



DOTTORATO DI RICERCA IN SCIENZE POLITICHE
CURRICULUM GOVERNO E ISTITUZIONI

XXXVIII CICLO

IDENTITÀ DIGITALE E COSTITUZIONE

Coordinatore: Prof. Giorgio Caravale

Tutor: Prof. Antonio Iannuzzi

Candidata: Francesca Ricciulli

INDICE

Note metodologiche e piano dell'indagine

CAPITOLO I

L'identità personale nella dimensione costituzionale

1. Le nozioni di “identità” e “identità personale”.	1
2. L'evoluzione del concetto di “identità personale” nell'ordinamento giuridico.	4
2.1. Gli orientamenti della dottrina originaria.	7
2.2. Le prime elaborazioni giurisprudenziali.	9
3. L'“identità personale” nel diritto costituzionale: la qualificazione dei “nuovi diritti” fondamentali.	13
3.1. La definizione dell'“identità personale” nella giurisprudenza costituzionale.	18
3.2. Il contributo della Corte di Cassazione nell'interpretazione costituzionale.	21
4. Gli sviluppi successivi della giurisprudenza costituzionale e i corollari del diritto all'identità personale.	24
4.1. Il diritto al nome quale manifestazione dell'identità personale.	25
4.2. Il diritto al nome quale espressione dell'ascendenza familiare.	28
4.3. Il diritto alla “verità biologica” nella costruzione della identità individuale.	29
4.4. Il diritto all'identità sessuale e il diritto all'identità di genere.	32
4.5. L'identità personale nel dibattito sul fine vita.	36
4.6. La protezione dei dati personali e il diritto all'oblio.	39
5. Focus: l'identità anagrafica tra tradizione ed evoluzione.	47
6. Prime conclusioni sull'identità personale.	52

CAPITOLO II

Il diritto all'identità digitale: profili nazionali e prospettive europee

1. Introduzione: l'identità digitale tra rappresentazione soggettiva e funzione identificativa.	56
2. L'identità digitale come diritto fondamentale.	61
3. La disciplina dei diritti digitali nella normativa di rango primario e prime riflessioni sulle tecniche di regolazione.	67
3.1. Il Codice dell'amministrazione digitale e la Carta della cittadinanza digitale.	71
3.2. Il diritto all'identità digitale per l'accesso ai servizi.	75
3.3. Il Sistema pubblico di identità digitale (SPID), la Carta di identità elettronica (CIE) e la Carta nazionale dei servizi (CNS).	77
3.4. Il punto di accesso telematico e l'applicazione “IO”.	84
3.5. Il diritto a servizi digitali semplici, sicuri e integrati.	86

3.6. L'Anagrafe nazionale della popolazione residente (ANPR) come piattaforma che attesta attributi.	87
3.7. Gli strumenti di garanzia e tutela dei diritti digitali.	91
4. La dimensione sovranazionale del diritto all'identità digitale nella sua funzione identificativa.	94
4.1. Il Regolamento (UE) 910/2014 (eIDAS).	96
4.2. Il Regolamento (UE) 2024/1183 (eIDAS2) e la costruzione dell'identità digitale europea.	99
4.3. L'European Digital Identity Wallet (EUDI Wallet).	100
5. Il portafoglio italiano (IT Wallet) e i portafogli digitali sviluppati negli altri Stati membri: una prospettiva comparatistica.	106
6. Prime conclusioni su stato dell'arte e prospettive dell'identità digitale nella sua funzione identificativa.	110

CAPITOLO III

L'identità e l'identificazione del minore nella dimensione digitale

1. Introduzione: l'identità personale e digitale del minore.	115
2. La tutela giuridica dei minori nei confronti dei mass media.	122
3. Minori, internet e piattaforme: le difficoltà dei legislatori nel regolare il rapporto tra minori e tecnologie digitali.	127
4. La protezione dei dati personali dei minori nell'ambiente digitale.	131
5. La verifica dell'età come strumento di protezione: una prospettiva transnazionale e interdisciplinare.	138
5.1. La disciplina sovranazionale in tema di verifica dell'età: la tutela dei minori nel Digital Services Act.	140
5.2. L'attuazione dell'art. 28, par. 4, DSA: le linee guida e il prototipo per la verifica dell'età della Commissione europea.	146
5.3. Il quadro normativo nazionale in tema di verifica dell'età. SPID per i minori: le Linee Guida dell'Agenzia per l'Italia digitale.	150
5.4. L'impatto del "Decreto Caivano".	152
5.5. I principi affermati dal Regolamento AGCOM in tema di verifica dell'età.	155
5.6. Le più recenti novità della normativa italiana in materia di verifica dell'età.	160
6. Il fenomeno dello "sharenting" e dei cc.dd. "baby influencers": identità personale e digitale eteroimposte e impatti sulla dignità del minore.	161
7. Tecniche di regolazione a confronto: l'esempio francese.	171
7.1. L'esperienza francese sull'obbligo di verifica dell'età.	172
7.2. L'approccio francese ai fenomeni dello "sharenting" e dei "baby influencer".	176
8. L'impatto dell'intelligenza artificiale sull'identità digitale del minore: stato dell'arte, profili di rischio e opportunità.	177
9. Prime considerazioni conclusive su tutela e prospettive dell'identità digitale del minore.	183
Considerazioni di sintesi della ricerca	192
Indice bibliografico	204

Note metodologiche e piano dell'indagine

Pare quantomai opportuno delineare il perimetro, la metodologia e la struttura della presente ricerca, offrendo una guida alla logica di sviluppo dei capitoli e alla coerenza interna dell'intero studio, anticipando una lettura organica del percorso argomentativo e provando ad illustrare come ciascun elemento contribuisca alla costruzione di un'analisi sistematica del tema oggetto di analisi.

La ricerca si colloca nel solco della riflessione costituzionalistica sui “nuovi diritti” e si propone di analizzare il processo di formazione, consolidamento e tutela dell'identità digitale, ponendo in primo piano la sua dimensione anagrafica e la sua funzione identificativa. L'identità digitale non rappresenta, infatti, un semplice strumento tecnico, bensì un vero e proprio pilastro dell'ordinamento digitale, essenziale per il riconoscimento della persona, per l'esercizio effettivo dei diritti digitali e per l'accesso ai servizi pubblici e privati, nonché, al tempo stesso, anche una misura di protezione della sfera personale nella dimensione digitale.

La trasformazione digitale, lungi dal modificare unicamente le modalità di esercizio dei diritti, comporta una ridefinizione profonda delle categorie giuridiche tradizionali, imponendo una riflessione articolata sui presupposti concettuali e sugli strumenti attraverso cui l'ordinamento tutela la persona nella sua dimensione individuale, relazionale e sociale.

In tale contesto, l'analisi assume una prospettiva costituzionalistica e sistematica, che integra lo studio dei diritti fondamentali con l'esame dei processi di adattamento dell'ordinamento alle rapide trasformazioni tecnologiche e sociali. La giurisprudenza costituzionale e di legittimità, in dialogo costante con l'ordinamento europeo, si configura come uno strumento imprescindibile per la costruzione di nuovi diritti e per la definizione di modelli di tutela coerenti con l'ambiente digitale, permettendo di leggere criticamente i principi costituzionali alla luce delle sfide poste dalla digitalizzazione.

Definendo più nel dettaglio il perimetro dell'indagine, la ricerca si concentra sulla funzione strutturale dell'identità digitale come strumento di interazione tra cittadini e istituzioni, necessario per garantire la fruizione dei diritti digitali, l'accesso ai servizi e la piena espressione della cittadinanza digitale. In questa prospettiva, l'analisi approfondisce la progressiva evoluzione dell'identità, dalla

dimensione analogica a quella digitale, con particolare attenzione agli strumenti e ai sistemi che ne consentono l'attribuzione, la verifica e la garanzia. Particolare rilievo è riservato all'identità digitale dei minori, considerata un caso paradigmatico per valutare le tensioni tra la tutela dei soggetti vulnerabili, la responsabilità delle piattaforme digitali e la libertà di iniziativa economica, nonché l'efficacia delle tecniche di regolazione a livello nazionale e sovranazionale.

Dal punto di vista metodologico, la ricerca adotta un approccio dogmatico, sistematico e comparatistico, articolato su più livelli di indagine. Il primo livello concerne l'analisi del sistema delle fonti vigenti, comprendente fonti costituzionali, primarie e secondarie, fonti europee e strumenti di soft law di rilevante incidenza. Il secondo livello si concentra sull'analisi della letteratura giuridica che si è occupata del tema in oggetto, privilegiando gli studi che trattano l'evoluzione del concetto di identità personale e digitale, la sua funzione identificativa e i correlati diritti fondamentali. Il terzo livello esamina la giurisprudenza costituzionale e di legittimità, integrata dai provvedimenti e dalle decisioni delle Autorità amministrative indipendenti competenti, al fine di cogliere le interpretazioni dei principi previsti dalla normativa e applicati all'identità digitale. Il quarto livello prevede un'analisi comparata dei modelli regolatori di altri ordinamenti, finalizzata ad esaminare le soluzioni adottate in altri ordinamenti per verificare potenzialità e criticità esportabili nel nostro sistema giuridico.

I diritti digitali e le tecniche di regolazione costituiscono i temi centrali della ricerca e le riflessioni sugli stessi il minimo comune denominatore dell'intera trattazione.

Lo studio si articola in tre capitoli, ciascuno concepito come unità analitica autonoma ma inserita in un disegno complessivo coerente, secondo il filo conduttore della traslazione dell'identità dalla dimensione analogica a quella digitale, con la funzione identificativa quale presupposto indispensabile per l'esercizio di ulteriori diritti.

