capaci di raccogliere i dati personali degli utenti. In generale, **non ritiene che i metodi di verifica e di stima dell'età a livello di sito web siano efficaci**. Sostiene che, come dimostrato da altre giurisdizioni che hanno implementato soluzioni a livello di sito web, queste si sono rivelate inefficaci in quanto i minori sono ancora in grado di accedere facilmente e agilmente a materiale per adulti online, perché la conformità a tali requisiti è soddisfatta solo da una o poche piattaforme per adulti e la loro implementazione risulta scarsa. Alla luce di quanto sopra, **ritiene che l'unica soluzione efficace per impedire l'accesso dei minori ai contenuti per adulti sia la verifica dell'età effettuata a livello di dispositivo attraverso il sistema operativo**, in cui l'impostazione predefinita per tutti gli account e tutti i dispositivi del sistema operativo sia quella di blocco dei contenuti per adulti.

AYLO sostiene che sia difficile poter considerare proporzionato qualsiasi meccanismo di *age assurance* implementato a livello di sito web/piattaforma, ad eccezione del metodo dell'autodichiarazione. Ritiene che i sistemi di *age assurance* a livello di sito web diversi dalle autodichiarazioni non rappresentano misure proporzionate alla luce della quantità di rischi che creano e del danno che causano tanto agli utenti interessati quanto al sostentamento commerciale dei fornitori di piattaforme di condivisione video. In questo contesto, sottolinea che, nel caso di verifica dell'età implementata a livello di sito web, il rischio è che chiunque, compreso un minore, venga spinto verso siti non conformi (ossia che decidono di non implementare tale verifica), ed è molto probabile che l'utente, anche minorenni, venga così esposto a contenuti illeciti ed "estremi" con cui, altrimenti, non sarebbe mai entrato in contatto. Pertanto, le conseguenze sociali negative nel caso di adozione di un simile strumento sarebbero dunque significative e del tutto inaccettabili, **pur essendo del tutto evitabili attraverso l'implementazione di controlli a livello di dispositivo**. Ritiene che i sistemi di verifica dell'età e di stima dell'età implementati a livello di sito web sono sempre **sproporzionati**, nella misura in cui l'obiettivo finale è quello di prevenire i rischi per i minori. Inoltre, sostiene che i sistemi di verifica e di stima dell'età a livello di sito web sono sproporzionati anche in considerazione dei diritti e delle libertà economiche delle piattaforme. Infatti, ritiene che qualsiasi richiesta di implementare un requisito di certificazione dell'identità sulle loro piattaforme porterebbe inevitabilmente a una perdita quasi totale di visitatori delle piattaforme stesse, che semplicemente passerebbero a fare altro e, di conseguenza, l'esistenza stessa delle piattaforme verrebbe messa a rischio, poiché non avrebbero quasi alcuna possibilità di sopravvivere alla perdita totale di traffico sulle stesse.

META è del parere che si possa fare un significativo passo avanti a livello europeo per garantire che i genitori debbano verificare l'età del proprio figlio una sola volta e che il minore abbia

successivamente accesso a un'esperienza adatta alla propria età in ogni singola app. **Ritiene che**, invece di obbligare i genitori a rintracciare le numerose applicazioni esistenti e tutte quelle che verranno sviluppate nei prossimi anni, **la verifica dell'età dovrebbe poter essere effettuata direttamente nel luogo (virtuale) in cui gli adolescenti scaricano l'applicazione stessa (app store o a livello di sistema operativo)**. Secondo l'operatore questo approccio ridurrebbe l'onere per i genitori di individuare le molteplici app utilizzate dai propri figli e destreggiarsi tra i diversi sistemi di verifica dell'età, minimizza il numero di volte e di spazi (virtuali) in cui dover condividere dati potenzialmente sensibili per verificare l'età. Inoltre, i genitori e gli adolescenti non sarebbero costretti a fornire i propri documenti di identità a tutte le applicazioni in circolazione per verificare la propria età o quella dei loro figli. Peraltro, fa notare che gli adolescenti e i genitori forniscono già ai **gestori degli app store** queste informazioni al momento dell'acquisto dei dispositivi e della creazione degli account, i quali hanno già integrato nei propri *app store* sistemi di notifica, revisione e approvazione che potrebbero essere utilizzati direttamente da parte dei genitori. **Ritiene, pertanto, che verificare l'età di un adolescente a livello di app store garantirebbe che le app scaricate dall'app store debbano rispettare gli stessi standard di protezione e fornire di conseguenza contenuti ed esperienze adatti all'età riscontrata**. Allo stesso tempo si favorirebbe anche un mercato più sano e competitivo, in quanto **l'obbligo di verificare l'età al momento dell'iscrizione per ogni singola app** creerebbe una barriera significativa all'ingresso e un ostacolo insormontabile allo sviluppo di nuovi attori sul mercato. Infine, ritiene che facilitare la verifica dell'età per le nuove app che si rivolgono agli adolescenti non solo favorirebbe la concorrenza, ma fornirebbe ai genitori una maggiore garanzia rispetto alla conformità agli obblighi normativi di tutte le app, anche di quelle di cui non hanno mai sentito parlare.

[OMISSIS – Un operatore] ritiene che un Operatore di rete disponga di informazioni sufficienti a svolgere un efficace processo di *age verification* solo in determinate condizioni, in quanto nella gran parte dei casi non avrebbe alcun modo di determinare con certezza se l'utente (ovvero il reale utilizzatore) sia maggiorenne o minorenni. Inoltre, non potrà in alcun modo essere ritenuto responsabile laddove il maggiorenne non si attivi per tutelare il minore dall'accesso a contenuti sensibili o nel caso in cui un minore decida attivamente di eludere i meccanismi di sicurezza posti a tutela dello stesso. Una soluzione potrebbe essere la verifica dell'età tramite informazioni contrattuali associate all'indirizzo IP utilizzato dall'utente. Tale soluzione consentirebbe di mettere in relazione l'Indirizzo IP utilizzato dall'utente durante la navigazione con le informazioni contrattuali dell'intestatario della SIM a disposizione dell'Operatore. La verifica tramite indirizzo IP richiede una necessaria distinzione tra la navigazione da parte dell'utente tramite una rete mobile o una rete fissa. Nel caso di una navigazione su rete mobile sarebbe possibile confrontare l'indirizzo IP dinamico dell'utente con le informazioni contrattuali a disposizione dell'Operatore solamente per un sottogruppo di utenti che richiedono la prova dell'età da rete mobile. Infatti, **ai fini della *age verification*, l'Operatore sarebbe in grado di determinare con certezza se l'utente è minorenni solamente nel caso di un utente che utilizzi una SIM "Junior" intestata al minorenni stesso**. In questo caso, [OMISSIS – Un operatore] spiega che l'IP dinamico usato dall'utente Junior (intestatario di una "SIM Junior") per navigare su rete mobile verrebbe associato dall'Operatore alla SIM di un minorenni, con conseguente KO sulla prova dell'età. Al contrario, laddove l'IP dinamico risultasse associato ad una SIM intestata ad un maggiorenne (ad es. nel caso del padre che si intesta

