Key4Biz
People&Tech News

ANALISI

Perché la Corte Costituzionale francese ha bocciato (parzialmente) la legge che vieta i social agli under 15

di **Avv. Alessandro del Ninno - Partner di FIVERS Studio Legale e Tributario**

18 Agosto 2026, ore 15:30

INTERNET

> *Analisi della decisione del Conseil constitutionnel tra tutela dei minori, libertà di comunicazione, privacy, age verification e Digital Services Act. Ne emerge una lezione che è insieme giuridica, tecnologica e organizzativa anche per il Parlamento italiano a cui diamo 7 consigli per la verifica dell'età.*

La protezione dei minori nell'ambiente digitale è ormai uno dei terreni nei quali emerge con maggiore evidenza la difficoltà di conciliare obiettivi regolatori tutti, in sé, meritevoli di tutela. Proteggere bambini e adolescenti dai rischi connessi all'uso dei social network non significa, infatti, soltanto stabilire quanto debba essere elevato il livello di protezione. Significa anche decidere **come** conseguirlo e, soprattutto, quali sacrifici possano essere imposti, a tal fine, alla libertà di espressione e di informazione, alla vita privata e alla protezione dei dati personali degli stessi minori e della generalità degli utenti.

È precisamente su questo secondo piano che assume particolare interesse la decisione n. 2026-911 DC del 14 agosto 2026 del Conseil constitutionnel francese. **La pronuncia non mette in discussione l'esigenza di una tutela particolarmente intensa dei minori**

legittima, a uno strumento normativo eccessivamente generale: un divieto di accesso ai social network per tutti i minori di quindici anni, sostanzialmente uniforme rispetto a servizi, rischi e situazioni profondamente diversi.

La pronuncia appare importante ben oltre i confini francesi: essa interviene, infatti, nello stesso spazio regolatorio occupato dal Digital Services Act, dal GDPR, dalle Linee guida della Commissione europea sulla protezione dei minori ai sensi dell'art. 28 DSA, dagli orientamenti dell'EDPB sull'age verification e, sempre più, dalle soluzioni europee di verifica dell'età. Ne emerge – allora – una lezione che è insieme giuridica, tecnologica e organizzativa: **la protezione dei minori non legittima automaticamente il massimo livello possibile di identificazione, restrizione o controllo degli utenti; richiede, piuttosto, una progettazione proporzionata al rischio e rispettosa, per costruzione, degli altri diritti fondamentali coinvolti**.

Dalla necessità di proteggere i minori alla legge francese: la ricostruzione dei passaggi della vicenda

I rischi che possono derivare dall'utilizzo dei social network da parte dei minori – dall'esposizione a contenuti dannosi alle dinamiche di dipendenza, dal cyberbullismo alle interazioni indesiderate, sino agli effetti di determinati sistemi di raccomandazione – costituiscono ormai un oggetto specifico della regolazione europea.

L'art. 28 del DSA impone ai fornitori di piattaforme online accessibili ai minori di adottare misure «*adeguate e proporzionate*» per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori. Lo stesso articolo vieta, quando il *provider* sappia con ragionevole certezza che il destinatario è minorenne, la pubblicità basata sulla profilazione mediante dati personali del minore. Il legislatore europeo ha però contestualmente precisato che l'adempimento di tali obblighi non deve trasformarsi in un incentivo alla raccolta di ulteriori dati personali al solo fine di stabilire se ciascun utente sia minorenne.

È in questo contesto che, il 18 novembre 2025, veniva depositata all'Assemblée nationale la proposta di legge francese volta a proteggere i minori dai rischi derivanti dall'utilizzo dei social network. Il testo originario muoveva anche dalle risultanze della commissione d'inchiesta dell'Assemblée nationale sugli effetti psicologici di TikTok sui minori e prevedeva, tra l'altro, il divieto di iscrizione ai social network per gli under

Già in questa fase, tuttavia, il Conseil d'État aveva individuato due criticità che avrebbero anticipato, in larga misura, quelle successivamente emerse davanti al Conseil constitutionnel.