Il primo capitolo si concentra sulle nozioni di identità e identità personale, ricostruendo le origini e l'evoluzione del concetto nell'ordinamento giuridico. In una prospettiva storico-dottrinale, vengono esaminati gli orientamenti della dottrina originaria e le prime elaborazioni giurisprudenziali che hanno contribuito a definire i contorni del diritto all'identità personale. La ricerca prosegue con l'analisi dell'identità personale nel diritto costituzionale, attraverso lo studio della

qualificazione dei nuovi diritti fondamentali e della giurisprudenza della Corte costituzionale, integrata dal contributo della Corte di cassazione nell'interpretazione costituzionale. Particolare attenzione è riservata ai corollari del diritto all'identità personale, quali il diritto al nome, sia nella sua dimensione individuale sia come espressione dell'ascendenza familiare, il diritto alla verità biologica, il diritto all'identità sessuale e di genere, nonché i profili legati al fine vita. La trattazione affronta anche la protezione dei dati personali e il diritto all'oblio, evidenziando come tali diritti, anche alla luce della loro evoluzione, rafforzino l'identità individuale nella sua dimensione pubblica e privata. Il capitolo si chiude con un approfondimento sull'identità anagrafica, esaminata nella tensione tra tradizione e innovazione, con l'obiettivo di delineare le basi concettuali necessarie per la successiva trasposizione dell'identità nella dimensione digitale.

Il secondo capitolo, entrando nel pieno dell'analisi, sposta l'attenzione sull'identità digitale, intesa come diritto fondamentale con funzione identificativa prodromico e presupposto per l'esercizio di ulteriori diritti. L'analisi si apre con una riflessione introduttiva sull'identità digitale tra rappresentazione soggettiva e funzione identificativa, per poi approfondire la disciplina dei diritti digitali nella normativa primaria italiana ed europea. In questo contesto, vengono esaminati sia i presidi normativi interni, in particolare quelli previsti dal Codice dell'Amministrazione Digitale che gli strumenti tecnici previsti dall'ordinamento come i sistemi di identificazione SPID, CIE e CNS e le applicazioni di accesso ai servizi digitali, come il portale "Io". Particolare attenzione è dedicata al diritto a servizi digitali semplici, sicuri e integrati, nonché all'Anagrafe Nazionale della Popolazione Residente (ANPR), in quanto piattaforma centrale per l'attestazione degli attributi identificativi. Sul piano sovranazionale, il capitolo analizza il ruolo della normativa europea sul tema, l'implementazione dell'identità unica europea e del relativo portafoglio, l'European Digital Identity Wallet (EUDI Wallet), nonché, in una prospettiva comparatistica, il portafoglio italiano (IT Wallet) sviluppato in attuazione del quadro sovranazionale e gli analoghi strumenti sviluppati attualmente in altri Stati membri.

Il terzo capitolo approfondisce l'identità digitale dei minori, un tema particolarmente sensibile per la combinazione tra vulnerabilità dei soggetti, responsabilità delle piattaforme digitali e sempre maggiore necessità di tutela. In questo caso si è scelto di soffermarsi sia sulla dimensione sostanziale che su quella

anagrafica dell'identità, con particolare attenzione al tema particolarmente attuale degli strumenti di verifica dell'età. La trattazione prende avvio con un'introduzione alla dimensione personale e digitale del minore, per poi analizzare la protezione giuridica dei minori nei confronti dei mass media e il ruolo delle piattaforme digitali. Vengono esaminati in particolare gli strumenti di verifica dell'età a cui si stanno orientando i Legislatori sia sul piano nazionale sia sovranazionale, attraverso il quadro normativo del Digital Services Act, le linee guida della Commissione Europea e l'attuazione delle disposizioni italiane, comprese le specifiche di SPID per i minori e il cosiddetto "Decreto Caivano". Il capitolo esplora anche fenomeni emergenti come lo sharenting e i baby influencer, valutandone l'impatto sulla costruzione dell'identità digitale dei minori e sul diritto alla riservatezza. Attenzione particolare è rivolta all'intelligenza artificiale, con l'analisi dei profili di rischio e delle opportunità per la tutela dei minori. Infine, viene condotta una riflessione comparatistica con l'esperienza francese, al fine di confrontare tecniche di regolazione diverse e individuare modelli più efficaci di protezione dei soggetti vulnerabili.

La ricerca intende offrire un contributo al dibattito sui diritti digitali, evidenziando come la costruzione dell'identità digitale non sia un mero strumento tecnico, ma un processo profondamente normativo e costituzionalmente orientato, capace di ridefinire i confini tra persona, tecnologia e istituzioni.

CAPITOLO I

L'identità personale nella dimensione costituzionale

SOMMARIO: 1. Le nozioni di “identità” e “identità personale” - 2. L'evoluzione del concetto di “identità personale” nell'ordinamento giuridico - 2.1. Gli orientamenti della dottrina originaria - 2.2. Le prime elaborazioni giurisprudenziali - 3. L'“identità personale” nel diritto costituzionale: la qualificazione dei nuovi diritti fondamentali - 3.1. La definizione dell'“identità personale” nella giurisprudenza costituzionale - 3.2. Il contributo della Corte di Cassazione nell'interpretazione costituzionale - 4. Gli sviluppi successivi della giurisprudenza costituzionale e i corollari del diritto all'identità personale - 4.1. Il diritto al nome quale manifestazione dell'identità personale - 4.2. Il diritto al nome quale espressione dell'ascendenza familiare - 4.3. Il diritto alla verità biologica nella costruzione dell'identità individuale - 4.4. Il diritto all'identità sessuale e il diritto all'identità di genere - 4.5. L'identità personale nel dibattito sul fine vita - 4.6. La protezione dei dati personali e il diritto all'oblio - 5. Focus: l'identità anagrafica tra tradizione ed evoluzione - 6. Prime conclusioni sull'identità personale.

1. Le nozioni di “identità” e “identità personale”.

Un'analisi sull'identità personale e sulla sua evoluzione risulta fondamentale e prodromica per indagare il tema dell'identità digitale sul quale si appunta la presente ricerca.

Il significato della parola “identità” si è evoluto in modo (si direbbe) sorprendente con il passare degli anni, divenendo sempre più multiforme e, a tratti, inafferrabile¹.

Ciò, anzitutto, per quanto riguarda il concetto stesso di “identità” - individuale, di gruppo, collettiva, sociale o nazionale - e le sue modalità di formazione².

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 ritiene di essere che come vuole essere rappresentata, oltre a come viene percepita e rappresentata dagli altri³.

¹ Per una ricostruzione storica approfondita cfr. G. Alpa, *Il diritto di essere sé stessi*, Milano, 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”. Cfr., altresì, P. Gleason, *Identifying Identity. A Semantic History*, in *The Journal of American History*, n. 4, 1983; F. Remotti, *L'ossessione identitaria*, Roma-Bari, 2017, p. XII.

² Cfr., tra gli altri, K. Heterington, *Expression of identity. Space, Performance, Politics*, 1998.

³ M. Ricca, *Oltre Babele: codici per una democrazia interculturale*, Bari, 2008.

Come si approfondirà nel prosieguo, peraltro, il rapporto di una persona con sé stessa e con l'altro è uno degli aspetti fondamentali quando si affronta questo tema⁴. È vero, infatti, che l'intera esistenza è costruzione della propria identità, non necessariamente tramite il confronto con ciò che ci circonda⁵. Tuttavia, la propria costruzione personale è destinata ad essere messa in discussione dall'interazione con gli altri. Occorre, in effetti, il riconoscimento altrui affinché la propria identità possa trovare tutela ed esplicarsi⁶.

Tutto ciò, come spiega Jane Austen, passa anche per l'uso del linguaggio. È celebre la distinzione tracciata dall'autrice tra "orgoglio" e "vanità", intesa come differenza tra l'opinione che abbiamo di noi stessi rispetto a quello che vorremmo che gli altri pensassero di noi⁷.

Da qui la dimensione psicologica, filosofica⁸, politica, sociale e culturale in cui si dirama l'identità⁹. Senza contare che, secondo alcuni, sarebbe la stessa costruzione della identità personale ad essere influenzata dalla tradizione, dalla cultura, dalla società e, in generale, dai valori della comunità di riferimento¹⁰. In questo senso, l'identità personale non sarebbe qualcosa che si ha *ab origine* quanto piuttosto un costrutto sociale e culturale, che, in modo consapevole o meno, si sceglie, aderisce e costruisce tramite un "processo di identificazione"¹¹ (c.d. "antiessenzialismo"). La costruzione dell'identità individuale è stata rappresentata, in questo

⁴ Cfr., ancora, G. Alpa, *Il diritto di essere sé stessi*, cit., 12. Come ricorda l'Autore, identità significa da un lato unicità di essere umano, che, visto dall'esterno, è un essere irripetibile e diverso dagli altri e dall'altro ipseità, cioè il modo in cui la persona si percepisce e vuole apparire. Cfr. anche G. Pino, *L'identità personale*, in S. Rodotà, P. Zatti (diretto da), *Trattato di biodiritto*, Milano, 2010, 297 ss., il quale, in tema di identità, evidenzia che "ogni asserzione o rivendicazione formulata in termini di identità presuppone al contempo la sottolineatura di una differenza".

⁵ Sul tema cfr. V.E. Mounier, *Il personalismo*, Roma, 2004; nonché, Z. Bauman, *Intervista sull'identità*, Roma-Bari, 2003.

⁶ L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004.