la SIM e la fa usare al figlio minorenni o nel caso di un utente maggiorenne) l'Operatore approverebbe **la prova dell'età sulla base dell'età anagrafica dell'intestatario della SIM, senza però avere certezza che il reale utilizzatore della SIM è un minorenni o un maggiorenne**. Nel caso di navigazione su rete fissa l'Operatore non avrebbe nessun modo di risalire all'età dell'utente che si appoggia all'indirizzo IP della rete fissa (ad esempio tramite Wi-Fi o tramite cavo Ethernet). Questo perché tutte i contratti di rete fissa sono per definizione intestati a clienti maggiorenni. Un'altra possibilità, spiega l'operatore, è la verifica tramite Parental Control, che laddove attivo sul dispositivo, consente di filtrare l'accesso a contenuti sensibili a livello di rete e di applicativi (ad es. tramite blocchi DNS o blocchi IP). La verifica tramite il Parental Control avverrebbe attraverso l'interrogazione dei database interni di **[OMISSIS – Un operatore]**, ovvero verificando se sulla numerazione che richiede l'accesso sia attivo il Parental Control o meno. Tuttavia, in linea con quanto già argomentato sopra, anche il caso di utilizzo del Parental Control come meccanismo di *age verification*, richiede una distinzione tra navigazione tramite rete mobile o tramite rete fissa, in quanto il sistema viene attivato direttamente sulla SIM. Nel caso di navigazione su rete mobile con una SIM Junior, il Parental Control viene pre-attivato di default e pertanto l'utente minorenni viene sempre tutelato, in quanto questo meccanismo impedisce l'accesso alle piattaforme prese in esame. Nel caso di una SIM non Junior, sarà in capo al genitore del minorenni la responsabilità di attivare il Parental Control sul dispositivo del minorenni. Pertanto, la verifica dell'età tramite Parental Control risulterebbe efficace solamente nel caso di utenti minorenni che risultano intestatari di una SIM Junior, per i quali è obbligatorio l'utilizzo del meccanismo di Parental Control. Al contrario, **[OMISSIS – Un operatore]** spiega che non avrebbe nessun modo di determinare se l'utente – utilizzatore di una SIM intestata ad un maggiorenne ma senza il Parental Control attivo – sia effettivamente maggiorenne o minorenni. Invece, evidenzia che nel caso di navigazione su rete fissa, poiché le utenze di rete fissa sono tutte intestate a maggiorenni, sarà in capo al genitore del minorenni la responsabilità di attivare i meccanismi di Parental Control sulla rete fissa e pertanto, all'utente minorenni verrà automaticamente bloccato l'accesso alle piattaforme a contenuti pornografici in tutti i casi in cui il Parental Control venga attivato sulla rete fissa dall'intestatario del contratto. Al contrario, al minore verrà garantito l'accesso al sito/piattaforma in tutti i casi in cui l'intestatario della rete fissa (maggiorenne) non attiva il Parental Control sulla rete fissa. Inoltre, segnala che l'operatore non avrà modo di verificare l'età dell'utilizzatore e per distinguere tra un utente maggiorenne o minorenni che si appoggia alla rete fissa (tramite Wi-Fi o tramite cavo Ethernet).

B. Valutazioni dell'Autorità

L'Autorità prende atto della proposta del GARANTE PER L'INFANZIA laddove ritiene che l'adozione di un sistema basato sull'utilizzo di una identità digitale di tipo SPID consenta di garantire un elevato grado di certezza nel determinare l'età dell'utente e, al contempo, nel rispetto del principio di proporzionalità. Tale soluzione potrebbe risultare appropriata laddove i fornitori mettessero a disposizione una funzione aggiuntiva di "prova dell'età" con garanzia dell'anonimato rispetto ai siti web e piattaforme a cui l'utente ha necessità di accesso.

Si prende atto altresì del fatto che le associazioni e i fornitori privati, WEBGROUP, AYLO, META, ritengono che **l'*age verification* debba essere effettuata in maniera più efficiente a livello di dispositivo dell'utente, ad esempio sotto forma di software di filtraggio (APP), anziché a livello di sito web (viene portato ad esempio il caso spagnolo). In altri casi si propone di verificare l'età nei dispositivi degli utenti a livello di sistema operativo** seppur si riconosce che questo approccio richiede la **collaborazione delle aziende produttrici di sistemi operativi. Un rispondente in particolare ritiene che la verifica dell'età dovrebbe poter essere effettuata direttamente nel luogo (virtuale) in cui gli adolescenti scaricano l'applicazione stessa (app store o a livello di sistema operativo).**

A tale riguardo, da un punto di vista giuridico l'Autorità osserva che il quadro normativo in materia di sistemi di verifica dell'età, e da ultimo lo stesso decreto-legge 123/2023 come convertito in legge, non prevede un obbligo in capo ai fornitori di terminali, di APP store, e di sistemi operativi o browser, bensì in capo a fornitori di siti web e piattaforme di video sharing. Con riferimento ai rischi per la sicurezza dei dati paventato da WEBGROUP, l'Autorità fa rilevare che l'approccio proposto in consultazione pubblica non prevede alcun trasferimento di informazioni personali e sensibili al sito web o piattaforma. La verifica dell'età è, infatti, fatta dal soggetto certificato che è già in possesso dei dati dell'utente (modello del soggetto terzo indipendente).

Con riferimento all'osservazione secondo cui sarebbe sufficiente basarsi sui sistemi di controllo parentale previsti dai sistemi operativi dei terminali, l'Autorità rinvia a quanto riportato nella delibera n. 9/23/CONS oltre che nello stesso articolo 13 del decreto-legge 123 del 2023 come convertito in legge. A livello generale è già previsto un obbligo in capo ai fornitori di servizi di comunicazione elettronica e in capo ai fornitori di terminali di implementare un sistema di *parental control*. Tuttavia, il legislatore ha comunque ritenuto di prevedere un sistema di *age verification* realizzato dai fornitori di siti web e piattaforme di video sharing, tra l'altro, in linea con le previsioni del TUSMA e del DSA prima richiamate.

L'Autorità ritiene comunque interessanti le soluzioni proposte basate sui sistemi operativi, sul browser (come in Spagna) e sulla etichettatura dei contenuti dei siti, non escludendo che possano contribuire a creare, in futuro, un ambiente *online* sicuro per i minori. L'Autorità ritiene opportuno, a tale proposito, istituire un tavolo tecnico di monitoraggio delle soluzioni tecniche, con la collaborazione di tutti i soggetti istituzionali e privati potenzialmente coinvolti. Il presente provvedimento, tuttavia, deve essere ancorato alle attuali previsioni di legge che pongono obblighi di tutela in capo ai fornitori di siti web e alle piattaforme di video sharing con la cautela di fissare una disciplina che sia proporzionale e rispettosa dei dati personali degli utenti.

L'Autorità, pertanto, conferma la previsione di un sistema di verifica dell'età realizzato dalla piattaforma di video sharing o gestore del sito web sulla base del modello proposto in consultazione in cui è escluso il trasferimento di dati degli utenti presso la piattaforma o sito visitati.