La prima criticità faceva riferimento al quadro regolatorio UE. Il DSA è costruito come disciplina armonizzata dei servizi intermediari e, secondo il Conseil d'État, gli Stati membri non possono utilizzare la legislazione nazionale per introdurre ulteriori obblighi direttamente gravanti sulle piattaforme nelle materie armonizzate dal Regolamento 2022/2065 (Legge sui Servizi Digitali). Rimane possibile perseguire finalità nazionali di politica sociale, compresa l'introduzione di limiti di età, ma occorre costruire la disciplina in modo compatibile con l'assetto delle competenze europee. Per questa ragione il Conseil d'État suggerìva di trasformare l'obbligo originariamente rivolto alle piattaforme in una regola sostanziale secondo cui al minore di quindici anni fosse vietato accedere al servizio.

La seconda criticità evidenziata dal Conseil d'État riguardava la proporzionalità. Il Conseil d'État ha osservato che la nozione di social network comprende servizi estremamente differenti quanto a contenuti, modalità di funzionamento e rischi per i minori. Un divieto generale avrebbe pertanto colpito nello stesso modo piattaforme delle quali erano stati documentati specifici rischi ma anche servizi collaborativi, informativi, associativi o basati su progetti *open source* rispetto ai quali rischi analoghi non risultavano dimostrati. Il Conseil d'État sottolineava, inoltre, l'assenza di una valutazione riferita all'età e al grado di maturità del minore e l'esclusione sostanziale del ruolo dei titolari della responsabilità genitoriale.

L'alternativa proposta dal Conseil d'État è particolarmente significativa: un modello graduato nel quale determinati servizi particolarmente pericolosi avrebbero potuto essere vietati in assoluto agli under 15, sulla base delle loro caratteristiche e, tra l'altro, dei sistemi di raccomandazione utilizzati; per gli altri servizi, invece, l'accesso avrebbe potuto essere subordinato a un'autorizzazione parentale espressa, revocabile e suscettibile di essere modulata anche rispetto alle funzionalità o alla durata dell'utilizzo.

Il testo definitivamente approvato il 21 luglio 2026 dall'Assemblée nationale e dal Sénat non ha tuttavia seguito questa impostazione: l'articolo 1 della "*Legge volta a proteggere i minori dai rischi ai quali li espone l'utilizzo dei social network*" introduceva nella Legge francese sulla fiducia nell'economia digitale ("*Loi n° 2004-*

piattaforma online» era vietato ai minori di quindici anni. Erano escluse soltanto alcune categorie – enciclopedie online, repertori educativi o scientifici e piattaforme dedicate allo sviluppo e alla condivisione di software libero o di progetti digitali educativi open source. L'entrata in vigore era prevista per il 1° settembre 2026 e, per gli account già esistenti, dopo ulteriori quattro mesi.

Il ricorso al Conseil constitutionnel e la Decisione del 14 agosto 2026

Fin qui la ricostruzione del percorso normativo della legge, che è stata sottoposta al vaglio del Conseil constitutionnel il 23 e 24 luglio 2026 da parte di sessanta parlamentari, due giorni dopo la sua approvazione definbitiva (in Francia, difatti, esiste un meccanismo attraverso il quale una minoranza parlamentare può deferire preventivamente una legge statale alla Corte costituzionale, mediante un controllo preventivo della legge previsto dall'art. 61 della Costituzione francese). La contestazione dei parlamentari ricorrenti ha investito, in particolare, la libertà di espressione e comunicazione garantita dall'art. 11 della *Déclaration des droits de l'homme et du citoyen*, il ruolo della responsabilità genitoriale e l'interesse superiore del minore, il diritto alla vita privata e, sotto ulteriori profili, l'esigenza che il legislatore definisca con sufficiente precisione le garanzie fondamentali relative all'esercizio delle libertà pubbliche.