⁷ J. Austen, *Pride and Prejudice*, Londra, 1813, afferma che "Vanità e orgoglio sono cose diverse, anche se spesso i due termini vengono usati quasi come sinonimi. Si può essere orgogliosi senza essere vanitosi. L'orgoglio si riferisce soprattutto all'opinione che abbiamo di noi; la vanità a quella che vorremmo che gli altri avessero di noi".

⁸ Si vedano i contributi raccolti in A.O. Rorty (ed.), *The Identities of Persons*, Berkeley, CA, University of California Press, 1976; nonché, R. Nozick, *Philosophical Explanations*, Cambridge, Belknap Press, 1981; Parfit, *Reasons and Persons*, Oxford, Oxford U.P., 1984; A.C. Varzi, *Parole, oggetti, eventi e altri argomenti di metafisica*, Roma, 2001.

⁹ V.D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, Parigi, 2000; L.L. Christians, *Dimensions philosophiques et religieuses des approches juridiques de l'identité*, in J. Pousson-Petit (ed.), *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002.

¹⁰ Cfr. G. Pino, *L'identità personale*, cit., 297.

¹¹ C.W. Appiah, *The Ethics of Identity*, Princeton University Press, NJ, 2005, spec. 66 ss. Ripreso anche da G. Pino, *L'identità personale*, cit., 298, in cui si legge che "Le caratteristiche costitutive (o almeno alcune di esse) dell'identità personale sono mutate da qualche modello più generale, offerto dall'ambiente sociale rilevante: quest'ultimo rende disponibili ad esempio una certa cultura, una certa religione (o più opzioni religiose), e attribuisce un certo significato ad altre caratteristiche dell'identità come il sesso, l'etnia, la razza, la lingua". La costruzione dell'identità individuale è così un processo di identificazione con qualcuno, o più, dei modelli o identità collettive disponibili nell'ambiente sociale"

senso, come un processo di identificazione con qualcuno, o più, dei modelli o identità collettive disponibili nell'ambiente sociale¹².

Si consideri, poi, che ciascun individuo non ha una sola identità definita e stabile ma, come è stato rilevato, in ciascuna persona convivono, al contempo, più identità¹³.

Giova precisare che il presente studio, approfondendo l'elaborazione giuridica effettuata a partire dal concetto di "identità", si concentra sull'identità della persona¹⁴, anche se molte delle riflessioni svolte valgono, e di fatto vengono estese nel linguaggio comune, anche agli altri esseri viventi o alle organizzazioni sociali.

Del resto, negli anni, come si vedrà, si è evoluta la stessa nozione di "persona".

Per quanto rileva ai fini della presente analisi, già alla fine degli anni Novanta, Stefano Rodotà evidenziava come il progresso tecnologico avesse ulteriormente complicato il dibattito sull'identità in ogni ambito del sapere. Tale evoluzione, infatti, aveva accentuato quella che egli definiva "*frammentazione della persona*", determinata dalla disseminazione e conservazione dei dati individuali in una molteplicità di spazi e sistemi¹⁵.

Secondo l'Autore, l'unitarietà del soggetto viene, di conseguenza, meno: non si forma solo un "doppio elettronico", ma una pluralità di "persone elettroniche", generate dal mercato in funzione dei diversi interessi che motivano la raccolta delle informazioni. L'individuo appare, dunque, "moltiplicato", e ciò dà origine a nuove questioni identitarie. Tali criticità, tuttavia, non dipendono solo dalla pluralità dei contesti informativi; esse emergono anche dalle possibilità che la rete offre a chiunque di celarsi dietro l'anonimato, adottare identità differenti, modificabili e interscambiabili. L'"Io frammentato", in questo senso, "esplode" nello spazio digitale. Ognuno può assumere molteplici configurazioni, divenendo metaforicamente "uno, nessuno e centomila".

Come è stato osservato, il sé finisce per riflettersi nelle molteplici "finestre" che si aprono sullo schermo del computer, divenute a loro volta una potente metafora per concepire l'identità come un sistema plurimo e distribuito.

¹² G. Pino, *Identità personale*, cit., 298.

¹³ G. Pino, *Identità personale* cit. Si veda, altresì, L.M. Friedman, *La società orizzontale*, Bologna, 2002.

¹⁴ Si intende "persona" nel senso ampio previsto dalla Costituzione italiana e da molte altre Leggi fondamentali del dopoguerra. In dottrina cfr. V.E. Mounier, *Il personalismo* cit.; J. Maritain, *Cristianesimo e democrazia* (1943), trad. it., Firenze, 2007, 62 ss.; Id., *L'uomo e lo Stato* (1951), trad. it., Genova-Milano, 2003; G. D'Amico, *Stato e persona. Autonomia individuale e comunità politica*, in F. Cortese, C. Caruso, S. Rossi (a cura di), *Immaginare la Repubblica. Mito e attualità dell'Assemblea costituente*, Milano, 2018.

¹⁵ S. Rodotà, *Prefazione alla Relazione annuale dell'Autorità Garante per la protezione dei dati personali*, 1997. Sullo stesso tema v. anche S. Rodotà, *Tecnologia e diritti*, Bologna, 1995; Id., *Trasformazioni del corpo*, in *Pol. dir.*, n. 1/2006, 3 ss.

Tali riflessioni, formulate negli ultimi decenni del XX secolo, invitano ad estendere ulteriormente l'analisi nel contesto attuale, segnato dall'avanzare dell'intelligenza artificiale e dal crescente dibattito sulla possibilità che le macchine acquisiscano tratti sempre più simili a quelli umani, sino a poterne in parte sostituire le funzioni. Un simile scenario, oggi tutt'altro che fantasioso, era stato già intuito secoli fa da Giacomo Leopardi, il quale osservava come la sua epoca potesse essere definita «l'età delle macchine». Non solo gli uomini vivevano «più meccanicamente» che in passato, ma era anche evidente il continuo proliferare di nuovi dispositivi, ideati e perfezionati quotidianamente per i più diversi ambiti dell'agire umano. Al punto che — scriveva Leopardi — non sono più gli uomini, ma le macchine a “*trattare le cose umane e fare le opere della vita*”¹⁶.

2. L'evoluzione del concetto di “identità personale” nell'ordinamento giuridico.

Storicamente la locuzione “identità personale” ha assunto diversi significati nel diritto¹⁷ e, come anticipato, è destinata - nel futuro prossimo - ad assumerne molti altri. Forse per questo, proprio Stefano Rodotà, diceva che “*profondissimo è divenuto il pozzo dell'identità, e su questo troppi giuristi evitano di sporgersi*”¹⁸.

Come affermato da Guido Alpa, del resto, “*nell'immaginario dei giuristi l'identità attraversa i secoli in un continuum di regole, teorie e concetti*” ed è “*un laboratorio*”, dato che “*non è una fotografia né un punto di arrivo*” ma uno strumento “*che di volta in volta può assolvere ad una funzione liberatoria o persecutoria*”.

In effetti, solo dopo la Seconda guerra mondiale, l'identità “*è diventata un metro di esaltazione della persona*”, mentre prima tendeva a “*soffocarla*”, essendo ragione di categorizzazione e potenziale discriminazione in caso di appartenenza ad un determinato *status*.

Ciò premesso, si può in generale affermare che, allo stato, all'interno del nostro ordinamento, il diritto garantisce i diritti inviolabili delle persone e riconosce la loro identità. L'identità, in questo senso, è oggi rappresentata da alcuni come una “*cornucopia in cui si tutelano la dignità, il credo religioso, le opinioni politiche e*

¹⁶ G. Leopardi, *Proposta di Premi fatta all'Accademia dei Sillografi*, Roma-Bari, 1928, 28.

¹⁷ V. Zeno-Zencovich, *Identità personale* voce, in *Dig. disc. priv.*, vol. IX, Torino, 1993, 22 ss.; G. Finocchiaro, *Identità personale (diritto alla)* voce, in *Dig. disc. priv.*, V Agg., Torino, 2010, 721 ss.; G. Pino, *L'identità personale*, cit.; Id., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003; nonché, L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit.; E. Raffiotta, *Appunti in materia di diritto all'identità personale*, in *Forumcostituzionale.it*, 26 gennaio 2010. Cfr. altresì le riflessioni raccolte in C. Honorati (a cura di), *Diritto al nome e all'identità personale nell'ordinamento europeo*, Milano, 2010; nonché, A. Morelli, *Persona e identità personale*, in *BioLaw Journal*, n. 2/2019, 45 ss.

¹⁸ Cfr. S. Rodotà, *Il diritto di avere diritti*, Bari, 2015, *passim*.

sindacali, l'etnia, il sesso e l'orientamento sessuale, la lingua, la disabilità, le origini genetiche"¹⁹. Si tratta, come si vedrà, del concetto affermatosi anche a livello sovranazionale. La Corte di Strasburgo, infatti, ha stabilito da tempo che l'essenza stessa della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali²⁰ è il rispetto della dignità e della libertà umana. In particolare, in base all'articolo 8 della Convenzione, dove la nozione di autonomia personale è un principio importante alla base dell'interpretazione delle sue garanzie, viene data protezione alla sfera personale di ogni individuo, compreso "il diritto di stabilire i dettagli della propria identità come singoli esseri umani"²¹.

Va precisato, però, che, se si registra una generale stagione positiva in Europa, dove, a partire dal dopoguerra, si vive un'epoca che è stata definita "l'età dei diritti"²², in diverse parti del mondo, sono al momento in discussione i diritti fondamentali dell'essere umano nella sua dimensione individuale e collettiva. Ciò non solo nell'ambito di ordinamenti storicamente considerati più arretrati sul tema del riconoscimento dei diritti²³ ma anche nel mondo occidentale (dai più considerato "ospitale alla cultura dei diritti umani" e avanguardista sul tema²⁴), anche alla luce delle registrate ripetute violazioni del diritto internazionale, nato proprio a presidio del patrimonio irrettrattabile e basilare dei diritti.