Con riferimento alla richiesta di qualche rispondente che ritiene che l’Autorità **dovrebbe fornire un elenco di fornitori di servizi AV controllati/certificati si rappresenta quanto segue.**

L’Autorità ritiene opportuno evidenziare che ogni sito web o piattaforma che rientra nell’ambito soggettivo e oggettivo di applicazione del presente provvedimento, o che comunque in modo volontario decida di applicare le presenti specifiche tecniche (come meglio chiarito nella sezione sull’ambito di applicazione), debba individuare il soggetto che sia in grado di fornire una prova dell’età in modo certificato nel rispetto dei requisiti di legge.

Ai fini dell’attività di vigilanza l’Autorità ritiene opportuno seguire un approccio analogo a quello utilizzato con la delibera n. 9/23/CONS, in tal caso con riferimento alle società che sono utilizzate dagli operatori per individuare i siti e domini da filtrare.

Si stabilisce, pertanto, che i fornitori di siti web e piattaforme che diffondono contenuti a carattere pornografico, ai sensi dell’art. 13 bis del decreto-legge 123/2023 come modificato in sede di conversione in legge, devono comunicare all’Autorità i soggetti terzi a cui è affidata l’attività di verifica dell’età unitamente a una dettagliata relazione contenente la descrizione delle competenze, delle modalità di verifica dell’età utilizzate e delle ragioni della scelta.

V. **SULLA LIBERTÀ’ DI SCELTA DEI SISTEMI DI VERIFICA DELL’ETA’ DA PARTE DEI SOGGETTI REGOLAMENTATI**

A. Osservazioni di soggetti istituzionali, operatori e associazioni

Il CNU valuta positivamente che sia il soggetto tenuto ai sensi dalla legge a scegliere gli strumenti di verifica dell’età da implementare nel proprio servizio, utilizzando uno strumento per quanto possibile non invasivo per raggiungere l’obiettivo prefissato, e a dimostrare l’efficacia dello strumento utilizzato secondo i requisiti fissati dall’Autorità, anche nel rispetto del principio di accountability previsto dal GDPR.

ALTROCONSUMO ritiene opportuno che l’Autorità circoscriva l’ambito di scelta da parte dei soggetti regolamentati a una rosa di **massimo tre sistemi di verifica** dell’età da essa previamente selezionati in base ai principi e requisiti fissati in quanto sostiene che lasciare alla piena discrezionalità dei soggetti interessati la scelta tra sistemi e processi tanto dissimili – e che comportano un dislivello in termini di sicurezza e garanzie – porterebbe a risultati non attendibili e a disparità di trattamento degli utenti.

[**OMISSIS – Un operatore**] condivide che debbano essere i soggetti regolamentati a scegliere quale modalità di *Age Verification* debba essere implementata, purché a valle del presente procedimento **vengano comunque previste un set di diverse modalità che siano ritenute compatibili con i**

principi e i requisiti stabiliti da codesta Autorità. È opinione dell'operatore che l'Autorità dovrebbe fornire ai soggetti regolamentati un "ventaglio" di opzioni per la verifica dell'età, lasciando che sia il singolo sito/piattaforma a scegliere di volta in volta quale servizio di *Age Assurance* utilizzare, sulla base di appositi accordi contrattuali con i relativi providers.

B. Valutazioni dell'Autorità

L'Autorità prende atto della condivisione, da parte dei rispondenti, dell'approccio proposto in consultazione in cui resta in capo al fornitore di piattaforme di video sharing e siti web di selezionare il sistema di verifica dell'età appropriato che risulti, comunque, conforme alle disposizioni fornite in questo provvedimento.

L'Autorità non ritiene, tuttavia, opportuno indicare una ristretta rosa di sistemi ritenuti obbligatori in quanto, allo stato, potrebbe rappresentare una misura non proporzionata e non conforme ai generali principi di neutralità tecnologica e libertà d'impresa.

VI. SULLE TEMATICHE RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI

A. Osservazioni di soggetti istituzionali, operatori e associazioni

AYLO sottolinea che l'art. 9, comma 1 del GDPR considera tutti i dati personali relativi all'orientamento sessuale di una persona interessata come una categoria particolare di dati personali e che questi dati personali sono particolarmente sensibili. In quanto tali, essi godono di una tutela speciale ai sensi del GDPR ossia il requisito secondo cui i dati devono essere limitati a quanto necessario deve dunque assumere un valore pregnante nel caso dei trattamenti concernenti dati personali sensibili. Ritiene che data l'assoluta mancanza di benefici comprovati in relazione all'utilizzo di rigidi sistemi di certificazione dell'identità/age-gating a livello di sito web, **non è né adeguato né pertinente né sorretto da un principio di necessità ai sensi dell'art. 5 del GDPR, ipotizzare di poter raccogliere e memorizzare i dati personali degli utenti ogni volta che un utente visita un sito web di contenuti per adulti e ciò è tanto più vero alla luce del fatto che i dati trattati nel caso specifico sono altamente sensibili**, in quanto si riferiscono al consumo di contenuti sessualmente espliciti da parte di un individuo. Se tali dati diventassero pubblici, ciò potrebbe avere conseguenze significative sulla loro vita familiare, sociale e professionale. I sistemi di certificazione dell'identità possono danneggiare in modo sostanziale il diritto all'autodeterminazione degli utenti dei siti web rispetto ai propri dati. I dati raccolti attraverso tali sistemi aumentano significativamente il rischio di *hacking* di tali dati. Inoltre, il rischio di *hacking* dei sistemi di certificazione dell'identità riguarda in particolare gruppi vulnerabili come la comunità LGBT+. Inoltre, la normalizzazione della pratica di **caricamento di dati personali per accedere ai siti web comporta rischi significativi, in quanto può portare a violazioni della privacy, furti di identità e uso non autorizzato di dati sensibili, evidenziando l'importanza della salvaguardia dei dati personali nell'era digitale.**

L'attribuzione di questa responsabilità alla piattaforma o alle piattaforme visitate da un utente implica che gli utenti inviino più volte informazioni private per accedere a diversi siti per adulti, normalizzando la divulgazione di dati personali su Internet e creando un rischio di furto di identità dei dati potenzialmente irreparabile a livello globale. **Per quanto riguarda le tematiche relative alla privacy, ritiene che i sistemi operativi offrano oggi agli utenti la possibilità di limitare la raccolta della cronologia di navigazione e di altri dati, fornendo un livello di protezione della privacy gestito direttamente dall'utente.** Questa autonomia è assente nei sistemi di verifica dell'età a livello di sito web, che spesso operano con politiche di conservazione e utilizzo dei dati poco trasparenti. In conclusione, ritiene che **i sistemi di verifica dell'età implementati a livello di dispositivo e di stima dell'età offrirebbero un metodo più sicuro e rispettoso della privacy, allineandosi al principio della minimizzazione dei dati e garantendo agli utenti un maggiore controllo sulle loro informazioni personali.**

