



FRANCESCA RICCIULLI

L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti

Il contributo, prendendo le mosse dallo schema di regolamento licenziato dall'AGCOM all'esito della consultazione sugli strumenti di *age assurance* avviata in attuazione del c.d. "Decreto Caivano", si propone di analizzare i futuri scenari normativi e applicativi relativi agli strumenti di identificazione e autenticazione dei minori. In particolare, si esamineranno gli strumenti attualmente previsti dalla normativa italiana, che stabilisce requisiti specifici per l'identificazione degli utenti, e le intersezioni di questi ultimi con le disposizioni da ultimo previste dal regolamento europeo c.d. "eIDAS 2", il quale si prefigge di garantire un'identità digitale sicura e interoperabile a livello europeo. Ciò al fine di approfondire opportunità e criticità poste dalle scelte effettuate dalla governance.

*Identità – Identità digitale – Minori – Portafoglio digitale – Strumenti di identificazione – Verifica dell'età
Servizi digitali*

The identity and digital identification of minors between national and international regulations and the measures of the competent authorities

This contribution, starting from the draft regulation approved by AGCOM following the consultation on age assurance tools initiated in implementation of the so-called "Caivano Decree", aims to analyze future regulatory and applicative scenarios related to the identification and authentication tools for minors. In particular, it will examine the tools currently provided for by Italian legislation, which establishes specific requirements for user identification, and the intersections of these with the provisions recently outlined in the European regulation known as "eIDAS 2", which aims to ensure a secure and interoperable digital identity at the European level. The goal is to explore the opportunities and challenges posed by the governance's choices.

Identity – Digital identity – Minors – Digital wallet – Identification tools – Age verification – Digital services

L'Autrice è dottoranda in Diritto pubblico presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. L'identità digitale del minore e la fruizione dei servizi online. – 2. L'evoluzione dell'identità digitale nella normativa italiana. – 3. SPID per i minori: le Linee guida dell'Agenzia per l'Italia digitale. – 4. Le più recenti novità della normativa in materia di *age verification* in Europa. – 5. I principi affermati da AGCOM sui metodi di *age assurance*. – 6. Prime conclusioni.

1. L'identità digitale del minore e la fruizione dei servizi online

Negli ultimi anni, il dibattito sull'opportunità di rafforzare la tutela dei minori nel contesto digitale è diventato sempre più rilevante, alla luce dell'integrazione crescente delle tecnologie digitali nella vita quotidiana dei giovani, che si trovano sempre più frequentemente a vivere in una dimensione digitale e a fruire di servizi online¹.

Il presente contributo vuole soffermarsi, in particolare, sull'identità digitale del minore e sulla sua identificazione, alla luce del decreto legge c.d. "Caivano"² e dello schema di regolamento adottato successivamente dall'AGCOM³.

Non può parlarsi di identità digitale del minore senza soffermarsi brevemente sui temi dell'"identità" e dell'"identità personale", nonché sulla accezione loro storicamente attribuita in ambito giuridico.

Il significato della parola "identità" si evoluto in modo sorprendente con il passare degli anni, divenendo sempre più multiforme e, a tratti, inafferrabile⁴.

Ciò, anzitutto, per quanto riguarda il concetto stesso di "identità" – individuale, di gruppo, collettiva, sociale o nazionale – e le sue modalità di formazione⁵. Va aggiunto, poi, che non solo esistono diversi tipi di identità ma anche varie dimensioni della stessa, in quanto deve essere considerato sia come una persona crede di essere che come vuole essere rappresentata, oltre a come viene rappresentata dagli altri⁶. Si aggiunge, poi, che ciascun individuo non ha una sola identità definita e stabile ma, come è stato rilevato dai più, in ciascuna persona convivono più identità⁷.

Proprio tale ultima circostanza deve essere considerata con particolare riferimento al tema in

1. Sulla tutela del minore, con particolare riferimento al contesto digitale, v. BATTELLI 2021. V. anche: STANZIONE 2014; DI SABATO 2011; STANZIONE-SCIANCELEPORE 2006.

2. d.l. 15 settembre 2023, n. 123, convertito con modificazioni dalla l. 13 novembre 2023, n. 159 (in G.U. 14 novembre 2023, n. 266).

3. Schema di provvedimento su modalità tecniche e di processo per l'accertamento della maggiore età degli utenti approvato dal Consiglio in data 24 ottobre 2024 e, al momento in cui si scrive, notificato alla Commissione europea ai sensi della Direttiva (UE) 2015/1535.

4. Per una ricostruzione storica approfondita cfr. ALPA 2021. L'autore afferma condivisibilmente che, «a differenza di quanto accadeva in passato, l'"identità personale" è diventata un'espressione polisensa e con molti margini di ambiguità». E, ancora, che «identità dunque è una parola con molti significati e per sua natura misteriosa e ambigua: attraversa i secoli portando con sé il bagaglio onusto del passato, si riflette nel presente e si proietta nel futuro»; v. anche GLEASON 1983.

5. Cfr., tra gli altri, HETERINGTON 1998.

6. RICCA 2008.

7. PINO 2010; FRIEDMAN 2002.

oggetto, poiché nel minore possono, in effetti, coesistere molteplici identità, riflesso della sua complessità interiore, e al contempo egli sviluppa nuove identità nel corso della sua crescita, adattandosi e trasformandosi in risposta alle esperienze e alle fasi evolutive che attraversa. In questo senso, la letteratura e la normativa si riferiscono al minore, parlando indifferentemente di “infanzia”, “adolescenza”, “gioinezza”, “fanciullo”, senza riuscire, spesso, ad afferrare la complessità di tale soggetto, che cresce e muta molto velocemente. Si potrebbe rilevare che ogni individuo cresce e si evolve incessantemente, ma deve considerarsi che la tutela del minore di età è, in linea generale, rafforzata e specifica in ragione di una sua presunta o effettiva maggiore “fragilità”⁸.

Da un punto di vista strettamente giuridico, come rilevato da vari autori, nel testo della Costituzione si rinviene più volte il termine “persona” ma è del tutto assente qualsiasi riferimento al termine “identità” o alla stessa associata ad attributi come “individuale” o “personale”⁹.

Nell’ambito della normativa di rango primario, invece, il concetto di identità personale si rinviene

prima nella legge n. 675 del 1996¹⁰ e, successivamente, nel d.lgs. n. 196 del 2003¹¹, ora modificato dal decreto legislativo n. 101 del 2018, che ha adeguato la normativa nazionale alle disposizioni del Regolamento generale per la protezione dei dati personali n. 2016/679 dell’Unione europea (c.d. “RGPD o in inglese “GDPR”). Si tratta di entrambi testi normativi relativi alla protezione dei dati personali.

Storicamente, in effetti, l’elaborazione della nozione giuridica di “identità personale” non si deve alle codificazioni ma alla dottrina e alla giurisprudenza che si sono sviluppate già in tempi più risalenti sul tema¹². In particolare, si sono sviluppate due nozioni di identità personale, una c.d. “estrinseca” e una “sostanziale”¹³. Quest’ultima è stata ricostruita in una prima frase come “diritto ad essere correttamente rappresentati”¹⁴, in una seconda, a partire dalla storica sentenza della Corte costituzionale del 1994, come “diritto ad essere sé stessi”¹⁵.

La nozione che viene in rilievo in questa sede, però, è la prima, cioè quella di identità c.d.