In questo contesto risulta più che mai attuale la lettura integrata tra identità, dignità e libertà proposta da alcuni autori poiché, riprendendo la condivisibile espressione di Guido Alpa, "il livello di civiltà di una società è dato dalla misura con cui è in grado di assicurare a ciascuno il diritto di essere sé stessi".

Ebbene, all'interno del nostro ordinamento giuridico, hanno trovato garanzia esplicita già da tempi più risalenti gli elementi principali di individuazione della persona, quali il nome e l'immagine. L'identificazione della persona, infatti, presuppone sempre la sua individuazione²⁵.

Alla luce dell'evoluzione della società, però, l'identità personale non si limita all'esigenza di identificazione della persona. Ciò, come si approfondirà nel prosieguo, ha portato ben presto i giuristi a realizzare che la sua tutela non potesse essere circoscritta al nome, all'immagine e agli altri mezzi di individuazione²⁶.

Sul piano normativo, come rilevato da vari autori, nel testo della Costituzione si rinviene più volte il termine "persona" ma è del tutto assente qualsiasi riferimento

¹⁹ G. Alpa, *Il diritto di essere sé stessi*, cit., 15.

²⁰ La Convenzione è stata firmata a Roma il 4 novembre 1950 e ratificata dall'Italia con l. 4 agosto 1955, n. 848.

²¹ Corte EDU, *Christine Goodwin c. Regno Unito*, 11 luglio 2002.

²² N. Bobbio, *L'età dei diritti*, Torino, 1990.

²³ Sull'evoluzione dei diritti individuali in Cina cfr. K. Hsin-Chi, *Universality, Indivisibility and Interdependence of Human Rights: the case of China*, in *Pontifical Academy of Social Sciences*, acta 15, Vatican City 2010, 359 ss.

²⁴ M. Cartabia, *In tema di "nuovi" diritti*, in Aa.Vv., *Studi in onore di Franco Modugno*, Napoli, 2011.

²⁵ Cfr. E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit.

²⁶ Cfr. F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995.

al termine “identità” o alla stessa associata ad attributi come “individuale” o “personale”. 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’introdurvi riferimenti espliciti all’idea prima di tutto di un’identità collettiva, eccetto i richiami al concetto di “nazione”²⁷.

Nell’ambito della normativa di rango primario, invece, il concetto di identità personale si rinviene prima nella legge n. 675 del 1996²⁸ e, successivamente, nel d.lgs. n. 196 del 2003²⁹, successivamente modificato dal d.lgs. n. 101 del 2018, che ha adeguato la normativa nazionale alle disposizioni del Regolamento generale per la protezione dei dati personali n. 2016/679/UE (di seguito anche “RGPD o, in inglese, “GDPR”)³⁰. Si tratta di entrambi testi normativi relativi alla protezione dei dati personali e tale circostanza, come sarà approfondito nel prosieguo della presente trattazione, non sembra casuale.

Un riferimento al diritto all’identità personale si rinviene, poi, in un contesto completamente diverso, quello del d.lgs. 22 gennaio 2004, n. 42, recante “Codice dei beni culturali e del paesaggio”. In realtà, anche in questo caso, la finalità sottesa alla norma è la tutela dei dati personali³¹. Anche all’interno di questa disposizione, poi, si menziona l’“identità personale” ma non viene fornita alcuna definizione.

Si può concludere, dunque, che storicamente 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 tema. Per questo motivo, con riferimento all’identità personale, si è spesso parlato, oltre che, come

²⁷ A. Morelli, *Persona e identità personale*, cit., 46.

²⁸ All’art. 1 si legge(va) che “*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*”. Il richiamato articolo è stato successivamente abrogato ai sensi dell’art. 183, comma 1, lettera a), del Codice in materia dei dati personali.

²⁹ Cfr. art. 2 ove si prevede che “*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*”.

³⁰ Regolamento n. 2016/679/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

³¹ Cfr. art. 126, d.lgs. n. 42/2004, recante “*Protezione dei dati personali*”. La disposizione, in particolare, al comma 2, recita che “*Su richiesta del titolare medesimo, può essere disposto il blocco dei dati personali che non siano di rilevante interesse pubblico, qualora il loro trattamento comporti un concreto pericolo di lesione della dignità, della riservatezza o dell’identità personale dell’interessato*”.

si è visto, di “laboratorio”, anche di “diritto senza legge”³². A tale proposito, peraltro, la dottrina non ha mancato di considerare il colpevole ritardo del Legislatore, che è intervenuto con i già menzionati testi normativi a distanza di circa venti anni dalla prima comparsa del tema in giurisprudenza³³.

2.1. Gli orientamenti della dottrina originaria.

Come si approfondirà nel prosieguo, è proprio la dottrina a concentrarsi in un primo momento sull’analisi della duplice accezione in cui siamo abituati a pensare all’“identità”³⁴.

In particolare, il profilo che più si prenderà in considerazione nell’ambito della presente trattazione, in quanto strettamente legato anche al tema dell’identità digitale³⁵, è l’identità come mezzo che consente l’identificazione di un soggetto³⁶. Non a caso, in effetti, il termine “identità” viene utilizzato nel linguaggio comune anche per esprimere il rapporto di esatta uguaglianza o coincidenza tra due elementi. Da qui, poi, la denominazione di strumenti come il “documento di identità” o la “carta di identità”³⁷.

Questa nozione dell’identità personale è, a ben vedere, la più tradizionale, è stata definita dalla dottrina più recente “estrinseca”, “esteriore” o “anagrafica”³⁸, 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 consociati³⁹ e si rinviene anche in alcune codificazioni più risalenti⁴⁰.

³² Cfr. A. Morelli, *I diritti senza legge*, in *Consulta online*, n. 1/2015, 10 ss.; nonché, S. Fiaccavento, *Tutela della persona e «creazione giurisprudenziale» del diritto*, in *Giust. civ.*, n. 5/1992, 233 ss.

³³ G. Pino, *Il diritto all’identità personale Interpretazione costituzionale e creatività giurisprudenziale*, cit., 121, rileva, in proposito, il lasso di tempo che intercorre tra 1974 e il 1996.

³⁴ Per un approfondimento sul tema del diritto all’identità personale da un punto di vista storico e con riferimento ad entrambe le prospettive cfr. A. Randazzo, *Diritto all’identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *Dirittifondamentali.it*, n. 3/2021, 1 ss.; E.C. Raffiotta, *Appunti in materia di diritto all’identità personale*, cit.; G. Pino, *Identità personale*, cit.; G. Resta, *Identità personale e identità digitale*, in *Dir. informatica*, 2007, 511 ss.

³⁵ Cfr. *infra* cap. II.

³⁶ G. Finocchiaro, *Identità personale (diritto alla) voce*, cit. Sulla individuazione “inequivoca” della persona v. G. Resta, *Identità personale e identità digitale*, cit., 523.

³⁷ Cfr. G. Falco, *Identità personale voce*, in *Nuovo dig. it.*, Torino, 1938, 649 ss.

³⁸ G. Pino, *Identità personale*, cit., 301, evidenzia che 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, vale a dire ciò che può rendere quella persona facilmente identificabile da parte del pubblico potere. Sul tema cfr., altresì, M. Martoni, *Identità personale anagrafica (autorizzata) vs identità personale autorappresentativa (manifestata)*, in *Riv. trim. dir. proc. civ.*, n. 1/2020, 179 ss.

³⁹ Cfr. G. Resta, *Identità personale e identità digitale*, cit. Cfr., altresì, il più recente lavoro monografico di C. Bassu, *Il diritto all’identità anagrafica. Il cognome materno tra personalità individuale e principio di eguaglianza*, Napoli, 2021.

⁴⁰ Sull’identificazione da parte del notaio v., ad esempio, l’art. 49, l. 16 febbraio 1913, n. 89. In dottrina cfr. M.M. Virgilio, *Rassegna critica di lessico giuridico*, in *Ragion pratica*, 2015, 547

Anche con riferimento a questo profilo, risulta fondamentale ricordare quanto si diceva su un altro aspetto, che è stato più volte messo in luce dalla dottrina nell'approfondimento teorico della nozione di identità, ossia la sua "prospettiva relazionale"⁴¹. In effetti, con riferimento all'identità come diritto che consente l'identificazione tramite il complesso dei dati personali caratteristici e fondamentali che consentono l'individuazione di un soggetto, le riflessioni svolte su questo punto risultano assolutamente valide. Non si usa, del resto, identificarsi con le persone con cui si è in relazione. Occorre sempre un'alterità.

Quanto alla seconda e diversa nozione, definita da alcuni come "dimensione sostanziale"⁴², a partire dagli anni Cinquanta, si realizza che l'identità personale è "qualcosa di più e di diverso" perché, oltre a una funzione identificativa, è in gioco la rappresentazione della personalità individuale⁴³.

È in questa fase che viene teorizzato da alcuni autori⁴⁴ che l'identità personale è l'essere sé medesimo con i propri caratteri e le proprie azioni anche nell'opinione degli altri, cioè "socialmente". Di conseguenza, la persona ambisce a una proiezione sociale del proprio io personale corrispondente alla realtà dello stesso io, per risultare, in ambito sociale, per quella che è realmente.