WEBGROUP ritiene che ad oggi non esista alcun sistema proposto dall'*age verification* in grado di garantire la protezione della privacy degli utenti. La condivisione dell'identità ai fini dell'accesso a un sito per adulti provoca inevitabilmente il collegamento dell'identità di qualsiasi utente al suo presunto orientamento o preferenza sessuale, che è la quintessenza della violazione della privacy e che espone a rischi elevati, compresa la sicurezza nazionale. Sostiene, invece, che **la verifica dell'utente a livello di dispositivo tramite software di filtraggio evita tali problemi perché riduce al minimo la quantità di dati condivisi** e non li associa all'accesso dell'individuo ai siti web pornografici e che non vengono raccolti altri dati oltre a quelli che normalmente vengono raccolti per configurare un dispositivo. Inoltre, tali dati non vengono memorizzati o condivisi online, ma conservati localmente sul dispositivo, mantenendo una privacy ottimale. Indipendentemente dalla modalità di esecuzione, *l'age verification* - sia attraverso (i) la raccolta diretta di documenti di identità da parte dell'editore del sito pornografico; (ii) la stima dell'età basata sulla cronologia di navigazione dell'utente Internet; (iii) l'elaborazione di dati biometrici allo scopo di identificare o autenticare una persona fisica (ad esempio, confrontando, attraverso la tecnologia di riconoscimento facciale, una fotografia mostrata su un documento d'identità con un autoritratto o un selfie); o (iv) **attraverso l'uso di ID digitali, come SPID, forniti in ambito pubblico** - rappresenta **una violazione della privacy** ove la tecnologia sia limitata e non abbastanza avanzata da proteggere e preservare i diritti fondamentali. Infatti, richiedere ai siti web di impegnarsi nell'AV o di utilizzare fornitori di AV terzi crea depositi di informazioni altamente sensibili e personalmente identificabili, che sono obiettivi lucrativi per gli hacker. **A questo proposito fa notare che i meccanismi di doppio anonimato AV costituiscono un'opzione interessante ma non ancora matura** e che, una volta sviluppati e testati debitamente, le autorità dovrebbero creare certificazioni per vagliare i fornitori di servizi ritenuti più sicuri/efficienti, non in un singolo Paese o in una selezione di Paesi, ma in modo coordinato e quantomeno in tutta l'Unione Europea.

ALTROCONSUMO ritiene che alcuni sistemi di verifica dell'età, tra cui quelli che prevedono la raccolta diretta di documenti o il trattamento di dati biometrici, debbano essere esclusi. **Non ravvisa particolari criticità nell'utilizzo delle identità digitali come lo SPID** in quanto si tratta di un sistema di riconoscimento e verifica collaudato e protetto. Quanto alla stima dell'età basata sulla cronologia di navigazione, ritiene che il soggetto chiamato alla verifica si ritroverebbe ad utilizzare

dati personali che già vengono potenzialmente trattati nelle operazioni di profilazione messe in atto dal soggetto stesso o da terze parti, per cui non ravvisa particolari criticità nell'utilizzo dello strumento in sé ma ritiene fondamentale la predisposizione di misure di pseudonomizzazione che non permettano di risalire all'identità del minore ma solo di rilevare elementi statisticamente ricorrenti nella navigazione dei soggetti di minore età.

B. Valutazioni dell'Autorità

L'Autorità rileva che **alcuni rispondenti, in rappresentanza di fornitori di piattaforme di video sharing e siti web, ritengono che il caricamento di dati personali per accedere a dette piattaforme e siti web comporti rischi significativi, in quanto può comportare a violazioni della privacy, furti di identità e uso non autorizzato di dati sensibili.** Pertanto, ritengono che **i sistemi di verifica dell'età implementati a livello di dispositivo offrirebbero un metodo più sicuro e rispettoso della privacy, allineandosi al principio della minimizzazione dei dati e garantendo agli utenti un maggiore controllo sulle loro informazioni personali.**

A questo proposito detti rispondenti ritengono che i meccanismi di doppio anonimato AV costituiscano un'opzione interessante ma non ancora matura e che, una volta sviluppati e testati debitamente, le autorità dovrebbero creare certificazioni per vagliare i fornitori di servizi ritenuti più sicuri/efficienti, non in un singolo Paese o in una selezione di Paesi, ma in modo coordinato e quantomeno in tutta l'Unione Europea.

Una associazione dei consumatori non ravvisa particolari criticità nell'utilizzo delle identità digitali come lo SPID in quanto si tratta di un sistema di riconoscimento e verifica collaudato e protetto.

L'Autorità condivide l'opinione dei rispondenti in relazione al fatto che non sia **adeguato, ai sensi dell'art. 5 del GDPR, ipotizzare di poter raccogliere e memorizzare i dati personali degli utenti ogni volta che viene visitata una piattaforma o un sito web con contenuti per adulti e ciò è tanto più vero alla luce del fatto che i dati trattati nel caso specifico sono altamente sensibili.** A tale riguardo l'Autorità, proprio in virtù dei rischi per la tutela dei dati personali evidenziati, ritiene opportuno confermare l'adozione di un sistema basato sulla verifica dell'età da parte di un soggetto indipendente certificato senza il trasferimento di dati personali al fornitore dei contenuti.

Resta fermo, come detto, l'interesse su sistemi basati su verifiche dell'età e filtraggio a livello del dispositivo seppur tali sistemi esulano dall'ambito del presente provvedimento in cui vanno stabilite le specifiche di processo e di sistema che restano in capo ai fornitori di piattaforme di video sharing e siti web che diffondono contenuti a carattere pornografico.

Si ribadisce che il sistema SPID, **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 indicate nell'Allegato A (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.** Pertanto, come illustrato negli allegati A e B, necessita di opportuni adeguamenti.

A tale riguardo l’Autorità ritiene opportuno includere, tra i sistemi idonei ai fini della *age assurance*, anche le soluzioni basate sul Digital Wallet richiamato nelle premesse del provvedimento di adozione delle specifiche tecniche. Ciò in quanto le soluzioni tecniche sono al vaglio della task force della Commissione europea e soddisfano allo stesso tempo i requisiti di tutela della privacy, non prevedendo alcun caricamento di dati dell’utente presso il sito o piattaforma visitati, e di armonizzazione delle soluzioni a livello Europeo. La soluzione inoltre utilizza una specifica applicazione installata nel cellulare dell’utente la quale consente di condividere, nell’ambito delle informazioni di identità digitale, con la piattaforma/sito il solo attributo di età- (ossia la prova della maggiore età). Si ritiene che trattasi di una soluzione che risponde alle preoccupazioni illustrate dai rispondenti istituzionali e privati.

VII. SULL’INTERVENTO DI SOGGETTI TERZI INDIPENDENTI

A. Osservazioni di soggetti istituzionali, operatori e associazioni

Il GARANTE PER L’INFANZIA ritiene che **l’impiego di soggetti terzi rispetto a coloro che gestiscono i siti e le piattaforme online, cui affidare il compito dell’accertamento dell’età degli utenti e il rilascio di una conseguente identità digitale certificata, offre diversi e significativi vantaggi**. Ritiene che questo approccio contribuisca a garantire un maggiore livello di imparzialità e affidabilità nel processo di verifica dell’età in quanto le entità esterne e indipendenti dalle piattaforme online, possono operare con un grado maggiore di trasparenza e obiettività, riducendo al minimo il rischio di conflitti di interesse o manipolazioni. Inoltre, in quanto soggetti specializzati, possono essere destinatari di rigorose norme e regolamenti in materia di protezione dei dati e, al contempo, favorire una maggiore coerenza e uniformità nel processo di verifica dell’età su diverse piattaforme e servizi online. Tutto ciò può contribuire a garantire che i minori possano essere protetti in modo uniforme e coerente in qualunque ambito del mondo digitale.