La decisione del Conseil constitutionnel del 14 agosto è importante, innanzitutto, per ciò che non afferma. Il Conseil constitutionnel non stabilisce che sia costituzionalmente illegittimo limitare l'accesso dei minori ai social network. Riconosce, al contrario, che il legislatore perseguiva tanto l'esigenza costituzionale di protezione dell'interesse superiore del minore quanto quella di prevenire le lesioni dell'ordine pubblico e che tali finalità possono giustificare restrizioni alla libertà di accesso di alcuni minori ai servizi social. In altri termini: **il Conseil constitutionnel non ha dichiarato incostituzionale l'intera legge, ma ha pronunciato una «non conformité partielle», censurando in particolare l'articolo 1 che introduceva il divieto di accesso ai social network per i minori di quindici anni.**

Il problema – appunto – è la misura della restrizione.

L'articolo 1 della legge è stato dichiarato contrario alla Costituzione perché la sua portata è eccessivamente generale. Non distingue i servizi sulla base delle funzionalità e dei contenuti, dei pericoli effettivamente generati o delle misure di protezione già

individualizzata che tenga conto dell'età, del grado di maturità e della situazione concreta del minore. Il risultato è un sacrificio della libertà di espressione e di comunicazione che non supera il necessario controllo di proporzionalità.

A ciò si aggiunge un secondo profilo, forse ancora più interessante per chi deve progettare concretamente i servizi digitali: **la verifica dell'età (cosiddetta "*age assurance o age verification*")**.

Un divieto basato sull'età non riguarda infatti soltanto i minori. Per distinguere chi può accedere da chi non può farlo occorre stabilire l'età di tutti gli utenti interessati, compresi gli adulti. La misura, pertanto, può produrre una interferenza generalizzata nella vita privata anche di persone che non appartengono alla categoria che il legislatore intende proteggere. Il Conseil constitutionnel rileva che la legge non aveva definito condizioni e limiti sufficienti relativi alla prova dell'età e non aveva quindi predisposto garanzie legali adeguate per la tutela della vita privata. Anche sotto questo profilo l'art. 1 non ha superato il controllo costituzionale.

Il rapporto tra la Decisione del Conseil constitutionnel, il DSA e le Linee Guida della Commissione UE sull'articolo 28 del DSA

La parte forse più significativa della decisione francese è la sua convergenza metodologica con il diritto europeo.

Le Linee guida della Commissione sull'art. 28 DSA, pubblicate nella Gazzetta ufficiale dell'Unione nel 2025, assumono espressamente che piattaforme diverse possono comportare rischi diversi per i minori e che, conseguentemente, l'appropriatezza e la proporzionalità delle misure devono essere valutate caso per caso. In materia di a*ge assurance* la Commissione afferma che le restrizioni all'accesso basate sull'età devono essere valutate rispetto alla possibilità di ottenere lo stesso livello di protezione mediante misure meno invasive e che ***age assurance* e limitazioni dell'accesso costituiscono strumenti complementari, non sostitutivi delle altre misure di sicurezza e di progettazione del servizio.**

La protezione effettiva dei minori non richiede necessariamente misure uniformi o generalizzate, ma può essere perseguita attraverso una combinazione di strumenti calibrati sui rischi concretamente presenti nel servizio. A seconda dei casi, possono rilevare impostazioni di privacy by default, interventi sui sistemi di raccomandazione,

effettivamente necessario e proporzionato, meccanismi di *age assurance*.

Le Linee guida europee seguono precisamente questa logica di intervento mirato: se il rischio riguarda soltanto determinate sezioni, contenuti o funzionalità della piattaforma, la misura di protezione dovrebbe concentrarsi su tali elementi, evitando di tradursi automaticamente in un divieto di accesso all'intero servizio. In altri termini, la protezione del minore deve essere costruita in funzione della natura e dell'intensità del rischio, privilegiando, ove possibile, soluzioni selettive rispetto a restrizioni generalizzate.

Questa logica spiega bene anche la decisione francese: il difetto non risiede nell'avere protetto troppo il minore in senso quantitativo, ma nell'avere utilizzato un criterio normativo troppo poco differenziato per bilanciare correttamente tutti i diritti coinvolti.