In particolare, Adriano De Cupis afferma che "*all'apparenza di sé medesimo, alla proiezione sociale della propria identità corrisponde un cospicuo interesse. Trattasi dell'interesse della persona all'affermazione sociale della propria individualità. La persona aspira a risultare, nell'ambito sociale, per quella che è realmente colle proprie qualità e le proprie azioni*"; tale interesse, rivolto a una proiezione sociale del proprio io personale corrispondente alla realtà dello stesso io, può precisamente denominarsi interesse all'identità personale".

Tale proiezione sociale, però, come rilevato dall'Autore, è suscettibile di offesa esterna e dunque deve essere ricompresa nella tutela giuridica e può considerarsi un bene giuridico. La tutela giuridica, secondo De Cupis, corrisponde al "*rispetto della verità personale*"⁴⁵, al diritto alla "*concreta rappresentazione della personalità*", come diritto a non essere travisato né offuscato⁴⁶.

ss., 548; A. Intini, *La identificazione di persone. Lettura dei documenti – Controllo di autenticità – Procedure*, IV ed., Roma, 1996, 19.

⁴¹ Cfr. A. Randazzo, *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, cit., 374.

⁴² G. Pino, *Identità personale*, cit.

⁴³ Cfr. G. Bavetta, voce *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, Milano, 1970, 955 ss.

⁴⁴ A. De Cupis, *Il diritto all'identità personale*, Milano, 1949. Cfr., altresì, T. Ascarelli, *Teoria della concorrenza e dei beni immateriali*, Milano, 1957; M. Are, *Interesse alla qualificazione e tutela della personalità*, in *Riv. dir. comm.*, I, 1965, 81 ss.

⁴⁵ A. De Cupis, *I diritti della personalità*, in A. Cicu, F. Messineo (a cura di), *Trattato di diritto civile e commerciale*, vol. IV, tomo I, Milano, 1982, 32 ss.

⁴⁶ G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, cit., 299. Sul "travisamento" cfr., anche, A. De Cupis, *I diritti della personalità*, cit., 31, secondo il quale "i travisamenti possono riscontrarsi in ogni rappresentazione della persona non aderente alla verità della persona medesima o per la omissione di elementi essenziali (azioni,

In linea con questa ricostruzione, di fondamentale importanza è “*la tutela dei segni distintivi personali, tra cui principale è il nome*”, grazie alla quale la persona può essere “*rappresentata e individuata in sé medesima e nelle sue azioni, escludendo la confusione con altre persone e, quindi, l’attribuzione ad essa di qualità ed atti non suoi*”.

Ciò non vuol dire che l’identità personale sia da tutelare solo nel caso in cui i segni distintivi siano a rischio (es. nome e pseudonimo), ma anche a fronte di una cattiva rappresentazione (sia se migliorativa che peggiorativa) di quell’individuo, “non aderente alla verità della persona”⁴⁷.

2.2. Le prime elaborazioni giurisprudenziali.

In disparte i tentativi di definizione che si sono registrati sul piano dommatico, a partire dagli anni Settanta, si sviluppa una cospicua giurisprudenza⁴⁸ che, come rilevato da alcuni autori, non si sofferma ancora sul diritto all’identità personale come “diritto ad essere ciò che si è” quanto piuttosto sul “diritto ad essere rappresentati correttamente” o, in altre parole, “a non essere travisati”⁴⁹. Ciò, del resto, del tutto in linea con la nozione recepita nell’ambito delle citate codificazioni e con quella elaborata dalla dottrina appena richiamata.

Tale fenomeno risulta coerente con alcune esigenze che stavano sorgendo nell’ambito della società. Con l’evoluzione delle tecniche di diffusione delle immagini e del nome – attraverso la stampa o le affissioni pubblicitarie, nonché in seguito la radiotelevisione – era emerso, con sempre maggiore urgenza, in particolare, il bisogno di dare copertura a interessi che la normativa vigente non riusciva a tutelare⁵⁰.

A tale proposito, può essere interessante menzionare - in quanto estremamente rappresentativa - la prima e notissima pronuncia sul tema, la decisione della Pretura di Roma del 6 maggio 1974⁵¹.

caratteri) reali o per l’introduzione di elementi irreali. [...] In tutte queste ipotesi di rappresentazione infedele, non veritiera, è sacrificata l’individualità personale, è violata la verità personale: è sempre offeso un uguale bene, e si afferma, quindi, l’esigenza di una uguale reazione giuridica”.

⁴⁷ Cfr. A. De Cupis, *La verità nel diritto (Osservazioni in margine a un libro recente)*, in *Foro it.*, 1952, 223 ss.

⁴⁸ Si vedano, in particolare, le pronunce della Pretura di Roma del 6 maggio 1974; Pretura di Pontedera del 10 maggio 1974; Pretura di Torino del 30 maggio 1979; Pretura di Roma del 2 giugno 1980; Pretura di Verona del 21 dicembre 1982; nonché, Cass. civ., 22 giugno 1985, n. 3769. Per un approfondimento del formante giurisprudenziale cfr. L. La Battaglia, *La tutela del diritto all’identità personale: valori personalistici e circolazione dei dati nel bilanciamento fra diritti costituzionalmente rilevanti*, in G. Comandé (a cura di), *Diritto privato europeo e diritti fondamentali: saggi e ricerche*, Torino, 2004, p. 270 ss.

⁴⁹ G. Pino, *Il diritto all’identità personale Interpretazione costituzionale e creatività giurisprudenziale*, cit., parla in proposito di “*landmark decision*” sul diritto all’identità personale e di “*battesimo giurisprudenziale*” del diritto.

⁵⁰ E.C. Raffiotta, *Appunti in materia di diritto all’identità personale*, cit.

⁵¹ Cfr. Pretura di Roma del 6 maggio 1974, in *Giurisprudenza italiana*, 1975, p. 514 ss.

Il caso di specie riguardava un uomo e una donna, che lamentavano l'utilizzo, a loro insaputa e senza consenso, di un'immagine - che li ritraeva insieme e realizzata per diverse e non politiche finalità - per un manifesto di propaganda del Comitato nazionale per il referendum abrogativo sul divorzio, al fine di sostenere il voto a favore del referendum.

In quella occasione, il giudice, prima di tutto, riconosceva la tutela ai ricorrenti per l'utilizzo abusivo dell'immagine⁵².

Nell'ambito di tale decisione, poi, veniva riconosciuta la tutela ai ricorrenti anche per la lesione derivante dall'accostamento delle finalità politiche del manifesto alle opinioni dei soggetti raffigurati, i quali avevano eccepito espressamente di avere un orientamento favorevole al divorzio e pertanto opposte a quelle sostenute dal messaggio del manifesto. A ciò si aggiungeva che i due, raffigurati come tali, non erano in realtà una coppia.

A tutela di tali interessi, il giudice rilevava, dunque, che costituisce violazione del diritto all'identità personale, inteso quale diritto a non vedere travisare la propria personalità individuale, l'affissione di un manifesto per la propaganda a favore dell'abrogazione della legge sul divorzio, nel quale sia ritratta l'immagine di persone che, nonostante siano sostenitori dell'istituto del divorzio, vengano fatte apparire come favorevoli alla sua abrogazione. Nell'ipotesi di travisamento della personalità individuale può, con provvedimento d'urgenza, ordinarsi la pubblicazione su organi di stampa di un comunicato tendente a ristabilire la verità.

Come spesso accade, la giurisprudenza interviene in concreto per tutelare interessi non garantiti dal Legislatore, peraltro in un caso in cui, come rilevato dalla dottrina, la controversia avrebbe potuto essere definita anche già solo sulla base delle considerazioni svolte dal giudice sul tema dell'uso abusivo dell'immagine⁵³. Come anche rilevato in senso critico dalla dottrina, però, al contempo, il giudice ordinario non si è preoccupato di argomentare nel merito il fondamento giuridico dell'identità personale ma si è limitato ad affermare l'esistenza di questo diritto in modo perentorio e apodittico⁵⁴.

È evidente, comunque, che la questione centrale della decisione è l'affermazione per via giurisprudenziale del diritto - indipendentemente dall'utilizzo abusivo dell'immagine - a non essere accostati a qualcosa che sia lontano dalle proprie idee o ideali e, in generale, non rappresentativo della propria reale personalità.

⁵² Il Pretore di Roma affermava, in particolare, che costituisce violazione del diritto all'immagine l'affissione di un manifesto per la propaganda a favore dell'abrogazione della legge sul divorzio nel quale venisse ritratta l'immagine di persone che avevano prestato il consenso alla pubblicazione della loro immagine molti anni addietro e per finalità diverse da quella perseguita con la pubblicazione e affissione del manifesto.

⁵³ G. Pino, *Il diritto all'identità personale Interpretazione costituzionale e creatività giurisprudenziale*, cit., 119.

⁵⁴ G. Pino, *Il diritto all'identità personale Interpretazione costituzionale e creatività giurisprudenziale*, cit., 120; E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit., 14.

Si registrano, comunque, in questo periodo, due filoni giurisprudenziali: il primo è in linea con la pronuncia appena ricostruita⁵⁵, l'altro - più formalista - secondo il quale la tutela della "verità storica" di una persona non può trovare garanzia come diritto soggettivo *tout court*, bensì solo indirettamente, qualora leda valori giuridicamente rilevanti o nel caso in cui ci sia una previsione legislativa espressa⁵⁶.