Il CNU valuta **assolutamente coerente con gli obiettivi di proporzionalità, protezione dei dati personali e sicurezza, devolvere a soggetti terzi indipendenti** (siano essi fornitori di servizi specializzati nella fornitura di identità digitale o un’organizzazione che ha identificato l’utente di Internet in altro contesto come una banca, un’amministrazione pubblica, ecc.) l’emissione di una “prova dell’età” certificata. Conviene, quindi, che non siano direttamente i siti e le piattaforme soggette all’obbligo di verifica dell’età ad effettuare direttamente le operazioni di verifica. Ritiene opportuno che una volta emessa la prova d’età certificata, essa venga fornita all’utente affinché questi abbia accesso o meno al contenuto richiesto sul sito o sulla piattaforma visitata. Sottolinea l’opportunità e la minimizzazione dei rischi di tale metodo di accertamento dell’età degli utenti, in quanto il soggetto che rilascia la prova dell’età non conosce il particolare sito o piattaforma che vuole visitare l’utente, e allo stesso tempo, il sito o piattaforma visitata acquisirà la prova dell’età senza venire a conoscenza dell’identità dell’utente in quanto non ci sarà trasmissione di dati identificativi dell’utente. Il CNU sottolinea, inoltre, la delicatezza dell’ulteriore passaggio attraverso cui i siti e le piattaforme interagiscono con il soggetto terzo indipendente essendo auspicabile che i fornitori dei

contenuti si dotino di strumenti chiari ed idonei volti ad acquisire ed implementare il sistema di verifica dell'età, al fine di decifrare la firma e stabilirne l'autenticità.

Il FAF ritiene che l'obiezione più comune verso l'adozione dei sistemi di *age verification* sia la violazione della privacy di chi si connette, che sarebbe obbligato a comunicare i propri dati personali contenuti in un documento d'identità. Per ovviare a tale problema **la soluzione praticabile è utilizzare un terzo attore** che sia garante di tali dati (sul modello dello SPID). Sottolinea che certamente si tratta di un'ipotesi più impegnativa in termini tecnologici, e anche economici, ma se si trattasse dell'unica strada in grado di mettere d'accordo tutti gli attori coinvolti andrebbe senz'altro promossa.

ALTROCONSUMO sottolinea la rilevanza di avere terze parti autorevoli e consiglia di affidare la funzione certificatrice a soggetti che già si occupano di identificazione e certificazione come le società che forniscono l'identità digitale, la firma digitale, la PEC mail in modo tale che ogni utente può scegliere a quale soggetto rivolgersi per munirsi della "prova dell'età". **Suggerisce, pertanto, aggiungere il servizio "prova dell'età" a quelli già forniti dai provider di identità digitale, firma digitale e PEC mail** dal momento in cui l'utente di uno o più dei suddetti servizi è già stato identificato, e la "prova dell'età" può essere emessa in automatico nell'area personale.

[OMISSIS – Un operatore] ritiene condivisibile che venga utilizzato un principio di indipendenza del fornitore in quanto tale meccanismo risponde anche alle esigenze del Regolamento GDPR, minimizzando la quantità di dati trattenuti dai siti/piattaforme che offrono contenuti pornografici e impedendo al soggetto terzo indipendente di venire a conoscenza del sito/servizio a cui vuole accedere l'utente. Ritiene, altresì, essenziale la definizione di un quadro normativo che consenta ai soggetti regolamentati di scegliere quale modalità di *Age Assurance* utilizzare e che non ribalti sugli Operatori di comunicazione elettronica l'obbligo ad assicurare la tutela dell'utente minorenni. **Pertanto, si rende disponibile ad assumere un ruolo di terza parte indipendente, in linea con quanto proposto nell'ambito della consultazione pubblica.** Ciononostante, per le motivazioni sopra esposte, ritiene che la fornitura di servizi di *Age Verification* da parte degli Operatori di comunicazione elettronica debba offerta su base volontaria e unicamente a fronte di una remunerazione economica da parte dei soggetti regolamentati. Infine, ritiene necessario l'imposizione di un periodo tecnico di almeno 12 mesi per consentire l'adeguamento alle nuove disposizioni e per l'implementazione tecnica, decorrenti dalla data di pubblicazione del provvedimento finale a valle della consultazione pubblica. Ritiene, altresì, che laddove gli Operatori TLC dovessero essere identificati come soggetti terzi indipendenti che discrezionalmente decidono di offrire tali servizi di *Age Verification*, sia da subito specificato dalla normativa di settore che le necessarie attività di *Age Verification* siano adeguatamente e sistematicamente remunerate dai soggetti regolamentati, sulla base di accordi commerciali. Sarebbe infatti paradossale che a fronte di un obbligo in capo ai soggetti regolamentati, i costi/investimenti da parte dei fornitori delle relative soluzioni tecniche per soddisfare i suddetti obblighi fossero in capo a quest'ultimi. Infatti, a livello tecnico l'Operatore dovrebbe infatti dotarsi di un sistema ad oggi non disponibile – che richiederà il sostenimento di investimenti oltre che costi ricorrenti - per evadere ciascuna richiesta da parte dei soggetti regolamentati. Sostiene che tale servizio sia da considerarsi,

per il soggetto terzo indipendente, un servizio commerciale, che l'Operatore può scegliere liberamente se offrire sul mercato sulla base di accordi commerciali con i soggetti regolamentati a fronte di una previsione normativa di obbligo a riconoscere un corrispettivo economico.

AYLO rappresenta di non essere in grado di valutare le attività dei fornitori terzi, tuttavia, ritiene che le problematiche relative ai sistemi di verifica o di stima dell'età implementati a livello di sito web siano le stesse, indipendentemente dal fatto che il loro funzionamento sia posto a carico della piattaforma o di un fornitore terzo. Tali terze parti, infatti, proprio come la piattaforma, sarebbero obbligate a svolgere attività di trattamento dei dati non proporzionate. Sostiene che, per le stesse ragioni legate alla sensibilità delle informazioni raccolte, questo tipo di servizio non potrebbe nemmeno essere ragionevolmente delegato a soggetti terzi controllati da enti pubblici o comunque soggetti a autorizzazione pubblica. **Ciò nonostante, ritiene comunque necessario coinvolgere terze parti che sviluppano sistemi operativi ("SSO").**

B. Valutazioni dell'Autorità

L'Autorità prende atto della generale condivisione, da parte dei rispondenti istituzionali e operatori, di un approccio basato su un soggetto terzo certificato o certificabile.

Si prende atto del fatto che qualcuno suggerisce di aggiungere il servizio "prova dell'età" a quelli già forniti dai provider di identità digitale, firma digitale e PEC e-mail dal momento in cui l'utente di uno o più dei suddetti servizi è già stato identificato, e la "prova dell'età" può essere emessa in automatico nell'area personale.

Non si condivide l'osservazione del rappresentante di fornitori di piattaforme/siti laddove ritiene che le problematiche relative alla verifica o stima dell'età implementati a livello di piattaforma/sito web siano le stesse, indipendentemente dal fatto che il loro funzionamento sia posto a carico della piattaforma/sito o di un fornitore terzo. Tali terze parti, infatti, proprio come la piattaforma/sito, sarebbero obbligate a svolgere attività di trattamento dei dati non proporzionate. Infatti, l'Autorità ha tale riguardo chiarito che il soggetto terzo è di norma già in possesso dei dati degli utenti per tutti gli scopi previsti dalla legge. Si tratterebbe di aggiungere, tra le informazioni di identità digitale, l'attributo di età da condividere in fase di accesso alla piattaforma/sito.