8. Si pensi, ad esempio, all’art. 61 c.p., che disciplina le circostanze aggravanti comuni, ovvero quelle situazioni al verificarsi delle quali il giudicante deve aumentare la pena finale da infliggere al reo. Ebbene, l’art. 61 n. 5 c.p. disciplina l’aggravante della minorata difesa, che ricorre ogniqualvolta l’autore del reato approfitta di «circostanze di tempo, di luogo o di persona, anche in riferimento all’età, tali da ostacolare la pubblica o privata difesa». Trattasi, pertanto, della situazione di colui che, per un qualunque motivo, si trova in una peculiare situazione di debolezza e/o inferiorità rispetto a colui che pone in essere la condotta delittuosa. Si noti anche che la “fragilità”, in questo, come in altri casi, può essere dovuta anche all’età molto avanzata.

9. Tra gli altri cfr. MORELLI 2019. Tale circostanza sarebbe da imputare al fatto che il peso dell’esperienza autoritaria, che rappresentò, in negativo, un punto di riferimento costante per i Costituenti sia per l’elaborazione della parte della Carta relativa ai diritti sia per quella concernente i poteri, evidentemente dissuase gli autori del testo dall’introdurre riferimenti espliciti all’idea di un’identità collettiva, eccetto i richiami al concetto di “nazione”.

10. Cfr. art. 1: «La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione», successivamente abrogato ai sensi dell’articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

11. Cfr. art. 2: «Il presente testo unico, di seguito denominato “codice”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali».

12. Per un approfondimento sul tema del diritto all’identità personale da un punto di vista storico e con riferimento ad entrambe le prospettive cfr. PINO 2010. Cfr. anche PINO 2003; TRUCCO 2004; RANDAZZO 2021; RAFFIOTTA 2010; RESTA 2007.

13. PINO 2010.

14. Lettura della prima dottrina: DE CUPIS 1949; ASCARELLI 1957; ARE 1965 e della prima giurisprudenza: Pretura di Roma del 6 maggio 1974 ma anche la nota Corte Cass n. 3769 del 22 giugno 1985.

15. Corte Cost. sent. n. 13 del 1994.

“estrinseca”, intesa come mezzo che consente l'identificazione di un soggetto¹⁶, in quanto più legata alla identità digitale¹⁷ e all'oggetto del presente contributo.

Questa nozione dell'identità personale è, a ben vedere, la ricostruzione più tradizionale ed è stata definita dalla dottrina più recente anche “anagrafica”¹⁸, in quanto si riferisce al complesso delle risultanze anagrafiche che servono a identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati¹⁹ e si rinviene anche in alcune codificazioni più risalenti²⁰.

È evidente che il tema riguarda ogni individuo, non solo i minori. L'identificazione delle persone all'interno della società, del resto, persegue un fine prima di tutto pubblicistico, regolando i rapporti tra i cittadini e lo Stato²¹. Più nel dettaglio, consente allo Stato di esercitare un controllo sul territorio e sulla popolazione, tanto per finalità di sicurezza quanto per la efficace e efficiente organizzazione dei servizi amministrativi. Tale controllo si riflette altresì nell'ambito del diritto privato, dove la precisa identificazione assume il ruolo di garanzia dei rapporti tra i consociati.

2. L'evoluzione dell'identità digitale nella normativa italiana

L'identità digitale avrebbe, secondo alcuni, la stessa natura bifronte dell'identità personale, potendo

essere intesa, in modo più sostanziale, come *alter ego* virtuale della persona²² oppure, in una nozione più tecnica, come insieme delle informazioni che di una persona consentono l'identificazione²³.

Da un punto di vista squisitamente giuridico, il concetto di “identità digitale” o “identità elettronica” è stato codificato, a livello nazionale, all'interno del d.lgs n. 82 del 2005, recante il “Codice dell'amministrazione digitale” (noto anche come “CAD”), testo di riferimento per la normativa in materia di trasformazione digitale della pubblica amministrazione.

Ai fini del presente contributo, può essere utile una precisazione proprio sull'ambito soggettivo del d.lgs n. 82 del 2005.

Se la versione originaria del Codice ne limitava l'ambito di applicazione solo alle pubbliche amministrazioni di cui all'art. 1, comma 2, d.lgs. n. 165/2001 e alle società ed enti inseriti nel conto economico consolidato dello stato (redatto da Istat), a seguito del d.lgs. n. 179/2016 e d.lgs. n. 217/2017, è stato novellato l'art. 2, comma 2 del Codice, prevedendo che le disposizioni in esso contenute si applichino, oltre alle pubbliche amministrazioni in senso stretto (art. 2, comma 2, lett. a)), anche:

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse²⁴; e

16. FINOCCHIARO 2010. Sulla individuazione “inequivoca” della persona v. RESTA 2007.

17. Per un approfondimento cfr. RICCIULLI 2024.

18. PINO 2010. Come affermato dall'autore, in questo senso, il rilievo giuridico dell'identità personale consiste nell'insieme dei segni distintivi esteriori della persona: il nome, alcune caratteristiche somatiche (l'altezza, il sesso), l'indirizzo di residenza – in ciò che può rendere quella persona facilmente identificabile da parte del pubblico potere.

19. cfr. RESTA 2007; BASSU 2021.

20. Sull'identificazione da parte del notaio v., ad esempio, l'art. 49, l. 89/1913.

21. Cfr. TRUCCO 2004.

22. In questo senso, IANNUZZI-LAVIOLA 2023, p. 12.

23. In questo senso, v. RESTA 2007. Per un approfondimento sul tema cfr. anche LUCIANI 2018; ALPA 2021.

24. Si riporta quanto contenuto nella Relazione illustrativa allo schema di decreto legislativo di attuazione della legge n. 124/2015 (recante “Deleghe al Governo in materia di riorganizzazione delle pubbliche amministrazioni”), nella quale si chiarisce che è stato previsto un elenco dettagliato di soggetti a cui si applicano le norme del CAD, specificando che «per i gestori di servizi pubblici ciò avviene in relazione ai servizi di pubblico interesse. Tenuto conto del grande numero di servizi pubblici forniti da soggetti privati in forza di concessioni, infatti, si è ritenuto opportuno riconoscere agli utenti analoghi diritti di cittadinanza digitale anche in relazione ai fornitori di detti servizi, in attuazione di quanto previsto dal principio di delega contenuto nell'articolo 1, comma 1, lettera h) ai sensi del quale tra gli obiettivi dell'intervento normativo vi è anche quello di semplificare le condizioni di

c) alle società a controllo pubblico, come definite nel d.lgs. 175/2016, escluse le società quotate di cui all'articolo 2, comma 1, lett. p), del medesimo decreto che non rientrino nella lettera b)²⁵.

Con riferimento alla *ratio* della novella legislativa, si ritiene che debba essere rinvenuta, oltre che nell'evitare sprechi di risorse pubbliche, nell'intento del Legislatore di rafforzare il riconoscimento dei diritti digitali dei cittadini e degli utenti, estendendo, a tal fine, il campo soggettivo di applicazione del Codice.

In tal senso, si ritiene utile ricordare che la Relazione illustrativa allo schema di decreto legislativo di attuazione della richiamata l. n. 124/2015 fissa come obiettivo principale dell'intervento normativo la semplificazione dell'esercizio dei diritti del cittadino, in materia di digitalizzazione, favorendo servizi per la collettività sicuri, accessibili, interoperabili e trasparenti. Si spiega, dunque, il perché sia stato previsto un ampliamento della platea dei soggetti, che a qualunque titolo e costituiti in qualsiasi forma giuridica, svolgono un servizio di pubblico interesse: il diritto ad un servizio pubblico qualitativamente alto, al quale il cittadino può partecipare direttamente e del quale ha diritto a rimanere soddisfatto.

Per completezza, risulta utile aggiungere che il comma 3 dell'art. 2 CAD specifica che «con riferimento al documento informatico, alle firme elettroniche e ai servizi fiduciari di cui al Capo II, alla

riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, al domicilio digitale e alle comunicazioni elettroniche di cui all'articolo 3-*bis* e al Capo IV, all'identità digitale di cui agli articoli 3-*bis* e 64, le disposizioni del Codice e le relative Linee guida concernenti si applicano anche ai privati, ove non diversamente previsto».