A proposito di quest'ultimo orientamento più formalista, può essere utile citare la notissima decisione n. 2242 del 13 luglio 1971, nella quale la Suprema Corte ribadisce che *"nel nostro sistema nessuna norma, o complesso di norme, prevede, neppure implicitamente, una situazione di diritto soggettivo che abbia come contenuto il potere di pretendere sempre e in ogni caso il rispetto della verità storica. Questa verità è tutelata sì, come diritto soggettivo in alcune situazioni, anche di ampia estensione, ma dalle norme che disciplinano queste situazioni non si può desumere un principio generale di tutela indiscriminata"*.

A partire dagli anni Ottanta, poi, sempre più pronunce menzionano nelle loro motivazioni il diritto all'identità personale, nella maggior parte con riferimento all'identità politica sia di persone fisiche che giuridiche⁵⁷.

Nel contesto appena descritto, il punto di svolta è rappresentato, però, dalla sentenza della Corte di Cassazione n. 3769 del 22 giugno 1985.

Si anticipa, sin da ora, che tale pronuncia ha il pregio da una parte di dare un contributo fondamentale al dibattito sulla definizione della identità personale che si era svolto sino a quel momento e dall'altra di spingere il diritto all'identità personale verso una dimensione costituzionale.

La sentenza decide il terzo grado del noto "caso Veronesi". La vicenda riguardava un oncologo di chiara fama di cui erano state strumentalmente travisate - per finalità commerciali - le dichiarazioni rilasciate in un'intervista. In particolare, nonostante l'intervista del dott. Veronesi fosse evidentemente volta a disincentivare il fumo di sigarette in ogni loro forma e marca, la società produttrice di tabacco Austria Tabakwerke aveva pubblicato sulla stampa periodica un inserto di pubblicità per promuovere la vendita di una determinata marca di "sigarette leggere", nel

⁵⁵ Cfr. Pretura di Roma, decisione del 7 maggio 1974, in *Foro it.*, 1974, p. 3227 ss., ove si sottolinea, tuttavia, che tale pronuncia non si riferisce all'identità di una persona fisica ma di una persona giuridica. In particolare, viene riconosciuta tutela al "partito comunista italiano" a fronte dell'illecita riproduzione di frasi volutamente incomplete e con intento illecito, che miravano a ledere l'identità dello stesso. Il Comitato per il referendum sul divorzio aveva infatti estrapolato frasi relative ad alcuni discorsi di Palmiro Togliatti, suscettibili di far credere all'elettorato che il partito fosse contrario al divorzio.

⁵⁶ Cass. civ., 13 luglio 1971, n. 2242; nonché, Pretura di Pontedera, decisione del 10 maggio 1974, in *Foro it.*, 1975, c. 491. Quest'ultima pronuncia riguarda sempre la possibilità di riconoscere tutela all'identità di una persona giuridica. Il giudice, in questo caso, afferma che i diritti soggettivi sono tipici e che, nel caso di specie, mancava la previsione di un diritto soggettivo di un partito politico a che non venisse manipolato il pensiero di un proprio *leader*. Al contrario, la censurata condotta avrebbe trovato tutela nell'alveo della disposizione di cui all'art. 21 Cost. quale esercizio del diritto di manifestazione del pensiero.

⁵⁷ Cfr. Pretura di Roma, ord. 2 giugno 1980; Pretura di Verona, ord. 21 dicembre 1982; Tribunale di Roma, sent. 15 settembre 1984.

quale era inserita la frase “secondo il prof. Umberto Veronesi – direttore dell’Istituto dei tumori di Milano – questo tipo di sigarette riduce quasi della metà il rischio del cancro”.

Ebbene, si premette che, in tutti i gradi di giudizio precedenti⁵⁸, i giudici avevano già affermato il diritto del prof. Veronesi alla “identità personale”, attraverso un’interpretazione estensiva del diritto al nome *ex artt. 6 e 7 c.c.*⁵⁹

La sentenza della Cassazione in oggetto, però, come si anticipava, ha il merito proprio di mutare l’orientamento sino a quel momento affermatosi (in particolare, dalla citata pronuncia della Cassazione n. 2242 del 13 luglio 1971.), che, si ricorda, tutelava il diritto all’identità personale solo nel caso coincidesse con la tutela di una fattispecie espressamente prevista dalla legge, cioè in quanto rientrante nella fattispecie di altri diritti come il nome, l’immagine, la riservatezza.

Perché la Cassazione decide di discostarsi da tale approccio? In casi come quello oggetto della pronuncia, ad avviso della Corte, non sono lesi il nome, l’immagine o l’onore della persona, bensì l’interesse, ritenuto meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la propria reale identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere riconosciuta con l’esplicazione dei criteri della normale diligenza e della buona fede oggettiva; il ricorrente ha, cioè, interesse a non vedersi all’esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc., quale si era estrinsecato od appariva, in base a circostanze concrete e univoche, destinato a estrinsecarsi nell’ambiente sociale. Questo diritto all’identità personale non può trovare fondamento nelle forme degli art. 7 e 10 c.c., in quanto in sede interpretativa non si può alterare il contenuto normativo dell’art. 7 e dell’art. 10 oltre i limiti consentiti dallo strumento dell’interpretazione estensiva e non si può attribuire alle due norme una portata innovativa incompatibile con la loro struttura. Infatti, i segni distintivi identificano il soggetto sul piano dell’esistenza materiale e della condizione civile e legale e l’immagine evoca le mere sembianze fisiche della persona; l’identità rappresenta, invece, una formula sintetica per contraddistinguere il soggetto da un punto di vista globale, nella molteplicità delle sue specifiche caratteristiche e manifestazioni.

Dunque, secondo la Cassazione, la disciplina inerente alla sua tutela avrebbe potuto dedursi per analogia dalle norme che tutelano beni collegati all’identità come

⁵⁸ Cfr. Tribunale di Milano, sent. 19 giugno 1980; Corte d’Appello di Milano, sent. 2 novembre 1982.

⁵⁹ Le sentenze dei primi due gradi di giudizio riconoscono il diritto all’identità personale come la garanzia affinché il nome di una persona fisica sia considerato come il “simbolo dell’intera personalità dell’individuo morale, intellettuale e sociale”. L’uso del nome altrui deve, in questo senso, considerarsi illecito quando sia tale da incidere negativamente sulla personalità del soggetto identificato.

il diritto al nome (art. 7 c.c.), consentendo al soggetto che subisce una lesione pregiudiziale alla sua identità personale la possibilità di chiedere in sede giudiziale la cessazione del fatto lesivo e il risarcimento del danno, nonché ottenere dal giudice l'ordine di pubblicazione della sentenza.

Si aggiunge che, come anticipato, la Suprema Corte cambia orientamento riconoscendo per la prima volta il fondamento costituzionale del diritto all'identità personale.

In particolare, individua il fondamento normativo del diritto all'identità personale direttamente nell'art. 2 della Costituzione. Infatti, osserva che il fondamento giuridico positivo della tutela che si avverte l'esigenza di assicurare all'interesse dell'intangibilità dell'identità personale debba individuarsi, “conformemente a un indirizzo di dottrina che va sempre più diffondendosi”, nell'art. 2 Cost., il quale dispone che la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali, ove si svolge la sua personalità.

Il diritto all'identità personale mira a garantire la fedele e completa rappresentazione della personalità individuale del soggetto nell'ambito della comunità, generale e particolare, in cui tale personalità individuale è venuta svolgendosi, estrinsecandosi e solidificandosi.

Si tratta di un interesse essenziale, fondamentale e qualificante della persona e la finalità dell'art. 2 Cost. è proprio quella di tutelare la persona umana integralmente e in tutti i suoi modi di essere essenziali⁶⁰.

3. L'“identità personale” nel diritto costituzionale: la qualificazione dei “nuovi diritti” fondamentali.

Può essere utile soffermarsi brevemente sulla nozione di “diritto fondamentale”, dato che, come si vedrà a breve, a partire dalla sentenza citata e grazie alla successiva attività della Corte costituzionale, si è assistito alla progressiva affermazione dell'identità personale non solo come diritto ma come diritto fondamentale della persona⁶¹.

⁶⁰ La Corte, tuttavia sembra operare due distinzioni: non aderisce alla teoria monista dei diritti della personalità e non attribuisce al diritto all'identità lo status di diritto costituzionale, riservato principalmente ai diritti espressamente previsti dalla Costituzione. In questo contesto, la disciplina del diritto all'identità personale va piuttosto desunta, per analogia, dagli altri diritti della personalità, con particolare riferimento al diritto al nome.

⁶¹ Per una trattazione di carattere generale si rinvia a B. Celano, *I diritti dello stato costituzionale*, Bologna, 2013; nonché, G. Pino, *Il costituzionalismo dei diritti. Struttura e limiti del costituzionalismo contemporaneo*, Bologna, 2017; Sul piano del diritto costituzionale italiano e comparato, si vedano altresì i contributi raccolti in V. Baldini (a cura di), *Che cosa è un diritto fondamentale? Atti del convegno annuale dell'Associazione “Gruppo di Pisa”, Cassino 10 e 11 giugno 2016*, Napoli, 2017.

Non sembrano esservi particolari dubbi per i diritti che trovano un loro fondamento nella Costituzione e che “fondano l’ordinamento giuridico”⁶².

In dottrina si è tentata anche una classificazione tramite la ricostruzione delle seguenti tre diverse definizioni: i) una di tipo contenutistico, secondo la quale sono fondamentali i diritti che proteggono un determinato interesse ritenuto particolarmente rilevante; ii) una, di tipo formale, secondo la quale sono fondamentali tutti quei diritti che trovano il loro fondamento in una fonte positiva posta al livello più alto della gerarchia delle fonti; iii) una estensionale indiretta, secondo la quale i diritti sono fondamentali in quanto considerati tali da alcuni soggetti⁶³.