L'Autorità, alla luce delle favorevoli posizioni espresse dai soggetti istituzionali rispondenti e delle problematiche relative alla tutela dei dati personali sollevate da altri rispondenti, conferma la necessità di un sistema basato sulla presenza di un soggetto terzo certificato, incluso i fornitori di sistemi di identità digitale.

L'Autorità ritiene, come già detto, condivisibile che l'intervento come soggetto terzo di una entità privata, come un operatore di comunicazioni elettroniche, debba avvenire su base di offerta di servizi soggetta a negoziazione commerciale, non essendo gli operatori telefonici soggetti all'obbligo di legge della verifica dell'età.

Nell'ambito di una architettura basata su un soggetto terzo, l'Autorità ritiene condivisibile che, tra le opzioni possibili, vi sia quella di aggiungere il servizio "prova dell'età" a quelli già forniti dai provider di identità digitale, firma digitale e PEC e-mail dal momento in cui l'utente di uno o più dei suddetti servizi è già stato identificato, e la "prova dell'età" può essere emessa in automatico nell'area personale.

Avuto riguardo alla richiesta di prevedere un periodo di implementazione di 12 mesi l'Autorità fa rilevare che la tempistica concessa per la realizzazione dei sistemi di cui al presente provvedimento è stabilita dal comma 4 dell'art. 13 bis citato.

VIII. SUL TEMA DELLA SICUREZZA DEI SISTEMI

A. Osservazioni di soggetti istituzionali, operatori e associazioni

META ritiene che la collaborazione dell'intero settore sul tema permetterebbe di garantire esperienze sicure e adatte all'età, prevenendo allo stesso modo la migrazione dei giovani su App meno sicure di quelle che hanno investito in sicurezza ed esperienze adatte all'età.

AYLO ritiene che i sistemi di verifica dell'età e di stima dell'età a livello di sito web comporterebbero un danno significativo, una violazione dei principi di protezione dei dati e un rischio enorme per il diritto all'autodeterminazione degli utenti del sito web, creando inutili rischi di hacking per la grande quantità di dati personali altamente sensibili degli utenti che dovrebbero essere raccolti. Evidenzia che i dati personali sono attraenti per i malintenzionati, pertanto i rischi di attacchi di phishing, furto d'identità, violazione dei dati e frode, aumentano man mano che gli utenti condividono le loro informazioni con un numero sempre maggiore di siti web e fornitori di servizi di verifica e stima dell'età online. **Sottolinea ancora una volta che la soluzione migliore per mitigare i rischi di sicurezza e i metodi di elusione nei sistemi di age assurance sia l'adozione di un metodo a livello di dispositivo.** Ciò significa che gli utenti verrebbero verificati una sola volta, attraverso il loro sistema operativo, e non su ogni sito web soggetto a restrizioni d'età. Questo ridurrebbe drasticamente i rischi per la privacy e creerebbe un processo molto semplice da applicare per le autorità di regolamentazione e da seguire per gli utenti: oltre il 95% dei dispositivi in tutto il mondo è alimentato da sistemi operativi di proprietà di tre società. AYLO afferma che, una volta che la verifica e la stima dell'età sarebbe effettuata la prima volta sul dispositivo dalle aziende che sviluppano i sistemi operativi e dai produttori di dispositivi, le quali già detengono i dati personali dei loro utenti, questi ultimi non sarebbero incoraggiati a condividere più volte le loro informazioni di identificazione personale sui vari siti. **Inoltre, i meccanismi di verifica implementati a livello di dispositivo possono offrire una maggiore sicurezza e ridurre il rischio di accesso non autorizzato o di violazione dei dati.** Localizzando la verifica dell'età all'interno del dispositivo, il trattamento viene isolato dalla miriade di vulnerabilità associate alle piattaforme online, compresi i tentativi di hacking e phishing. Infine, ritiene che con una soluzione implementata a livello di dispositivo non ci sarebbe nemmeno il rischio di una deviazione del traffico Internet, ovvero il rischio che gli utenti che non vogliono rivelare le proprie informazioni personali per accedere a un sito web si spostino dai siti conformi a quelli meno sicuri e non conformi.

WEBGROUP ritiene che **qualsiasi soluzione di *age verification* a livello di dispositivo sia più sicura dei sistemi realizzati da terzi**. Inoltre, *l'age verification* implementato direttamente dalle piattaforme rischia di dare ai genitori un falso senso di sicurezza, influenzando e compromettendo il monitoraggio parentale dei minori e delle loro attività online ed è inoltre probabile che si inducano gli utenti, compresi i minori, ad avventurarsi in parti non regolamentate del web, compreso il dark web, rischiando di esporsi a contenuti espliciti più estremi, compresi i contenuti criminali, e causando problemi molto più gravi di quelli che *l'age verification* imposta alle piattaforme avrebbe voluto affrontare. Inoltre, ritiene che solo quando un nuovo utente accede a un dispositivo personale dovrebbe essere richiesta la verifica dell'età. Una verifica aggiuntiva può essere richiesta anche quando i dati di navigazione in Internet indicano che il dispositivo è utilizzato da una persona diversa dal proprietario, o in caso di sospetto furto di identità o uso improprio.

Sostiene, altresì, che uno degli aspetti negativi dell'*age verification* imposta sulle piattaforme è che tale verifica non è limitata al terminale dell'utente, data la natura internazionale di Internet e del traffico di dati. ***Age verification* a livello di dispositivo** avviene nel dispositivo dell'utente, indipendentemente dall'origine geografica del sito web o del suo contenuto per adulti, il che riguarda anche l'uso delle VPN e **l'elusione è molto meno facile con i sistemi verifica limitati al terminale dell'utente**.

ALTROCONSUMO ritiene che il metodo auto-dichiarativo sia insufficiente a certificare l'età dell'utente per ovvie ragioni, confermate anche dalle pratiche elusive registrata nell'utilizzo di alcune piattaforme social da parte dei più giovani (ad es. Tik Tok). Inoltre, ritiene che, qualora il sistema di *age assurance* prevedesse un controllo dell'età basato sulla stima, sia necessario predisporre un meccanismo di double check da parte del sito/piattaforma tramite richiesta di prova documentale. Evidenzia che questo genere di meccanismo deve essere accompagnato dalle dovute tutele e responsabilità sul trattamento dei dati personali. Con riferimento alla frequenza di verifica dell'età, ritiene che, **qualora la funzione certificatrice fosse affidata ai soggetti fornitori di identità digitale, firma digitale e PEC mail, si potrebbe predisporre un sistema di richiesta ad ogni accesso**.

B. Valutazioni dell'Autorità

L'Autorità rileva che i fornitori di piattaforme e siti web che hanno risposto sul tema della sicurezza ritengono che la soluzione migliore per mitigare i rischi di sicurezza e i metodi di elusione nei sistemi di *age assurance* sia l'adozione di un metodo a livello di dispositivo. Inoltre, i meccanismi di verifica implementati a livello di dispositivo possono offrire una maggiore sicurezza e ridurre il rischio di accesso non autorizzato o di violazione dei dati.