Gli insegnamenti della decisione francese (anche per il legislatore italiano): proporzionalità, differenziazione del rischio e tutela della privacy

La vicenda francese offre, sotto questo profilo, un insegnamento che va oltre la specifica soluzione censurata dal Conseil constitutionnel. La tutela dei minori costituisce una finalità pienamente legittima e, anzi, particolarmente rilevante nell'ordinamento costituzionale ed europeo; ciò non significa, tuttavia, che qualsiasi misura adottata in suo nome possa considerarsi automaticamente proporzionata. La decisione mostra come il vero punto di equilibrio debba essere ricercato nella capacità della disciplina di differenziare gli interventi in funzione dei rischi effettivi, delle caratteristiche del servizio e della posizione concreta degli utenti coinvolti.

Ne deriva una conseguenza importante anche sul piano applicativo: quanto più una misura incide in modo generalizzato sull'accesso ai servizi digitali o comporta trattamenti di dati riferiti all'intera platea degli utenti, tanto maggiore deve essere la capacità del legislatore e, a valle, delle imprese, di dimostrarne necessità, adeguatezza e proporzionalità. La protezione dei minori non può quindi essere ridotta a una soglia anagrafica o a un meccanismo uniforme di verifica, ma deve tradursi in un sistema di misure selettive, coerenti con la natura del rischio e costruite secondo i principi di minimizzazione e protezione dei dati fin dalla progettazione.

tecnica e organizzativa dovrebbe essere progettata per conseguire tale risultato senza raccogliere o rendere disponibili alla piattaforma informazioni ulteriori rispetto a quelle strettamente necessarie.

E allora, sul piano tecnico, il principale insegnamento della vicenda riguarda probabilmente la necessità di separare due operazioni che vengono ancora troppo spesso confuse: **accertare un requisito di età e identificare l'utente**.

Il GDPR impone – come è noto – i principi di minimizzazione, limitazione delle finalità e protezione dei dati fin dalla progettazione e per impostazione predefinita. L'EDPB, nella Dichiarazione 1/2025 sull'*age assurance*, ha ulteriormente chiarito che il metodo utilizzato deve essere il meno intrusivo tra quelli efficaci e che la determinazione dell'età deve essere progettata secondo un approccio basato sul rischio.

La direzione tecnologica assunta dall'Unione europea è coerente con questo principio. Il *blueprint* europeo per l'*age verification* mira a consentire all'utente di dimostrare di trovarsi sopra una determinata soglia – ad esempio 15 o 18 anni – senza comunicare alla piattaforma la propria identità, la data di nascita o altri attributi non necessari. La soluzione europea prevede una prova anonima dell'età e tecnologie orientate alla non correlabilità delle transazioni; Italia, Francia, Danimarca, Grecia e Spagna hanno partecipato alla fase di adozione e personalizzazione della soluzione. Nell'aprile 2026 la Commissione ha inoltre raccomandato agli Stati membri di rendere disponibili soluzioni robuste e rispettose della privacy entro la fine del 2026.

Il paradigma di riferimento dovrebbe quindi consistere, ove tecnicamente e giuridicamente possibile, nella verifica del solo requisito anagrafico necessario per l'accesso al servizio, evitando l'identificazione dell'utente e la raccolta di ulteriori dati personali non strettamente necessari.

Per un'impresa – anche italiana, ovviamente – questa distinzione modifica radicalmente l'architettura del trattamento. Un processo che acquisisce copia del documento, nome, cognome, data di nascita e fotografia presenta un livello di interferenza e un profilo di rischio molto diversi da un sistema nel quale un soggetto terzo restituisce alla piattaforma soltanto un'attestazione anonima del superamento della soglia richiesta.

L'Italia – tra l'altro – possiede già precedenti operativo rilevante. Un ptimo precedente è rappresentato dalla **disciplina AGCOM sull'accesso a contenuti pornografici,** pienamente applicabile secondo le tempistiche stabilite dalla delibera n. 96/25/CONS, che ha introdotto il criterio del cosiddetto «doppio anonimato»: la piattaforma riceve dal soggetto verificatore soltanto la prova della maggiore età e il verificatore non deve conoscere il servizio al quale l'utente intende accedere. La regolazione italiana richiede inoltre proporzionalità, minimizzazione, sicurezza, precisione, inclusività e non discriminazione. Pur trattandosi di un diverso settore e di una diversa soglia di accesso, il modello AGCOM dimostra concretamente che tutela del minore e identificazione generalizzata dell'utenza non devono necessariamente coincidere.