Ebbene, qualificare un diritto come fondamentale non è marginale, alla luce del fatto che ciò comporta inevitabilmente la sua “inviolabilità”⁶⁴. Non solo. Qualificare un diritto come fondamentale comporta essere titolare di una pretesa qualificata - nei confronti di soggetti pubblici e privati - la cui ampiezza può dipendere dal grado di tutela che tale diritto ha ricevuto sia a livello interno che esterno⁶⁵.

Secondo alcuni⁶⁶, e come in realtà sembra emergere da alcuni passaggi della pronuncia appena citata, la Suprema Corte, con questa sentenza, avrebbe “fatto sua” la tesi di quella dottrina che aveva inteso l’art. 2 della Costituzione come una fattispecie “aperta”, cioè come norma che non si limita soltanto a riepilogare i diritti fondamentali espressamente menzionati nel testo costituzionale, bensì come disposizione idonea a includere e assicurare tutela a nuovi interessi emergenti ed essenziali della persona.

In effetti, il ragionamento effettuato dalla Cassazione richiama inevitabilmente il noto dibattito sull’art. 2 Cost., che ha impegnato e continua a impegnare i costituzionalisti.

Si fa riferimento alla contrapposizione tra gli orientamenti che hanno qualificato l’art. 2 Cost. come norma a “fattispecie chiusa” e a “fattispecie aperta”.

Come noto, a parere dei sostenitori del primo orientamento, l’art. 2 andrebbe letto, con un approccio restrittivo, come norma esclusivamente ricognitiva dei diritti enumerati. I diritti inviolabili, dunque, in quest’ottica, sarebbero solo quelli qualificati come tali⁶⁷.

⁶² Cfr. M. Luciani, *Positività, metapositività e parapositività dei diritti fondamentali*, in G. Brunelli, A. Pugiotto, P. Veronesi (a cura di), *Scritti in onore di Lorenza Carlassare*, vol. III, Napoli, 2009, 1055 ss.

⁶³ G. Pino, *Il costituzionalismo dei diritti*, cit., 54.

⁶⁴ Cfr. A. Baldassarre, *Diritti inviolabili* voce, in *Enc. giur.*, vol. XI, Roma, 1989, 1 ss.

⁶⁵ G. Pino, *Il costituzionalismo dei diritti*, cit., 56.

⁶⁶ E.C. Raffiotta, *Appunti in materia di diritto all’identità personale*, cit., 8.

⁶⁷ Con riferimento al dibattito dottrinario sull’art. 2 Cost. come norma a fattispecie chiusa cfr. A. Pace, *Problematica delle libertà costituzionali*, Padova, 1985. Sul tema cfr. anche N. Zanon, *Corte costituzionale, evoluzione della “coscienza sociale”, interpretazione della Costituzione e diritti fondamentali: questioni e interrogativi a partire da un caso paradigmatico*, in *Riv. AIC*, n. 4/2017, 1 ss.; A. Morelli, *I diritti senza legge*, cit., 14; R. Bin, *Chi è il giudice dei diritti? Il modello costituzionale e alcune deviazioni*, in *Riv. AIC*, n. 4/2018, 1 ss.; A. Ruggeri, *Crisi dello Stato nazionale, dialogo intergiurisprudenziale, tutela dei diritti fondamentali: notazioni introduttive*, in *Consulta online*, 2014, 1 ss; P. Barile, *Diritti dell’uomo e libertà fondamentali*, Bologna, 1984, 65 ss.;

Secondo la ricostruzione alternativa, invece, è ammissibile, come affermato anche dalla Cassazione nella sentenza citata, la possibilità di un allargamento del patrimonio costituzionale dei diritti, in ragione del fatto che l'art. 2 Cost. sarebbe, in realtà, una "clausola aperta"⁶⁸.

Può essere utile ricordare che entrambi gli orientamenti sono stati oggetto di critiche. Il primo perché, vedendo l'art. 2 come meramente ricognitivo, oltre a privarlo di utilità concreta, comporterebbe una eccessiva restrizione dei diritti inviolabili, che, a quel punto, sarebbero rappresentati esclusivamente dagli artt. 13, 14, 15 e 24 Cost. Senza contare il fatto che l'art. 2 risponde, invece, a parere di molti, anche all'esigenza di rimuovere le condizioni sociali di diseguaglianza⁶⁹.

La seconda, dal canto suo, è priva di appiglio positivo e non si preoccupa di cercare l'ancoraggio dei cc.dd. "nuovi diritti"⁷⁰. Questi ultimi, detti anche "diritti emergenti", sono sempre necessariamente conseguenti a quelli costituzionalmente previsti e l'eventuale fondamento costituzionale di essi risiede nella possibilità di ricondurli all'evoluzione di significato delle disposizioni costituzionali⁷¹.

Proprio sul fondamento dei "nuovi diritti", a parere di alcuni, cadono entrambe le teorie. Del resto, il "problema dei nuovi diritti" è quello della loro tutela effettiva. Come rilevato da autorevole dottrina, emerge sul tema l'esigenza fondamentale di "*rendere effettive le situazioni di diritto formalmente attribuite o comunque ricollegabili a qualcuna delle proclamazioni con cui la Costituzione impegna la Repubblica a fare questo o quello*"⁷². Tale "problema" - che consiste nel fatto che a esigenze emergenti non sempre corrispondono situazioni giuridiche soggettive effettivamente tutelabili⁷³ - di regola dovrebbe essere risolto dal Legislatore che dovrebbe enuclearli e specificarli. Se non lo fa, però, il tutto è lasciato alla giurisprudenza - soprattutto costituzionale e di legittimità - che è chiamata, con riferimento al "nuovo diritto", a svolgere il ruolo interpretativo-creativo che le è proprio, partendo dalle disposizioni costituzionali esplicite.

P. Caretti, G. Tarli Barbieri, *I diritti fondamentali. Libertà e diritti sociali*, V ed., Torino, 2022, 145 ss.

⁶⁸ Sulla configurazione dell'art. 2 Cost. quale norma a "fattispecie aperta" cfr. A. Barbera, *Art. 2 Cost.*, in G. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1975, 50 ss., il quale, successivamente, ha precisato i limiti della materia in Id., "*Nuovi diritti*": *attenzione ai confini*, in L. Califano (a cura di), *Corte costituzionale e diritti fondamentali*, Torino, 2004, 19 ss.

⁶⁹ P. Ridola, *Diritti di libertà e costituzionalismo*, Torino, 1997, 46.

⁷⁰ F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, cit.; A. Pace, *Il c.d. diritto all'identità personale e gli art. 2 e 21 della Costituzione*, in *Giur. civ.*, n. 9/1980, 409 ss.; S. Piccini, *Appunti sui diritti della personalità e sui c.d. nuovi diritti. Tutela e promozione dell'identità personale*, in *Dir. famiglia e persone*, n. 1/2021, 227 ss.

⁷¹ Cfr. F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, cit., 43, secondo il quale "*Solo in questo modo i diritti emergenti dall'evoluzione sociale possono trovare il loro fondamento positivo di diritti per l'innanzi non contemplati in quanto non (ancora) riconoscibili*".

⁷² S. Rodotà, *Statuti e carte delle libertà*, in *Pol. dir.*, 1980, 170 ss.

⁷³ Cfr. C. Colapietro, M. Ruotolo, *Diritti e Libertà*, in F. Modugno (a cura di), *Manuale di diritto pubblico*, Torino, 2023, 631 ss.

Ciò ha spinto alcuni a elaborare una terza tesi⁷⁴, secondo la quale non tutti i diritti possono spiccare il volo a partire dalla lettera della Costituzione. In particolare, tale orientamento ammette l'estensione dei diritti oltre al perimetro disegnato dalla Costituzione, solo nel caso si tratti di "diritti inviolabili"⁷⁵ e riferiti al principio supremo della libertà-dignità⁷⁶.

Può essere utile precisare, per completezza, che, a parere di alcuni, i nuovi diritti, a differenza dei diritti contenuti nelle Costituzioni, hanno la caratteristica di essere assoluti, nascendo privi di limitazioni perché hanno generalmente origine giurisdizionale e perché il principio di non discriminazione tende a rimuovere ogni limitazione alle nuove situazioni soggettive⁷⁷.

L'espansione dei nuovi diritti, di conseguenza, non è scevra da rischi, che sono stati negli anni paventati dalla dottrina. In particolare, la progressiva espansione dei diritti individuali sembra essere parallela al dilagare di una concezione culturale individualistico libertaria dei diritti che porta a "negare e rimuovere ogni forma di limitazione ai diritti soggettivi" e il "progresso per accumulazione" potrebbe portare ad una "degenerazione utopistica"⁷⁸, nell'ambito della quale, però, si rischia di non centrare l'obiettivo. Del resto, i diritti umani sono indivisibili e interdipendenti e, di conseguenza, ogni nuovo diritto entra nel bilanciamento complessivo con i vecchi diritti e alterna l'assetto complessivo⁷⁹. Di conseguenza, "il puro moltiplicarsi dei diritti non avvicina alla meta desiderata ma - al contrario - può far naufragare l'intero viaggio". In che modo ciò potrebbe accadere? La dottrina prospetta un insperato scenario nel quale i nuovi diritti, anziché servire allo scopo per cui sono nati - ossia come baluardo della persona contro le degenerazioni del potere - diventino essi stessi strumenti di potere o finiscano per essere strumento per promuovere solo interessi di alcuni gruppi più influenti. Con questa consapevolezza, alcuni propongono la sfida giuridica che pongono i nuovi diritti nel XXI secolo differentemente da quella posta nel XX: "Se allora il problema giuridico principale era quello di assicurare una tutela effettiva ai diritti proclamati nella Carta e quindi potenziare gli strumenti di garanzia e implementazione dei diritti, oggi il problema più grande e delicato è quello di conservare la natura dei diritti

⁷⁴ F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, cit., 48.