Gli articoli da 3 a 9 di questo Codice dell'amministrazione digitale formano la «Carta della cittadinanza digitale», sezione che prevede un nucleo minimo di diritti e doveri digitali degli «utenti» e che questi ultimi vantano nei confronti dei soggetti citati obbligati all'applicazione del Codice²⁶.

Diritto fondamentale previsto dalla Carta della cittadinanza digitale è il diritto all'identità digitale, regolato dall'art. 3-*bis* CAD²⁷. La disposizione prevede il diritto di chiunque di accedere ai servizi online dei soggetti di cui all'art. 2, comma 2 CAD, utilizzando un sistema di identificazione elettronica, come lo SPID (Sistema Pubblico di Identità Digitale)²⁸ o la Carta di Identità Elettronica (CIE), nonché tramite la c.d. «app IO» (punto di accesso telematico di cui all'art. 64-*bis* CAD).

L'art. 7 CAD, dedicato ai servizi online, dal canto suo, prevede l'obbligo per i soggetti di cui all'art. 2, comma 2 CAD di consentire l'accesso ai propri servizi tramite il proprio sito a valle, se occorre, di identificazione tramite gli strumenti menzionati, oppure tramite il punto di accesso telematico di cui all'art. 64-*bis* CAD (c.d. «app IO»)²⁹.

esercizio dei diritti e l'accesso ai servizi di interesse dei cittadini, obiettivo che si persegue ampliando il novero dei soggetti tenuti ad applicare le norme del CAD».

25. Con riguardo alla lettera c), pur non essendo particolarmente critica l'interpretazione circa i soggetti individuati dalla disposizione, vista la chiara definizione di società a controllo pubblico, quali «società in cui una o più amministrazioni pubbliche esercitano poteri di controllo», più problematica risulta l'esclusione delle società quotate, come definite all'articolo 2, comma 1 del d.lgs. 175/2016. Il CAD, infatti, esclude le società quotate dall'applicazione del testo, ma solo se le medesime società non siano gestori di servizi pubblici e non esercitino servizi di pubblico interesse.

26. Ad eccezione di casi specifici, di solito tutti i soggetti di cui all'art. 2, comma 2 CAD.

27. Art. 3-*bis* CAD, rubricato «Identità digitale e Domicilio digitale», al comma 01, afferma che «Chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, tramite la propria identità digitale e anche attraverso il punto di accesso telematico di cui all'articolo 64-*bis*».

28. «Insieme aperto di soggetti pubblici e privati» che, previo accreditamento da parte dell'AgID, «identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete» (cfr. art. 64, comma 2-*ter*, CAD). Sistema istituito dall'art. 17-*ter* d.l. 21 giugno 2013, n. 69 (conv. con mod. dalla legge 9 agosto 2013, n. 98), di modifica dell'art. 64 del d.lgs. n. 82/2005, al fine di «favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese» (cfr. art. 64, comma 2-*bis*, CAD).

29. Art. 7 CAD, rubricato «Diritto a servizi on-line semplici e integrati» afferma che: «1. Chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato, tramite

Con specifico riferimento a SPID, il d.P.C.M. del 24 ottobre del 2014 ha definito l'identità digitale come "la corrispondenza biunivoca tra un utente e i suoi attributi identificativi, certificata attraverso dati raccolti e registrati in formato digitale"³⁰ e SPID come "sistema che consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano".

La normativa vigente, quindi, impone alle pubbliche amministrazioni di rendere accessibili tramite SPID i servizi in rete erogati che richiedono identificazione informatica (cfr. art. 64, comma 2-*quater*, CAD). Al contempo, però, la stessa normativa riconosce ai privati, ai fini dell'erogazione dei propri servizi in rete, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti (art. 64, comma 2-*quinquies*, CAD).

La normativa regolamentare sullo SPID in materia di adesione al sistema da parte dei fornitori di servizi online, pertanto, prevede una disciplina differenziata a seconda che il soggetto fornitore aderente sia o meno un ente tenuto a garantire i diritti digitali degli utenti sanciti nella "Carta della cittadinanza digitale".

I fornitori di servizi, dunque, secondo quanto previsto nel Decreto, sono deputati a inoltrare, nell'ambito di un servizio online, le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e a riceverne l'esito.

Per quanto riguarda ulteriori profili di regolazione tecnica, il d.P.C.M. in esame attribuisce all'Agenzia per l'Italia Digitale il compito di definire con proprio regolamento, tra l'altro, le regole tecniche e le modalità attuative per la realizzazione dello SPID e le modalità di accreditamento dei soggetti aderenti (cfr. art. 4, commi 2 e 3, d.P.C.M.).

Rileva dunque il "Regolamento recante le modalità attuative dello SPID" (cfr. Det. D.G. AgID n. 44 del 28 luglio 2015 e ss.mm.ii), che definisce le regole per il rilascio dell'identità digitale all'utente da parte del gestore (*identity provider*), nonché le

modalità di gestione e utilizzo dell'identità digitale. In particolare, con riferimento all'utilizzo dell'identità digitale, rileva l'art. 25 del Regolamento, che disciplina l'autenticazione tramite SPID, ossia «il processo in cui l'utente, usando le proprie credenziali SPID, dimostra la propria identità al gestore dell'identità digitale al fine di accedere a servizi disponibili in rete».

Secondo quanto stabilito nel regolamento, «Le relazioni tra i soggetti coinvolti nel processo (l'utente, il gestore dell'identità digitale, il fornitore di servizi ed, eventualmente, il gestore di attributi qualificati) si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata dal soggetto titolare di una identità digitale, portano all'autorizzazione o al diniego della fruizione di un servizio erogato da un fornitore di servizi». Tali interazioni determinano la produzione di particolari certificazioni, dette "asserzioni SPID" da parte dell'*identity provider*, che consente l'utilizzo delle stesse da parte dei fornitori di servizi. L'asserzione SPID viene rilasciata una volta che il gestore dell'identità digitale abbia verificato l'identità del soggetto sulla base di credenziali fornite dallo stesso. Se tale verifica ha esito positivo, l'asserzione SPID viene emessa, ad uso del fornitore dei servizi.

L'art. 24 del Decreto "Semplificazioni", intervenendo sull'articolo 64 del CAD, ha disposto l'equiparazione di SPID e CIE e indicato il 28 febbraio 2021 quale data per lo switch off delle modalità diverse di identificazione per l'accesso ai servizi online delle pubbliche amministrazioni da parte dei cittadini (nuovo art. 64, comma 3-*bis*, CAD).

Pertanto, i soggetti di cui all'art. 2, comma 2, lett. a) CAD (solo le pubbliche amministrazioni in senso stretto), a partire da quella data, devono utilizzare esclusivamente i suddetti strumenti di identificazione digitale per l'accesso dei soli cittadini (non si parla anche di imprese e professionisti) ai propri servizi online.

A partire da tale data, è fatto divieto alle pubbliche amministrazioni di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei

gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso di cui all'articolo 64-*bis*, anche attraverso dispositivi mobili» [...].

30. Il d.P.C.M. 24 ottobre 2014 reca "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese" e costituisce normativa di attuazione dell'articolo 64 CAD.

cittadini ai propri servizi in rete diverse da SPID, CIE o CNS, fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il 30 settembre 2021³¹.

Parallelamente a questi sviluppi nazionali, si sta lavorando anche a livello europeo per creare una identità digitale unica europea. Il Regolamento n. 910 del 2014, noto come "Regolamento eIDAS", aveva già posto le basi per la creazione di un quadro normativo comune per l'identità digitale, le firme elettroniche e altri servizi fiduciari.