Un secondo sviluppo, molto recente e interessante, è relativo al provvedimento del **Garante per la protezione dei dati personali adottato avverso Character.AI lo scorso 3 luglio 2026.** In tale provvedimento il Garante ha rilevato specifiche criticità nei meccanismi di verifica dell'età di un servizio di IA generativa accessibile anche ai minori. L'Autorità ha prescritto alla società di garantire il corretto funzionamento dei sistemi di age verification, rendere effettivi i meccanismi che impediscono nuovi tentativi di registrazione ai minori già bloccati – il cosiddetto *cooling-off period* – e configurare per impostazione predefinita come privati i profili dei minorenni. Non si tratta di una disciplina generale dell'age assurance, ma è un precedente applicativo importante perché mostra che **l'effettività della verifica dell'età sta diventando anche un parametro concreto di enforcement del GDPR nei servizi digitali destinati o accessibili ai minori**.

Contemporaneamente, nel Parlamento italiano si stanno moltiplicando proposte che vorrebbero estendere la verifica dell'età ai social network, fino a collegarla a un vero e proprio divieto di accesso per gli under 15: è proprio quest'ultimo sviluppo (approccio rilevato nelle tre diverse proposte di legge presentate a gennaio, febbraio e luglio 2026) che rende la decisione del Conseil constitutionnel francese particolarmente tempestiva per il dibattito italiano.

Interpretare correttamente la soglia dei 14 anni prevista dall'articolo 8 del GDPR e dall'articolo 2-*quinquies* del Codice della privacy italiano

Un altro profilo operativo merita – a parere di chi scrive – particolare attenzione.

servizi della società dell'informazione. Da ciò, tuttavia, **non può ricavarsi che il diritto europeo o italiano riconosca automaticamente a ogni quattordicenne un generale diritto di accedere a qualsiasi social network.**

L'art. 8 GDPR ha un oggetto molto più circoscritto: disciplina la validità del consenso quale base giuridica del trattamento quando un servizio della società dell'informazione è offerto direttamente al minore. Non regola tutti i trattamenti di dati dei minori, non disciplina in via generale la loro capacità di agire e non costituisce, da solo, una normativa sull'età minima di accesso a un servizio digitale. Lo stesso Garante italiano evidenzia espressamente questa distinzione. In tale scenario, l'approccio corretto per applicare tale disciplina normativa passa attraverso una serie di quesiti che un'impresa dovrebbe porsi: se il minore possa accedere giuridicamente al servizio; se e a quali condizioni possa validamente prestare il consenso *data protection;* quali misure di protezione siano comunque necessarie perché il servizio sia accessibile ai minori. Confondere questi tre piani può produrre errori sia nel design del prodotto sia nell'individuazione della base giuridica dei trattamenti.

Dalla decisione del Conseil constitutionnel francese al design dei servizi: come le imprese italiane dovrebbero progettare meccanismi di age assurance e di tutela dei minori

La pronuncia del Conseil constitutionnel francese suggerisce alle imprese europee un fondamentale cambiamento nell'approccio alla specifica tematica dell'*age assurance*. A parere di chi scrive, possono essere suggeriti i seguenti passaggi successivi di una vera progettazione rispettosa del *legal design*.

Il primo cambiamento è metodologico. Occorre partire da una **mappatura dei rischi per i minori propria del servizio**. Quali contenuti possono incontrare? Quale ruolo svolgono i i sistemi di raccomandazione? Il servizio permette messaggistica privata, contatti con sconosciuti, live streaming, geolocalizzazione, acquisti, monetizzazione o pubblicità comportamentale? Sono presenti meccanismi che possono favorire un uso intensivo o compulsivo? Quali rischi derivano dagli altri utenti e quali, invece, dal design stesso della piattaforma? È questa analisi che dovrebbe precedere la scelta dell'eventuale tecnica di *age assurance*, in coerenza con il modello europeo che richiede appunto una valutazione contestuale della proporzionalità delle misure.

piattaforma può aver bisogno di distinguere messaggistica, pubblicazione pubblica, raccomandazione algoritmica, live streaming, advertising, acquisti o accesso a categorie specifiche di contenuto. La medesima logica può condurre a impostazioni differenti in relazione a fasce di età diverse: è precisamente ciò che mancava al divieto francese censurato.