Gli stessi osservano che ***age verification* a livello di dispositivo** avviene nel dispositivo dell'utente, indipendentemente dall'origine geografica del sito web/piattaforma o del suo contenuto per adulti, il che riguarda anche l'uso delle VPN e **l'elusione è molto meno facile con i sistemi verifica limitati al terminale dell'utente**.

L'associazione dei consumatori ritiene che, qualora la funzione certificatrice fosse affidata ai soggetti fornitori di identità digitale, firma digitale e PEC e-mail, si potrebbe predisporre un sistema di richiesta ad ogni accesso.

L'Autorità condivide le preoccupazioni dei rispondenti appartenenti alla categoria dei fornitori di piattaforme e siti web in relazione ai rischi per la sicurezza dei dati connessi all'ipotesi di condivisione di tali informazioni attraverso Internet. Come detto, le soluzioni di verifica a livello di terminale appaiono interessanti ma esulano dall'ambito del presente procedimento che riguarda i fornitori dei servizi di piattaforme di condivisione video e siti web.

In relazione al tema della sicurezza l'Autorità ritiene che il sistema adottato con il presente provvedimento, tra l'altro potenzialmente basato su un sistema di crittografia a chiave pubblica e privata o comunque a connessioni protette, fornisca ampie garanzie sebbene nessuno può escludere, nel settore dell'informatica, la possibilità di aggiramenti delle soluzioni individuate. Parimenti risultano connotati dai requisiti di sicurezza modelli basati sull'identità digitale come l'ID Wallet in quanto non prevedono il trasferimento di informazioni personali in rete.

IX. SUI CRITERI DI PRECISIONE ED EFFICACIA

A. Osservazioni di soggetti istituzionali, operatori e associazioni

META ritiene che le norme debbano tenere in debito conto gli sforzi e la buona fede dimostrata nello sviluppo e nell'implementazione di soluzioni sempre più efficaci di verifica dell'età, e che, in ultima analisi, **ciò debba avvenire a livello di sistema operativo, per rendere il processo il più semplice, coerente ed efficace possibile.** Inoltre, è dell'opinione che, nonostante l'efficienza dei sistemi di verifica dell'età, gli utenti online possano ancora rappresentare in modo errato la propria età e accedere a servizi e applicazioni che non sono stati progettati per loro. Per questo motivo, sostiene un approccio su più fronti e più livelli che combini strumenti diversi volti a facilitare esperienze adeguate all'età.

AYLO, pur apprezzando la volontà dell'Autorità di raccogliere dati metrici sull'accuratezza e l'efficacia dei meccanismi di verifica dell'età e di fissare soglie specifiche, ritiene che fornire raccomandazioni definitive su questi temi vada oltre il proprio ambito di competenza e confida nella capacità dell'Autorità di valutare e decidere relativamente a questi parametri, sottolineando la necessità di **misure che bilancino l'efficacia con i principi della privacy e della protezione dei dati degli utenti, tenendo conto anche dei rischi che abbiamo sottolineato riguardo a qualsiasi soluzione di verifica dell'età o di stima dell'età implementata a livello di sito web.**

ALTROCONSUMO ritiene che il sistema di verifica dovrebbe avere ad oggetto non tanto il dispositivo di accesso, quanto i contenuti a cui si accede e quelli che si inviano. Infatti, ritiene che, ad oggi sia troppo facile postare un video sui social che potrebbe violare ogni regola di privacy, decoro o persino sicurezza. Tuttavia, sostiene che utilizzare un gatekeeper universale che blocca solo l'accesso, secondo un principio "o tutto o niente" non risolve il problema, e che piuttosto ci

vorrebbero dei sistemi di controllo via via più sofisticati (e stringenti) a seconda dell'attività che s'intende fare online. Sottolinea anche che controllare un cellulare è forse più facile che controllare un PC (anche perché ad ogni dispositivo mobile corrisponde un'utenza registrata), laddove nel PC si può risalire solo all'indirizzo IP che può essere pure facilmente mascherato o falsato; inoltre, c'è una modalità di accesso diversa: su PC, di solito, il browser è la porta di accesso a tutti i servizi internet, mentre su dispositivo mobile spesso si usano le app e questo, a sua volta, richiede due approcci diversi al problema di come controllare gli accessi, ognuno con proprie specificità.

WEBGROUP sostiene che, in generale, nel caso di piattaforme che offrono esclusivamente contenuti per adulti, sarebbe **molto più efficace realizzare l'AV a livello di dispositivo tramite software di filtraggio**. Inoltre, dal punto di vista dell'efficacia, ritiene che solo le piattaforme stabilite in Italia siano soggette agli obblighi stabiliti dalla legge del Paese d'origine, lasciando la stragrande maggioranza dei siti pornografici più trafficati non soggetti all'obbligo di age verification. Tuttavia, i software di filtraggio sui dispositivi possono impedire ai minori di vedere tutti i contenuti per adulti, non solo quelli pubblicati in Italia e, pertanto, le campagne educative sull'uso delle opzioni di filtraggio disponibili potrebbero essere più efficaci e molto meno invasive delle libertà e della privacy rispetto ai requisiti *age verification* imposti ai provider.

B. Valutazioni dell'Autorità

L'Autorità prende atto del fatto che non sono state fornite specifiche valutazioni quantitative sui requisiti di precisione ed efficacia dei sistemi di verifica dell'età descritti nel documento di consultazione pubblica, per cui rinvia alla documentazione disponibile in letteratura e richiamata nel provvedimento.

X. SUI CRITERI DI ACCESSIBILITÀ, FACILITÀ D'USO E NON DISCRIMINAZIONE

A. Osservazioni di soggetti istituzionali, operatori e associazioni

[OMISSIS - Un fornitore di piattaforma video sharing] ritiene che sia opportuno tenere presente che, nel contesto degli strumenti di age assurance, maggiore la specificità e la granularità delle informazioni richieste dal fornitore, maggiore è l'impatto sull'utente in termini di raccolta di dati personali e *user experience*. L'applicazione di metodi data-intensive non solo accresce il rischio per la sicurezza dei dati, ma può anche scoraggiare gli utenti da un accesso legittimo ai servizi. Per esempio, il ricorso a metodi che si basano sull'accertamento dell'età attraverso la fornitura di un documento di identità può portare a un peggioramento della *user experience*, nonché alla condivisione di informazioni personali non necessarie, in particolare se richiesto nell'ambito di un servizio non rischioso come, ad esempio, un sito per imparare una nuova lingua online. Inoltre, nell'ambito del bilanciamento dei vari diritti, è importante considerare la pluralità di esigenze e caratteristiche degli utenti. Poiché non tutti dispongono di una carta di credito o di un documento d'identità, verificare l'età utilizzando esclusivamente identificatori rigidi rischierebbe di escludere categorie di persone

marginalizzate o provenienti da contesti socio-culturali svantaggiati dall'accesso ai servizi e all'informazione, contribuendo così ad ampliare il divario culturale ed economico. Inoltre, **[OMISSIS - Un fornitore di piattaforma video sharing]** ritiene che i meccanismi di *age assurance* debbano prevedere l'impegno massimo da parte dell'industria per garantire che le soluzioni fornite siano semplici ed efficaci, anche nel contesto dell'esercizio della supervisione da parte di genitori e tutori. Solo in questo modo sarà possibile promuovere la fiducia degli utenti nel processo, garantendo al contempo la protezione efficace dei minori dai contenuti per adulti.