Da ultimo, è stato raggiunto un accordo sul Regolamento c.d. "eIDAS 2", che mira a creare il Portafoglio Europeo di Identità Digitale (*European Digital Identity Wallet* – EDIW). Questo permetterà ai cittadini europei di utilizzare una sola identità digitale per accedere ai servizi pubblici e privati in tutta l'Unione europea³².

In attuazione di quanto previsto a livello sovranazionale, si sta lavorando al *wallet* italiano, c.d. "IT Wallet". Il Sistema *IT-Wallet* è istituito dall'art. 20, comma 1, lett. e), d. 2 marzo 2024, n. 19, (convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56), che ha novellato il CAD introducendo l'art. 64-*quater*, recante "Sistema di portafoglio digitale italiano – Sistema IT-Wallet".

L'istituzione del Sistema *IT-Wallet*, per espressa previsione normativa, persegue una duplice finalità: innanzitutto, valorizzare e rafforzare l'interoperabilità tra le banche dati pubbliche attraverso la Piattaforma Digitale Nazionale Dati ("PDND"), di cui all'articolo 50-*ter* del CAD, e, inoltre, favorire la diffusione e l'utilizzo di servizi in rete erogati da soggetti pubblici e privati (cfr. comma 1).

Ai sensi del comma 2, il Sistema *IT-Wallet* si compone di due soluzioni di portafoglio digitale, pubblico e privato. L'*IT-Wallet* pubblico è reso disponibile mediante il punto di accesso telematico di cui all'articolo 64-*bis* del CAD ("app IO")³³.

3. SPID per i minori: le Linee guida dell'Agenzia per l'Italia digitale

Nel contesto normativo appena descritto, il 3 marzo 2022, con Determinazione n. 51, l'Agenzia per l'Italia Digitale ha pubblicato le *Linee guida operative per la fruizione dei servizi SPID da parte dei minori*³⁴. Tali Linee guida intendono definire le modalità di rilascio dell'identità digitale al minore e le modalità di fruizione dei servizi online mediante tale identità.

Anche in questo caso, la *ratio* dell'intervento è la particolare condizione di fragilità riconosciuta al minore. Si legge, infatti, nelle Linee guida che «la normativa vigente consente la creazione dell'identità digitale in favore di tutti i cittadini. Risulta evidente, tuttavia, la necessità di una tutela specifica per un soggetto fragile come il minore».

In particolare, il documento individua le modalità operative che i gestori dell'identità digitale e i fornitori di servizi SPID devono porre in essere al fine di consentire ai minori la fruizione dei servizi in rete in piena sicurezza.

Gli obiettivi, per espressa previsione delle Linee guida, sono: «1. consentire ai minori di acquisire la propria identità digitale, previa richiesta da parte di chi esercita la responsabilità genitoriale; 2. consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando – salvo casi specifici – la possibilità di autorizzazione e verifica da parte dell'esercente la responsabilità genitoriale; 3. consentire ai fornitori di servizi in rete la selezione dei propri utenti in base all'età».

Più che i profili tecnici, rilevano, in questa sede, i principi fondamentali sottesi al documento.

In primo luogo, emerge il *principio di responsabilità genitoriale*. Le Linee guida attribuiscono un ruolo centrale al genitore, in qualità di esercente la responsabilità genitoriale, nel processo di rilascio

31. Per un approfondimento cfr. BELISARIO–RICCIULLI–PAGNOTTA 2020.

32. Per un approfondimento cfr. MANCA 2024.

33. Per un approfondimento cfr. RICCIULLI 2024.

34. Cfr. il testo della Determinazione. Ai sensi dell'art. 14-*bis* CAD, comma 2, lett. a), infatti, tra le funzioni dell'Agenzia c'è quella di a) emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea.

e gestione dell'identità digitale SPID del minore. Solo il genitore in possesso di un'identità SPID può richiederne una per il figlio, garantendo un primo livello di controllo e sicurezza. Inoltre, il genitore è costantemente coinvolto attraverso un sistema di notifiche che lo informa delle richieste di accesso del minore ai servizi online, consentendogli di autorizzare o negare l'accesso in base alle proprie valutazioni.

Un secondo principio cardine è quello della *protezione dei dati personali del minore*, declinato secondo i principi del GDPR. Le Linee guida sottolineano, infatti, l'importanza di applicare i principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, aggiornamento, limitazione della conservazione, integrità e riservatezza. In particolare, la procedura di identificazione del minore è stata progettata per richiedere solo i dati strettamente necessari, riducendo al minimo l'esposizione del minore a rischi di privacy.

Le Linee guida promuovono inoltre il principio di *gradualità nell'autonomia del minore*. Si riconosce che il grado di autonomia del minore nell'utilizzo di SPID deve essere commisurato alla sua età e maturità. Per i minori infraquattordicenni, l'accesso è limitato ai servizi essenziali, come quelli scolastici o di prevenzione e consulenza, senza la necessità di autorizzazione genitoriale. Ai minori ultraquattordicenni è concesso un maggiore livello di autonomia, con la possibilità di accedere a un più ampio ventaglio di servizi, previa autorizzazione del genitore. Al compimento della maggiore età, il neo maggiorenne acquisisce il pieno controllo della propria identità digitale, con la possibilità di revocare o mantenere l'identità precedentemente rilasciata. Si ritiene che tale principio risulti fondamentale per la creazione di un'autonoma identità del minore, laddove la scelta di approcci più repressivi potrebbe proteggere ma anche disincentivare lo sviluppo della personalità.

Infine, le Linee guida pongono l'accento sul principio di *flessibilità e adattabilità*. Il sistema di gestione di SPID per i minori è stato progettato per

adattarsi alle diverse esigenze e situazioni, offrendo un elevato grado di personalizzazione. Ad esempio, i gestori dell'identità digitale (IdP) hanno la possibilità di implementare diverse modalità di identificazione del minore, anche in assenza di un numero di telefono cellulare o di un dispositivo mobile. Questa flessibilità garantisce l'inclusione di tutti i minori, a prescindere dalla loro condizione sociale o tecnologica.

Ebbene, posto il generale favore con cui all'epoca fu salutato il provvedimento dell'Agenzia, che si fonda sui condivisibili principi appena esposti, ritengo debbano essere svolte almeno due ordini di riflessioni.

La prima è che SPID per i minori fa parte di una più complessa strategia della governance legata alla volontà di diffondere l'identità digitale e lo strumento SPID. Al netto dell'utilità dello strumento per i fini di verifica dell'età, infatti, la scelta di estendere SPID ai minori ha indubbiamente anche contribuito ad ampliare la platea delle persone che potevano (e in alcuni casi dovevano) dotarsi di un'identità digitale in un momento, come quello che stava vivendo il Paese nel 2022, in cui il Legislatore, a valle della pandemia da Covid-19 e degli investimenti del PNRR, puntava a diffondere l'identità digitale presso fasce sempre più ampie della popolazione.

Si aggiunge che tale strumento, nonostante gli investimenti effettuati anche ad opera del PNRR, presenta ancora diversi limiti. Sebbene, come esposto, lo SPID potrebbe, ai sensi dell'art. 2, comma 3, del CAD, essere reso obbligatorio anche per i servizi resi dai privati oltre che per i soggetti pubblici, gli stessi sarebbero sempre liberi di investire su strumenti di identificazione alternativi. Come esposto, del resto, solo per le pubbliche amministrazioni in senso stretto, ha validità lo "switch off" degli strumenti alternativi previsto dal Legislatore con il "Decreto Semplificazioni". È proprio, però, con riferimento ai servizi privati, soprattutto i social network, che si avverte da anni l'esigenza di regolarne l'accesso. Si registrano, in questo senso, innumerevoli proposte di legge sul tema³⁵.