Il terzo cambiamento riguarda la corretta applicazione pratica dell'articolo 25 del GDPR e in particolare del principio di **privacy by design**. L'impresa dovrebbe domandarsi quale sia l'informazione minima necessaria: età esatta, fascia di età o semplice superamento di una soglia. Dovrebbero essere valutate soluzioni che impediscano al *provider* di *age assurance* di conoscere il servizio successivamente utilizzato e alla piattaforma di ricevere dati identificativi non necessari. Tempi di conservazione, possibilità di correlare verifiche successive, log, accessi amministrativi, sicurezza delle credenziali e riutilizzo dei dati per finalità ulteriori devono essere progettati coerentemente con gli artt. 5 e 25 GDPR. Nei casi in cui l'*age assurance*possa comportare un rischio elevato per i diritti e le libertà degli utenti, dovrà inoltre essere verificata l'applicabilità dell'art. 35 GDPR e quindi la necessità di una DPIA: anche l'EDPB sottolinea espressamente che la necessità delle Valutazioni di Impatto appare frequente in molti sistemi di *age assurance.*

Il quarto cambiamento che le imprese dovrebbero considerare riguarda la **qualità tecnica e l'affidabilità dei sistemi di verifica dell'età**. Questi strumenti, infatti, non sono necessariamente infallibili e possono generare errori (falsi positivi e negativi) sia nel riconoscere come minorenne un utente che ha invece superato la soglia richiesta, sia nel consentire l'accesso a un minore che avrebbe dovuto essere escluso. Tali errori non costituiscono soltanto un problema di funzionamento del sistema, perché possono incidere direttamente sui diritti degli utenti e sull'effettività delle misure di protezione.

Per questa ragione, elementi come accuratezza, accessibilità, rischio di discriminazioni algoritmiche (dette *bias*) essere considerati parte integrante della conformità giuridica del sistema. Le Linee guida della Commissione richiedono infatti che la scelta delle misure di *age assurance* sia fondata su una valutazione concreta della loro adeguatezza ed efficacia rispetto al rischio da prevenire, e non sulla semplice disponibilità tecnica di uno specifico strumento.

Il quinto profilo riguarda il rapporto con i **fornitori tecnologici coinvolti nei sistemi di age assurance**. L'affidamento a un soggetto terzo delle attività di verifica dell'età non

trattamento dei dati.

È quindi necessario definire con precisione i ruoli privacy dei soggetti coinvolti, regolare contrattualmente le finalità del trattamento e gli eventuali limiti al riutilizzo dei dati, verificare l'adeguatezza delle misure di sicurezza adottate e comprendere in quale fase e presso quale soggetto avvenga concretamente la verifica. Allo stesso modo, occorre chiarire quali informazioni vengano effettivamente restituite alla piattaforma, come siano gestiti eventuali incidenti di sicurezza e secondo quali modalità e tempi i dati vengano cancellati. Particolare attenzione deve infine essere riservata al rischio che il sistema di age assurance, soprattutto se utilizzato trasversalmente rispetto a più servizi, possa trasformarsi in uno strumento di correlazione o tracciamento degli utenti oltre quanto strettamente necessario per la verifica dell'età.

Infine, un **sesto cambiamento riguarda la cultura organizzativa e il modello di governance interno delle imprese**. I temi dell'age assurance e della protezione dei minori non possono essere considerati di esclusiva competenza delle funzioni privacy o legali, perché incidono direttamente sulle caratteristiche del servizio, sulle modalità di accesso, sulla sicurezza, sull'esperienza utente e sul funzionamento delle piattaforme. Richiedono quindi un coordinamento stabile tra le funzioni legale, DPO/privacy, progettazione dei servizi e dei prodotti e me marketing, solo per citarne alcune.