Il CNU evidenzia l'importanza del criterio relativo alla facilità d'uso e all'accessibilità del sistema di *age assurance*, che deve essere rispettato dai soggetti regolamentati al fine di garantire che il sistema di verifica dell'età sia facilmente utilizzabile da tutti gli utenti, indipendentemente dalle loro caratteristiche e soprattutto che risulti accessibile da parte di utenti con disabilità, garantendo, ad esempio, che vi sia la possibilità di utilizzare i lettori di schermo per completare con successo il processo di verifica.

ALTROCONSUMO evidenzia che come per l'identità digitale, che è obbligatoriamente in uso ai cittadini, uno strumento analogo non dovrebbe sollevare particolari criticità in termini di accessibilità e che in particolare i minori raggiungono un livello di informatizzazione medio/alto. Viceversa, per le fasce meno informatizzate, come per l'identità digitale, esistono canali più analogici come le attivazioni presso sportelli/negozi fisici da utilizzare anche per certificare l'età. Per quanto riguarda il criterio di inclusività e non discriminazione, ritiene che nel caso in cui il sistema di verifica conducesse a risultati imprecisi o erronei, si potrebbe pensare a una procedura di revisione su istanza dell'interessato o del sito/piattaforma per una verifica più accurata sulla scorta di dati certi. Ad esempio, se il sistema di stima dovesse qualificare come minorenne un soggetto maggiore d'età questi potrebbe ricorrere alla procedura di revisione presentando un documento di identità. Viceversa, se il sito/piattaforma dovesse ritenere falsata la *age assurance* su un minore potrebbe richiedere la prova documentale dell'età all'utente

B. Valutazioni dell'Autorità

L'Autorità ritiene condivisibile l'osservazione secondo cui maggiore è la specificità e la granularità delle informazioni richieste dal fornitore, maggiore è l'impatto sull'utente in termini di raccolta di dati personali e *user experience*. L'applicazione di metodi data-intensive non solo accresce il rischio per la sicurezza dei dati, ma può anche scoraggiare gli utenti da un accesso legittimo ai servizi.

L'Autorità pertanto favorisce l'adozione di sistemi sicuri ma, allo stesso tempo, di facile utilizzo da parte dei cittadini.

XI. SUL CRITERIO DI TRASPARENZA

A. Osservazioni di soggetti istituzionali, operatori e associazioni

AYLO sostiene pienamente lo spirito dell'Autorità volto a una maggiore trasparenza, indipendentemente dal sistema di verifica o di stima dell'età utilizzato e crede nella necessità di

fornire agli utenti, sia adulti che minori, spiegazioni chiare ed esaustive su qualsiasi tipo di trattamento in atto sulle nostre piattaforme.

WEBGROUP ribadisce che l'*age verification* dovrebbe essere limitata ed eseguita nel dispositivo personale e, in via sussidiaria, l'utente dovrebbe essere informato nella misura richiesta dalle leggi sulla protezione dei dati (GDPR), il che probabilmente comporterebbe la richiesta del consenso dell'utente affinché la terza parte venga a conoscenza dell'identità personale e dell'età, esclusivamente per scopi di verifica dell'età e con l'esclusione di qualsiasi altro dato personale, compresa la conoscenza di qualsiasi attività Internet dell'utente. Nella misura richiesta dalla legge, l'utente dovrebbe anche essere informato che la terza parte indipendente è certificata da un'autorità di certificazione, il cui ruolo sarebbe quello di organizzare il funzionamento della verifica dell'età da parte della terza parte fornendo le specifiche crittografiche per il servizio e di certificare le terze parti (con la possibilità di revocare le terze parti se necessario).

ALTROCONSUMO ritiene che un veicolo di trasparenza sia l'utilizzo di info-grafiche e tutorial da parte dei soggetti regolamentati, dell'Autorità e dei soggetti certificatori.

B. Valutazioni dell'Autorità

L'Autorità ritiene condivisibile le osservazioni relative alla necessità della massima trasparenza nei confronti degli utenti.

XII. SUL TEMA DELLA FORMAZIONE E INFORMAZIONE

A. Osservazioni di soggetti istituzionali, operatori e associazioni

AYLO sostiene che la stampa, i blog e i siti web rappresentano strumenti utili per promuovere l'importanza della verifica e della stima dell'età e per sensibilizzare sui pericoli e sui rischi associati a Internet. AYLO dichiara di trattare i meccanismi di *age assurance* da molti anni e di aver condotto attività di sensibilizzazione con la stampa e anche tramite i nostri siti rispetto ai pericoli connessi agli strumenti di verifica e della stima dell'età implementati a livello di sito web. Inoltre, dichiara che la pagina di accesso ai loro siti include anche un disclaimer e una richiesta di autodichiarazione dell'età volta a dissuadere gli utenti minorenni dal visitare i siti. Inoltre, ritiene che le misure tecniche da sole non siano quasi mai sufficienti a risolvere di per sé le problematiche sociali e che una protezione adeguata ed efficace dei minori non potrà mai funzionare in modo significativo senza la partecipazione dei genitori. Affinché ciò avvenga, è dell'opinione che i genitori devono innanzitutto essere in grado di partecipare in modo significativo e che dovrebbero essere formati nel modo più completo possibile sul comportamento tipico dei bambini e degli adolescenti su Internet. In particolare, dovrebbero essere informati su come i loro figli utilizzano Internet e su quali sono i relativi pericoli e le relative opportunità. Infine, accoglie con favore qualsiasi impegno dell'Autorità volto a migliorare la formazione dei genitori in questo senso.

Il **CNU** ritiene che solo con una serie di interventi, non solo normativi e regolamentari, ma anche nell'ambito della comunicazione e educazione digitale, si potrà portare un contributo concreto

affinché vi possa essere un'efficace verifica dell'età e quindi una sempre più efficace tutela dei minori dai rischi del web.

Il **GARANTE PER L'INFANZIA** ritiene che, al di là delle soluzioni tecniche, resta fondamentale una vasta opera di educazione e sensibilizzazione al digitale rispetto al tema della protezione della salute fisica e psichica dei minori in rete. Tale iniziativa è da portare avanti preventivamente e parallelamente all'introduzione di nuovi strumenti sul piano tecnico che utilizzi tutti i canali disponibili di informazione e formazione, attivando tutte le opportune sinergie istituzionali e soprattutto coinvolgendo attivamente i minori stessi nel processo decisionale riguardante le politiche di protezione online, ascoltando le loro esperienze, opinioni e preoccupazioni per contribuire a sviluppare misure di *age assurance* più efficaci e rispettose dei loro diritti e desideri.

ALTROCONSUMO ritiene che le associazioni rappresentative dei consumatori siano un canale valido di divulgazione.

B. Valutazioni dell'Autorità

L'Autorità ritiene certamente condivisibili le osservazioni dei rispondenti relative alla necessità di una adeguata formazione e informazione dei minori e degli stessi genitori.