35. Quelle di Sportiello [C. 1771](#), Bonelli [C.1800](#) e Madia [C.1863](#) sono solo alcune delle proposte di legge sul tema attualmente in discussione.

4. Le più recenti novità della normativa in materia di *age verification* in Europa

Come noto, da anni la normativa in materia di *data protection* ha stabilito regole dedicate e più stringenti agli utenti minorenni³⁶.

Da ultimo, i temi dei servizi digitali e dei diritti degli utenti rispetto agli stessi sono stati profondamente impattati dall'entrata in vigore del Regolamento 2022/2065, Digital services act (c.d. "DSA").

Quest'ultimo, all'articolo 28, prescrive che tutti i fornitori di piattaforme online adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori, anzitutto mediante l'attivazione dei meccanismi di verifica dell'età. Inoltre, ai sensi dell'articolo 35, paragrafo 1, lettera j) del DSA, i fornitori di piattaforme online di dimensioni "molto grandi" e di motori di ricerca online di dimensioni "molto grandi" devono adottare misure di attenuazione dei rischi sistemici, tra cui "misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi".

Disposizioni analoghe sono contenute nella Direttiva (UE) 2018/1808, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato, recepita in Italia con d.lgs. 208/2021, Testo Unico dei servizi di media audiovisivi (cd. "TUSMA")³⁷.

La normativa sovranazionale, dunque, richiama l'esigenza di meccanismi di *age assurance*³⁸,

stabilendo che i minori hanno diritto ad un livello più elevato di protezione dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale, anche introducendo misure più rigorose nei confronti di ogni servizio della società dell'informazione.

Alla luce della normativa sovranazionale ma anche in ragione di vicende contingenti, è intervenuto il già citato d.l. 15 settembre 2023, n. 123, convertito con mod. dalla l. n. 159 del 2023, c.d. "Decreto Caivano", recante "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale"³⁹.

In particolare, prevede, al Capo IV, "Disposizioni per la sicurezza dei minori in ambito digitale" e, tra le altre cose, nell'ambito dell'art. 13-*bis*, introduce disposizioni per la verifica della maggiore età con specifico riferimento all'accesso a siti pornografici, sulla base della presunzione secondo la quale i contenuti a carattere pornografico minerebbero il rispetto della "dignità" dei minori e ne "compromettono" il "benessere fisico e mentale", comportando, di conseguenza, un problema di "salute pubblica". La disposizione prevede, di conseguenza, al comma 2, che i gestori di siti web e i fornitori delle piattaforme di condivisione video (ovunque stabiliti), che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto.

Il Governo ha colto l'occasione anche per ottemperare a quanto previsto dall'art. 49, comma 2, del DSA sui servizi digitali, designando l'Autorità per le garanzie nelle comunicazioni quale Coordinatore dei servizi digitali per l'Italia.

36. Cfr. art. 8 e considerando 38 GDPR, nonché il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101).

37. OROFINO 2022.

38. Con il termine "Age assurance" o "Garanzia dell'età" si intende l'insieme dei metodi, sistemi e processi utilizzati per determinare l'età o la fascia di età di un individuo a vari livelli di confidenza o certezza.

39. Il decreto prende il nome dai gravi fatti avvenuti nel Comune di Caivano, che hanno coinvolto alcuni minori. In particolare, il Governo ha adottato il decreto «Ritenuta la straordinaria necessità e urgenza di introdurre disposizioni per il contrasto alla criminalità minorile e all'elusione scolastica, e per la tutela delle minori vittime di reato» e «la straordinaria necessità ed urgenza di rafforzare la tutela dei minori nello spazio cibernetico e rispetto all'offerta di contenuti e servizi on line, al fine di garantirne il benessere e il pieno sviluppo fisico e mentale».

Ebbene, si ritiene che tale intervento del Governo debba essere letto alla luce dell'approccio scelto anche in altri Paesi europei⁴⁰.

In Francia, ad esempio, la Corte d'appello di Parigi ha emesso una recentissima ordinanza⁴¹ nei confronti di alcuni gestori di siti extraeuropei che offrono contenuti pornografici, in ragione del fatto che tali piattaforme non adotterebbero misure sufficienti per verificare l'età degli utenti. In particolare, in base all'ordinanza, i fornitori di servizi di telecomunicazione sono obbligati a impedire l'accesso a tali siti entro 15 giorni dalla notifica dell'ordine, finché detti siti non avranno adottato un sistema di verifica dell'età più rigoroso. Si legge nell'ordinanza che la Corte ha ritenuto che "l'interesse del minore" sia un "aspetto primario" che giustifica l'eventuale violazione di "altri diritti come la libertà di espressione o di comunicazione".

La Francia, del resto, aveva già adottato una legge che prevede l'obbligo per i siti per adulti di verificare che i minori non accedano ai loro contenuti⁴². Quest'ultima, analogamente al "Decreto Caivano", prevede altresì l'adozione da parte dell'Autorità di regolamentazione della comunicazione audiovisiva e digitale francese (Arcom) di un documento che determini i requisiti tecnici minimi applicabili ai sistemi di verifica, dell'età che devono essere utilizzati dai siti che diffondono contenuti pornografici.

L'Arcom, in data 9 ottobre 2024, ha pubblicato una bozza sottoposta a consultazione pubblica e alla Commissione nazionale per l'informatica e la libertà civili (CNIL)⁴³, che agisce nel Paese quale autorità per la protezione dei dati personali.

In effetti, anche la Commissione europea sta monitorando attentamente la questione della verifica dell'età, che, come anticipato, è considerata una priorità nel contesto del Digital Services Act. In questo senso, a giugno scorso, ha richiesto chiarimenti a piattaforme che offrono contenuti pornografici sulle misure adottate per mitigare i rischi legati alla protezione dei minori online, come previsto dal DSA⁴⁴. Inoltre, il 31 luglio 2024 la Commissione ha pubblicato un invito agli *stakeholder* a presentare contributi volti a sostenere la Commissione per l'elaborazione di orientamenti nel quadro del DSA, al fine di raccoglierne i contributi sull'ambito di applicazione, l'approccio e il contenuto degli orientamenti. Infine, il 14 ottobre 2024 la Commissione ha pubblicato il bando di procedura ad evidenza pubblica per attività di sviluppo, consultazione e supporto per una soluzione di *age verification*⁴⁵. Parallelamente, sotto un altro profilo attinente più strettamente alla questione della protezione dei dati personali, nella seduta del 14 marzo 2024 del Comitato europeo per la protezione dei dati, le autorità nazionali per la protezione dei dati hanno discusso l'attribuzione di un mandato al Comitato stesso ai fini dell'individuazione di criteri per i trattamenti di verifica dell'età, con l'obiettivo di giungere a un approccio coerente e armonizzato per quanto riguarda i principi generali di protezione dei dati da garantire in tale contesto e i requisiti tecnici per detti sistemi, proprio in virtù della sussistenza di diversi obblighi giuridici a introdurre un meccanismo di verifica da parte della normativa unionale (come, per l'appunto, il DSA e l'AVMS).

40. Cfr. sul tema NATALE 2024.

41. *Decisione de la chambre 1-3 de la cour d'apel de Paris sur le blocage de plusieurs sites internet permettant l'accès des mineurs, sur le territoire français, a des contenus pornographiques*, 17 ottobre 2024.

42. Legge n. 2024-449. La legge per la sicurezza e la regolamentazione dello spazio digitale (la "Legge SREN") è stata adottata il 21 maggio e pubblicata nel "Journal Officiel" il 22 maggio. Alcuni dei gestori dei siti hanno avviato azioni legali per contestare l'applicazione della norma.

43. *Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne* del 9 ottobre 2024.

44. Le richieste sono state fatte dopo che queste piattaforme erano state classificate come "grandi piattaforme digitali" ai sensi del DSA lo scorso dicembre. I siti coinvolti hanno successivamente presentato ricorso e le cause sono attualmente tuttora in corso.