Le decisioni relative alle soglie di accesso, alle tecniche di verifica dell'età e alle funzionalità disponibili per le diverse fasce di utenti dovrebbero essere assunte sulla base di una valutazione documentata dei rischi e dei diritti coinvolti a cui **partecipano tutte le funzioni aziendali coinvolte, tecnicamente, legalmente, e commercialmente.** La vicenda francese, da questo punto di vista, suggerisce un passaggio da una logica di adempimento *ex post* a un modello di *governance* del prodotto/servizio digitale nel quale la tutela dei minori e la proporzionalità delle misure siano integrate fin dalle fasi di progettazione e sviluppo del servizio.

Un'ultima considerazione riguarda le **imprese multinazionali**, che possono trovarsi a gestire un ulteriore livello di complessità. La protezione dei minori è infatti un ambito nel quale i diversi Stati membri stanno adottando o valutando soluzioni non sempre coincidenti, mentre le piattaforme digitali operano normalmente su scala transnazionale. Ne deriva il rischio concreto di una frammentazione regolatoria, con soglie di età, tecniche di *age assurance* e condizioni di accesso ai servizi differenti da Paese a Paese.

regole applicabili ai servizi intermediari e, secondo il Conseil d'Etat, gli Stati membri possono certamente perseguire proprie finalità di politica sociale, anche introducendo in determinate condizioni limiti di età. **Non possono però utilizzare tali finalità per imporre alle piattaforme un nuovo insieme di obblighi nazionali nelle materie già disciplinate in modo armonizzato dal DSA.**

Per un'impresa italiana che offre i propri servizi in più Stati membri diventa quindi opportuno distinguere tra un **quadro europeo comune**, fondato su DSA, GDPR, sicurezza, governance e soluzioni di age assurance rispettose della privacy, e un **livello nazionale**, nel quale gestire le eventuali soglie di età o le ulteriori limitazioni previste dalle singole legislazioni. Anche l'architettura europea dell'age verification sembra muoversi in questa direzione, perché consente di dimostrare il superamento di soglie differenti senza comunicare alla piattaforma né l'identità dell'utente né, necessariamente, la sua età esatta.

Conclusioni: dalla "digital majority" alla responsabilità di progettare ambienti digitali adeguati all'età

La decisione francese offre infine una chiave interpretativa più generale.

Il dibattito pubblico tende spesso a concentrare l'intera questione della protezione dei minori sulla ricerca di una «età giusta»: tredici, quattordici, quindici o sedici anni. Ma il diritto europeo sta progressivamente indicando che la sola soglia cronologica non è sufficiente a risolvere un problema che dipende anche dal tipo di servizio, dalle funzionalità disponibili, dai sistemi di raccomandazione, dalla natura dei contenuti, dalla possibilità di interazione con altri utenti, dal design persuasivo e dalla capacità del minore di utilizzare consapevolmente il servizio.

La soglia di età può costituire una misura necessaria in determinate situazioni. Ciò è particolarmente evidente per servizi o contenuti che, per loro natura, non devono essere accessibili ai minori. Ma la logica che emerge dal DSA, dalle Linee guida della Commissione, dall'EDPB e ora dalla vicenda costituzionale francese è quella di una **protezione proporzionata al rischio e incorporata nell'architettura del servizio**.

La *compliance* futura in materia di minori non potrà probabilmente essere risolta con una clausola nelle condizioni generali o con un semplice *age gate*. Sarà sempre più necessario poter dimostrare perché il servizio è accessibile o non accessibile a una

vengono effettivamente trattati, come sono state configurate le funzionalità per i minori e come vengono periodicamente rivalutati rischi ed efficacia delle misure.

È questa, in definitiva, la lezione più rilevante della decisione n. 2026-911 DC: la tutela rafforzata dei minori è un obiettivo costituzionalmente ed europeisticamente forte; proprio per questo deve essere perseguita mediante una regolazione altrettanto rigorosa nel bilanciamento degli altri diritti fondamentali.

L'autore

Avv. Alessandro del Ninno - Partner di FIVERS Studio Legale e Tributario

Key4Biz People&Tech News

Il giornale specializzato sull'Innovazione tecnologica, analizzata in chiave economica, sociale e geopolitica.

Direttore: ***Luigi Garofalo***

Editore ***Supercom*** *- P. Iva 02681090425*