45. European Commission, *Call for tenders EC-CNECT/LUX/2024/OP/0073 – Development, Consultancy and Support for an Age Verification Solution*.

5. I principi affermati da AGCOM sui metodi di *age assurance*

L'Autorità per le garanzie nelle comunicazioni è attiva da diversi anni sul tema della tutela dei minori nello spazio digitale⁴⁶.

Da ultimo, con delibera n. 61/24/CONS, in attuazione della l. 13 novembre 2023, n. 159, che dispone la conversione, con emendamenti, del citato "Decreto Caivano", ha avviato una consultazione pubblica⁴⁷ sugli strumenti di *age assurance*⁴⁸.

A tale consultazione hanno partecipato altre istituzioni, associazioni di categoria e di

consumatori, piattaforme di condivisione video. È stato altresì acquisito parere favorevole del Garante per la protezione dei dati personali⁴⁹ (con qualche precisazione, anche riguardo al metodo più sicuro da utilizzare per la validazione dell'identità dell'utente).

In data 7 ottobre 2024, l'AGCOM ha reso noto che, nella seduta del 24 settembre 2024, a valle della consultazione, è stato approvato uno schema di regolamento⁵⁰ che disciplinerà le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti. Tale schema, in quanto contenente

-
46. V. delibera n. 9/23/CONS, del 25 gennaio 2023, recante "Adozione delle linee guida finalizzate all'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di sistemi di protezione dei minori dai rischi del cyberspazio".
47. Cfr. art. 13-bis, commi 3, 4 e 5, d.l. 123 del 2023, i quali recitano: «3. L'Autorità per le garanzie nelle comunicazioni stabilisce, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo. 4. Entro sei mesi dalla data di pubblicazione del provvedimento di cui al comma 3, i soggetti di cui al comma 2 si dotano di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni impartite nel predetto provvedimento. 5. L'Autorità per le garanzie nelle comunicazioni vigila sulla corretta applicazione del presente articolo e, in caso di inadempimento, contesta ai soggetti di cui al comma 2, anche d'ufficio, la violazione, applicando le disposizioni di cui all'articolo 1, comma 31, del decreto legislativo 31 luglio 1997, n. 249, e li diffida ad adeguarsi entro venti giorni. In caso di inottemperanza alla diffida, l'Autorità per le garanzie nelle comunicazioni adotta ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino, da parte dei soggetti di cui al comma 2, di condizioni di fornitura conformi ai contenuti della diffida dell'Autorità. Poteri specifici, del resto, sono assegnati all'Autorità dal Testo Unico sui Servizi Media Audiovisivi (TUSMA) a tutela dei minori, articoli 41 e 42, rispetto a contenuti che possano nuocere al loro sviluppo fisico, mentale o morale».
48. Come si legge nelle definizioni dello schema di Regolamento per «"Garanzia dell'età" o "Age assurance" si intende l'insieme dei metodi, sistemi e processi utilizzati per determinare l'età o la fascia di età di un individuo a vari livelli di confidenza o certezza. Le tre categorie principali di metodi di assicurazione dell'età sono l'autodichiarazione, la verifica dell'età e la stima dell'età. Autodichiarazione (di seguito anche Self-declaration) si riferisce all'insieme di processi in cui un utente inserisce una data o seleziona una casella di un form, anche online, per dichiarare di essere sopra/sotto una determinata età, senza fornire altre prove; Stima dell'età (di seguito anche Age estimation) si riferisce ai metodi che stabiliscono che con una certa probabilità un utente abbia una certa età, rientri in una fascia di età o sia superiore o inferiore a una certa età. I metodi di stima dell'età includono l'analisi automatizzata di dati comportamentali e ambientali, confrontando il modo in cui un utente interagisce con un dispositivo o con altri utenti della stessa età, metriche derivate dall'analisi dei movimenti del corpo, il riconoscimento facciale, o l'analisi delle capacità o conoscenze. Nei metodi utilizzati per una stima dell'età rientrano anche quelli effettuati mediante algoritmi e il ricorso a tecnologie basate sull'intelligenza artificiale. Verifica dell'età (di seguito anche Age verification) fa riferimento a quei sistemi che si basano su identificatori rigidi (fisici) e/o fonti di identificazione verificate, che forniscono un elevato grado di certezza nel determinare l'età di un utente».
49. Come previsto dall'art. 13-bis, comma 3, d.l. 123 del 2023.
50. V. *Modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai sensi dell'articolo 13 bis del decreto legge 5 settembre 2023, n. 123 convertito con modificazioni dalla legge 13 novembre 2023, n. 159*.

disposizioni rientranti nella definizione di “regola tecnica” di cui alla Direttiva (UE) 2015/1535, è stato notificato alla Commissione europea per l'ultimo vaglio. Conseguentemente, in virtù della procedura attivata, l'AGCOM non potrà adottare il regolamento prima del 17 gennaio 2025, salvo eventuali ulteriori estensioni del termine richiesti dalla Commissione ai fini della valutazione di conformità con il diritto unionale.

L'Autorità ha scelto, al fine di non impattare eccessivamente sugli operatori di mercato e di prevenire l'obsolescenza tecnologica, un approccio tecnologicamente neutrale, che consente ai soggetti tenuti alla realizzazione dei processi di *age*

assurance «una ragionevole libertà di valutazione e scelta», stabilendo tuttavia i principi e requisiti che devono essere soddisfatti dai sistemi messi in campo⁵¹.

Rispetto ai contenuti di siti e piattaforme, l'Autorità ha precisato che le modalità tecniche prescelte nell'ambito del provvedimento in oggetto sono “altamente raccomandate” anche con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori quali ad esempio le categorie previste dalla delibera 9/23/CONS⁵².

51. Tali principi sono: *Proporzionalità*: occorre trovare un equilibrio adeguato tra i mezzi impiegati per verificare l'età e l'impatto che tali mezzi possono avere sulla limitazione dei diritti delle persone. *Protezione dei dati personali (riservatezza)*: i sistemi di verifica dell'età devono rispettare le normative sulla protezione dei dati previste dal Regolamento GDPR (UE) 2016/679, garantendo la minimizzazione dei dati, la precisione e la limitazione della conservazione. Non è ammesso il trattamento di dati personali come quelli presenti sui documenti di identità, immagini fotografiche o video, dati delle carte di credito, o altre informazioni personali sensibili. *Sicurezza*: Il sistema di verifica dell'età deve prevedere adeguate misure di sicurezza informatica per ridurre i rischi di attacchi e proteggere il sistema da tentativi di elusione, conformemente al GDPR e alla proposta di Cyber Resilience Act (CRA). *Precisione ed efficacia*: Il sistema deve essere accurato nel determinare l'età, minimizzando gli errori. La verifica dell'età deve essere eseguita ad ogni accesso ai siti o piattaforme di condivisione video che diffondono contenuti pornografici. La validità della verifica termina quando l'utente esce dal servizio, dal browser o quando si verificano eventi come la sospensione del sistema operativo o 45 minuti di inattività. *Funzionalità, accessibilità e facilità d'uso*: I sistemi di verifica dell'età devono essere semplici da utilizzare, adattandosi alle capacità e necessità specifiche dei minori, senza ostacolare l'accesso ai contenuti su Internet. *Inclusività e non discriminazione*: Il sistema di verifica dell'età deve essere progettato in modo da evitare, o almeno minimizzare, qualsiasi forma di pregiudizio o discriminazione involontaria nei confronti degli utenti. *Trasparenza*: Gli operatori devono essere chiari e trasparenti con gli utenti riguardo ai sistemi di verifica dell'età utilizzati, ai dati trattati e alle finalità di tale trattamento. Le spiegazioni devono essere semplici, comprensibili e accessibili sia agli adulti che ai minori. *Formazione e informazione*: È fondamentale educare e sensibilizzare i minori, i genitori e il personale scolastico e giovanile sulle pratiche di sicurezza informatica e sui rischi legati all'uso di Internet. *Gestione dei reclami*: I fornitori dei servizi di verifica dell'età devono garantire un canale dedicato alla gestione rapida dei reclami in caso di errori nel processo di determinazione dell'età.

52. Cfr. schema di Regolamento AGCOM in cui si legge: «Ritenuto 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; Ritenuto, ad ogni buon fine che, alla luce del contesto normativo di riferimento prima richiamato e alle risultanze della consultazione medesima, le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti che con la presente delibera si approvano in attuazione del citato decreto-legge (come convertito in legge) 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».

Fermo restando l'approccio per principi e requisiti generali che lasci gli operatori liberi di scegliere, al fine di garantire il requisito della riservatezza "rafforzata", le specifiche dell'Autorità prevedono un sistema di verifica dell'età che utilizzi il modello del "doppio anonimato", in cui non si deve permettere ai fornitori di verifica dell'età di conoscere il servizio per il quale viene eseguita la verifica, di sapere se due verifiche provengono dalla stessa fonte o se un utente ha già utilizzato il sistema di verifica. Tale modello è quello scelto anche dalla Francia e che si rinviene tra le citate specifiche tecniche approvate dall'ARCOM.

In funzione del requisito appena ricordato, il sistema proposto dall'Autorità prevede l'intervento, per la fornitura della prova della maggiore età, di soggetti terzi indipendenti certificati, attraverso un processo di verifica dell'età che prevede due passaggi logicamente separati: identificazione e autenticazione della persona identificata, per ciascuna sessione di utilizzo del servizio regolamentato (cioè, la fornitura di contenuti pornografici tramite sito o piattaforma web)⁵³.

Ciò ha portato all'esclusione espressa di SPID, che, almeno nella sua conformazione attuale, non garantisce il doppio anonimato.

Nonostante, infatti, l'AGCOM all'interno del documento valorizzi il fatto che, come si è esposto,

i gestori dell'identità digitale sono soggetti terzi essi stessi (sia nei riguardi del soggetto regolamentato, sia rispetto a "enti statali" e gestori di "banche dati pubbliche") e in possesso di determinati requisiti soggettivi e oggettivi stabiliti dalla normativa di settore, selezionati sulla base di specifiche procedure di qualificazione e sottoposti a vigilanza da parte dell'Agenzia per l'Italia Digitale, si legge che «il sistema SPID, ad esempio, non risulta, ai fini dell'attuazione delle disposizioni di cui all'art.13-bis della legge 13 novembre 2023, n. 123, pienamente conforme alle specifiche tecniche AGCOM di seguito indicate (essenzialmente nella parte in cui è prescritto il c.d. doppio anonimato), nel momento in cui si trasferisce all'Identity Provider la richiesta di autenticazione del Service Provider, che contiene il nome a dominio del sito visitato. Infatti, tale sistema di autenticazione SPID consente all'Identity Provider di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'Identity Provider»⁵⁴.

Di particolare interesse, ai fini del presente contributo, è anche il passaggio dello schema di regolamento sui portafogli digitali. Infatti, si fa espresso riferimento all'identità digitale europea, ricordando che le piattaforme online di dimensioni molto grandi, come definite dal DSA (*Digital Services*

53. Il sistema è diverso a seconda che si parli di sistemi di verifica dell'età non basati su applicativi installati nel terminale utente o di sistemi basati sull'uso di applicativi installati sul dispositivo. Nel primo caso, il processo di verifica dell'età deve essere diviso in tre fasi distinte: 1. Emissione della prova dell'età: La prima fase consiste nell'ottenere una "prova dell'età" attraverso un processo di identificazione gestito da enti indipendenti dal fornitore di contenuti. Questo processo può avvenire, ad esempio, tramite l'accesso a un sito web utilizzando un browser. Gli enti che rilasciano questa prova possono essere fornitori specializzati nella gestione dell'identità digitale o organizzazioni che hanno già verificato l'identità dell'utente in altri contesti. Questi soggetti, che emettono la prova dell'età, non sono a conoscenza del fine per cui l'utente intende utilizzarla. Inoltre, devono essere certificati da un'Autorità competente, che garantisce l'affidabilità del sistema di identificazione adottato. 2. Consegna della prova all'utente: Nella seconda fase, la prova dell'età viene comunicata unicamente all'utente, che avrà la responsabilità di presentarla al sito o alla piattaforma che intende visitare. L'utente può ottenere la prova scaricandola direttamente dal sito dell'ente certificatore e successivamente inviarla autonomamente, attraverso il web, alla piattaforma che richiede la verifica dell'età. 3. Verifica della prova da parte della piattaforma: Infine, la piattaforma o il sito visitato dall'utente esamina la prova dell'età ricevuta e determina se concedere o meno l'accesso al contenuto richiesto. Questa fase rappresenta l'autenticazione dell'età dell'utente, che viene eseguita sulla base della prova fornita. Nel caso, invece, di sistemi di *age assurance* basati sull'uso di applicativi installati sul dispositivo, il soggetto terzo dovrà mettere a disposizione dell'utente una APP per la certificazione e la generazione della "prova dell'età", al fine di consentire all'utente di effettuare l'autenticazione e fornire la prova dell'età al sito web o piattaforma visitata, direttamente utilizzando l'APP installata sul proprio dispositivo e il servizio presente nella piattaforma/sito web deputato a tale scopo.

54. Cfr. all. B al regolamento sezione I.8 "Osservazioni sull'uso di sistemi pubblici".

Act), che impongono agli utenti di autenticarsi per accedere ai servizi online, dovranno accettare anche l'uso dei portafogli europei di identità digitale, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione, come la prova dell'età.

6. Prime conclusioni

In conclusione, si può affermare che SPID nasce come sistema per l'accesso sicuro ai servizi amministrativi e pubblici, nell'ambito dei quali l'identificazione dell'utente è un requisito essenziale. Proprio perché concepito per identificare in modo certo e univoco i cittadini, tale strumento non è in grado di soddisfare le esigenze di anonimato richieste in altri contesti, come l'accesso a contenuti online in cui l'età deve essere verificata senza necessariamente rivelare l'identità dell'utente.

In questo senso, l'identità digitale diventa terreno per riflessioni più ampie relative al bilanciamento di diversi interessi.

Nel contesto descritto, il minore, che gode già di una protezione specifica per via del suo *status*, assume anche i ruoli di "utente", "interessato" e "consumatore" rispetto ai servizi digitali, nonché di "utilizzatore", se questi ultimi sono anche basati su sistemi di intelligenza artificiale. Questa nuova realtà introduce ulteriori rischi e nuove necessità giuridiche in relazione alla tutela dell'identità digitale dei minori.

A livello nazionale e sovranazionale, si assiste, in effetti, a un aumento delle autorità responsabili della protezione dei dati personali, dell'identità digitale e della tutela dei minori nel contesto virtuale. La creazione di nuove figure regolatorie e il moltiplicarsi delle normative possono sembrare, in apparenza, un segnale positivo, anche alla luce della collaborazione interistituzionale che si è manifestata nella realizzazione di tavoli tecnici, protocolli d'intesa e linee guida congiunte.

Tuttavia, sebbene virtuoso, l'interessamento di più autorità potrebbe risultare inefficace nel garantire una protezione coerente e unitaria: l'eccessiva frammentazione rischia, infatti, di generare confusione sia tra i destinatari delle norme (minori, famiglie e imprese), sia tra le stesse istituzioni coinvolte.

Un esempio di questa complessità riguarda l'obbligo di trasparenza di cui, come si è visto, parla

anche il summenzionato schema di regolamento imposto agli operatori per i meccanismi di verifica dell'età, aggiungendosi a quello previsto dalle normative in materia di protezione dei consumatori e degli interessati per ciò che riguarda il trattamento dei loro dati personali. Imporre obblighi di trasparenza, come dimostrato in passato dalla normativa in materia di *data protection*, non garantisce di per sé una maggiore consapevolezza da parte degli utenti: nonostante lo sforzo del GDPR per rafforzare la trasparenza, spesso, le informative privacy, pur essendo dettagliate e obbligatorie, risultano di difficile comprensione, soprattutto per i minori e le loro famiglie. Questa complessità porta frequentemente gli utenti ad accettare termini e condizioni e *privacy policy* senza una piena consapevolezza rispetto alle conseguenze delle proprie scelte.

La trasparenza, dunque, rimane un principio cardine ma con la consapevolezza che da sola non è sufficiente a garantire una comprensione più profonda. Occorre promuovere iniziative di formazione e sensibilizzazione per sviluppare una cultura digitale solida e radicata. In questo senso, è essenziale un intervento non solo normativo, ma anche educativo e culturale, mirato a una formazione capillare rivolta a minori, famiglie e istituzioni scolastiche. L'alfabetizzazione digitale è infatti un fattore cruciale per promuovere una cultura della consapevolezza e della responsabilità nel mondo digitale. Scuole, genitori e tutori devono essere preparati a guidare i minori verso un utilizzo consapevole delle tecnologie e delle piattaforme online. La crescita equilibrata dell'identità digitale richiede un approccio integrato, probabilmente più complesso di quello attualmente adottato a livello nazionale.

A tale proposito, l'approccio repressivo e settoriale scelto dal Governo italiano rischia di non affrontare efficacemente i pericoli reali per i minori. Il Legislatore, o il Governo in sua vece, dovrebbe evitare interventi mossi dalla contingenza (come nel caso del d.l. "Caivano") e settoriali e adottare piuttosto una visione globale e integrata dei rischi digitali, ponendo attenzione particolare a tutti i fenomeni e gli ambiti (si pensi al gioco d'azzardo), che rappresentano effettivamente una minaccia per i minori. Anche dal confronto con l'approccio francese emerge che, sebbene in entrambe le esperienze ci si concentri a livello normativo esclusivamente sui contenuti pornografici, la scelta francese

si fonda sull'analisi di dati⁵⁵ ed è assunta tramite uno atto normativo ordinario e non eccezionale come è (o almeno dovrebbe essere), invece, la decretazione d'urgenza in Italia.

Non è un caso che l'AGCOM abbia altamente raccomandato le modalità tecniche prescelte nell'ambito del provvedimento adottato dalla stessa anche 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.

Non si tratta solo di un tema di opportunità ma anche di legittimità. Solo nei prossimi mesi sarà possibile testare la tenuta del sistema delle fonti approntato dall'ordinamento italiano sul tema. Del resto, l'art. 13-*bis* del citato "Decreto Caivano" forse

costituiva regola tecnica e non è stato notificato alla Commissione europea, con la conseguenza che la stessa delega ad AGCOM per adottare il regolamento sarebbe inficiata. Qualche dubbio sorge anche con riferimento alla compatibilità del 13-*bis* con il principio del "country-of-origin", pilastro della Direttiva e-Commerce.

Sarà fondamentale dunque valutare come si evolveranno le reazioni istituzionali e giudiziarie. Da un lato, i giudici nazionali potrebbero essere chiamati a pronunciarsi sulla conformità della norma alle disposizioni europee, dall'altro, la Commissione europea potrebbe aprire una procedura di infrazione qualora ritenesse che il "Decreto Caivano" violi i principi e le regole del mercato unico digitale.

Riferimenti bibliografici

- G. ALPA (2021), *Il diritto di essere se stessi*, La nave di Teseo, 2021
- M. ARE (1965), *Interesse alla qualificazione e tutela della personalità*, in "Rivista del diritto commerciale", 1965, n. 1
- T. ASCARELLI (1957), *Teoria della concorrenza e dei beni immateriali*, Giuffrè, 1957
- C. BASSU (2021), *Il diritto all'identità anagrafica. Il cognome materno tra personalità individuale e principio di eguaglianza*, Editoriale Scientifica, 2021
- E. BATTELLI (a cura di) (2021), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Giappichelli, 2021
- E. BELISARIO, F. RICCIULLI, S. PAGNOTTA (2020), *Amministrazione digitale, guida ragionata agli switch off*, Maggioli, 2020
- A. DE CUPIS (1949), *Il diritto all'identità personale*, Giuffrè, 1949
- D. DI SABATO (2011), *Il contratto del minore tra incapacità di contrarre e capacità di consumare*, in "Rivista di diritto dell'impresa", 2011, n. 1
- G. FINOCCHIARO (2010), (voce) *Identità personale (diritto alla)*, in "Digesto Discipline Privatistiche - Sezione Civile", V agg., Utet Giuridica, 2010
- L.M. FRIEDMAN (2002), *La società orizzontale*, il Mulino, 2002
- P. GLEASON (1983), *Identifying Identity. A Semantic History*, in "The Journal of American History", vol. 69, 1983, n. 4
- K. HETERINGTON (1998), *Expression of identity. Space, Performance, Politics*, SAGE Publications, 1998
- A. IANNUZZI, F. LAVIOLA (2023), *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in "Diritto costituzionale", 2023, n. 1

55. Nel citato provvedimento dell'ARCOM si fa riferimento a ricerche che dimostrano che «2,3 milioni di minori visitano siti pornografici ogni mese» e che «la percentuale di minori che visitano siti "per adulti" è aumentata di 9 punti in 5 anni, passando dal 19% alla fine del 2017 al 28% alla fine del 2022».

- M. LUCIANI (2018), *Quale identità?*, in A. Somma, A. Fusaro, G. Conte, V. Zeno-Zencovich (a cura di), "Dialoghi con Guido Alpa", Roma Tre-Press, 2018
- G. MANCA (a cura di) (2024), *Il regolamento eIDAS n. 2024/1183*, in "Rivista elettronica di Diritto, Economia, Management", n. spec., 2024, n. 4
- A. MORELLI (2019), *Persona e identità personale*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 2
- V. NATALE (2024), *Tutela dei minori online: possibili soluzioni per un'accurata verifica dell'età*, in "Agenda Digitale.eu", 6 giugno 2024
- M. OROFINO (2022), *La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065*, in "MediaLaws", 2022, n. 3
- G. PINO (2010), *Identità personale*, in S. Castignone, L. Lombardi Vallauri (a cura di), "Trattato di biodiritto", Giuffrè, 2010
- G. PINO (2003), *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, il Mulino, 2003
- E.C. RAFFIOTTA (2010), *Appunti in materia di diritto all'identità personale*, in "Forum di Quaderni Costituzionali", 26 gennaio 2010
- A. RANDAZZO (2021), *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in "dirittifondamentali.it", 2021, n. 3
- G. RESTA (2007), *Identità personale e identità digitale*, in "Il Diritto dell'informazione e dell'informatica", 2007, n. 3
- M. RICCA (2008), *Oltre Babele: codici per una democrazia interculturale*, edizioni Dedalo, 2008
- F. RICCIULLI (2024), *I diritti digitali: verso un'identità unica europea*, in "Diritto Pubblico Europeo – Rassegna Online", 2024, n. 1
- P. STANZIONE (2014), *I contratti del minore*, in "Europa e diritto privato", 2014, n. 4
- P. STANZIONE, G. SCIANCALEPORE (2006), *Minori e diritti fondamentali*, Giuffrè, 2006
- L. TRUCCO (2004), *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Giappichelli, 2004