⁷⁵ Cfr. Corte cost. 15 dicembre 1988, n. 1146 in cui sono definiti "inviolabili" quelli assunti come valori primari e principi supremi dell'ordinamento costituzionale.

⁷⁶ C. Colapietro, M. Ruotolo, *Diritti e Libertà*, cit., 635.

⁷⁷ M. Cartabia, *In tema di "nuovi" diritti*, cit., 631, la quale osserva che tutti i diritti positivizzati, anche quelli inviolabili, sono sempre accompagnati da limitazioni. La libertà personale, ad esempio, pur inviolabile, può essere limitata nei casi previsti dalla legge e dall'autorità giudiziaria.

⁷⁸ M. Cartabia, *In tema di "nuovi" diritti*, cit., 633. Secondo la teoria dell'autrice, la moltiplicazione e assolutizzazione dei diritti sono due fenomeni casualmente concomitanti ed espressione di una medesima concezione dell'uomo e del suo vivere sociale.

⁷⁹ *Ibidem*, 633.

*individuali come garanzia della persona umana nei confronti di ogni forma di potere, preservandoli dal rischio di diventare essi stessi uno strumento di esercizio di potere sulla persona umana*⁸⁰.

Ebbene, ciò premesso sulla tematica in generale, quando si parla di “identità” da un punto di vista costituzionale si fa riferimento, dunque, il più delle volte, ai “nuovi diritti”, elaborati dalla Corte costituzionale e ricondotti dalla stessa, attraverso il combinato disposto degli art. 2, 3 (secondo comma) e 13 Cost., ai diritti fondamentali della persona⁸¹.

Come noto, l’art. 13 Cost. parla di una libertà personale qualificata come “inviolabile”, assistita sia da riserva di legge che di giurisdizione. Prima di tutto, infatti, come noto, la disposizione precisa che non è ammessa alcuna forma di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non nei casi previsti dalla legge o per atto motivato dell’autorità giudiziaria. Si sofferma anche sulle misure cautelari e sui diritti delle persone già soggette a detenzione. In sintesi, come noto, la disposizione contiene, anzitutto, “*le guarentigie supreme dell’habeas corpus, che sono una delle pietre angolari della convivenza civile in un regime democratico*”⁸².

Tuttavia, accedendo, tramite le tesi interpretative citate, a una lettura diversa della libertà della persona di cui all’art. 13 Cost., nella sua dimensione psicofisica - della mente e del corpo nella loro indissolubile unità, dotata di comprensività potenzialmente illimitata - questa si configura come la vera matrice dei singoli diritti personali enumerati e degli eventuali altri diritti (non enumerati) che, in quanto parallele dirette esplicazioni, vanno considerati, alla pari degli altri, come diritti positivi della persona⁸³.

In altre parole, a tale “*diritto fundamentalissimo della persona*” possono essere ricondotti sia i singoli diritti personali enumerati nella Costituzione sia una serie di diritti elaborati dalla giurisprudenza costituzionale, nel momento in cui si è trovata a fronteggiare esigenze sorte anche a distanza di molti anni dall’entrata in vigore della carta fondamentale.

Tali nuovi diritti che promanano dalla libertà personale così intesa si approfondiranno nel prosieguo. *In primis*, viene chiaramente in rilievo per il presente scritto il diritto all’identità personale in tutte le sue declinazioni come elaborate dalla giurisprudenza della Corte costituzionale come derivato dall’art. 13 Cost.

Con riferimento alla dimensione sovranazionale, il diritto all’identità personale non trova esplicito riconoscimento all’interno del testo della CEDU. Non-

⁸⁰ *Ibidem*, 635.

⁸¹ F. Modugno, *I “nuovi diritti” nella giurisprudenza costituzionale*, cit.; C. Colapietro, M. Ruotolo, *Diritti e Libertà*, cit., 636; M. Cartabia, *In tema di “nuovi” diritti*, cit., 633.

⁸² Corte cost., 9 luglio 1959, n. 49.

⁸³ F. Modugno, *I “nuovi diritti” nella giurisprudenza costituzionale*, cit., 51.

stante ciò, la Corte di Strasburgo tramite la propria attività interpretativa l'ha ricondotto all'interno dell'art. 8 della Convenzione⁸⁴, grazie al progressivo allargamento della nozione di tutela della vita privata⁸⁵. Proprio la Corte, attraverso un insieme ampio e talvolta particolarmente dettagliato di pronunce, soprattutto in materia di art. 8 della Convenzione europea dei diritti dell'uomo, ha contribuito a ridefinire e ampliare le istanze di tutela dell'identità personale.

3.1. La definizione dell'“identità personale” nella giurisprudenza costituzionale.

La giurisprudenza costituzionale ha avuto il pregio di elevare il diritto all'identità personale a rango di diritto fondamentale e di attribuire allo stesso un nuovo significato. Se, in effetti, come si è visto, fino a questo momento le codificazioni e la giurisprudenza sopra menzionate avevano elaborato una nozione di identità personale legata al diritto di essere correttamente rappresentati, è da questo momento che avviene il riconoscimento del diritto a essere sé stessi⁸⁶.

In particolare, nella prima pronuncia costituzionale sul tema in oggetto, la sentenza n. 13 del 1994⁸⁷, si legge che, “*tra i diritti che formano il patrimonio ir-retrattabile della persona umana, l'art. 2 della Costituzione riconosce e garantisce anche il diritto all'identità personale*”. E ancora che “*si tratta del diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo*”.

L'oggetto della vicenda era il diritto al mantenimento del nome ma la Consulta ha colto l'occasione per estendere notevolmente il campo di analisi. Ciò si evince anche dal fatto che, fino a questo momento, il diritto di identità, come visto,

⁸⁴ L'art. 8 della CEDU afferma il diritto al rispetto della vita privata e familiare. In particolare, prevede che “*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*”. La disposizione è stata definita una vera e propria “nursery” dei nuovi diritti da M. Burbergs, *How the right to respect for private and family life, home and correspondence became the nursery in which new rights are born: Article 8 ECHR*, in E. Brems, J. Gerards (a cura di), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights*, Cambridge University Press, Cambridge, 2014, 315 ss.

⁸⁵ Si veda, tra le prime sentenze della Corte EDU che optano per una interpretazione estensiva dell'art. 8, Corte EDU, *Niemietz c. Germania*, 19 dicembre 1992; Si veda sull'identità personale, Corte EDU, *Bensaid c. Regno Unito*, 6 febbraio 2001.

⁸⁶ Cfr. G. Pino, *L'identità personale* cit., 301, il quale osserva, testualmente, che “*Sembrirebbe trattarsi di un diritto non tanto a che le proprie scelte e adesioni (moralì, professionali, culturali, religiose ecc.) siano correttamente rappresentate, ma piuttosto che siano rispettate*”.

⁸⁷ Cfr. Corte cost., 3 febbraio 1994, n. 13.

era stato evocato dalla giurisprudenza in fattispecie diverse rispetto a quella oggetto della pronuncia⁸⁸.

Nella fattispecie, il Tribunale di Firenze aveva sollevato una questione di legittimità costituzionale - in riferimento all'art. 2 della Costituzione - degli artt. 165 e segg. del Regio decreto 9 luglio 1939 n. 1238, nella parte in cui non prevedevano che “*a seguito di rettifica degli atti dello stato civile per ragioni indipendenti dall'interessato, il soggetto stesso possa mantenere il cognome fino a quel momento attribuito e che è entrato a far parte del proprio diritto costituzionalmente garantito all'identità personale*”.

In sintesi, infatti, ai sensi dell'art. 165 dell'ordinamento dello stato civile, il Procuratore della Repubblica di Firenze, aveva richiesto la rettifica dell'atto di nascita di un soggetto al fine di eliminare il riferimento al padre dello stesso, che non lo aveva riconosciuto. In caso di rettifica, conseguenza automatica e inevitabile era il cambiamento del cognome attuale con quello della madre poiché, in base all'articolo 262 del codice civile, il figlio, a questo punto naturale, assume il cognome dell'unico genitore che lo ha riconosciuto.

Il figlio, però, chiedeva di conservare integralmente il proprio nome, quale segno distintivo ormai acquisito nelle proprie relazioni sociali, rivendicando un interesse concreto, attuale e immediato.

Ad avviso del giudice *a quo*, se la rettifica è atto dovuto, in quanto la *fidefacienza* del registro dello stato civile risponde ad una pubblica necessità, accanto ad essa può configurarsi il diritto del soggetto a conservare il nome con il quale fin dalla nascita è stato individuato, conosciuto e stimato nel proprio ambiente sociale e che perciò ha assunto le caratteristiche di un segno distintivo, con rilevanza e autonomia proprie, della sua identità, come caratteristica precisa, personalissima e proiettata all'esterno.

Ma nell'ordinamento dello stato civile, conclude il giudice *a quo*, non esiste una norma di salvaguardia applicabile alla fattispecie, sebbene le esigenze di protezione dell'identità personale trovino riconoscimento diretto nell'art. 2 della Costituzione quale garanzia generale di tutela della persona umana.

La denunciata illegittimità costituzionale consiste, dunque, nel mancato riconoscimento del diritto del soggetto al mantenimento del cognome attribuito, allorché il medesimo sia ormai da ritenersi parte integrante della propria identità personale, indipendentemente da quello che successivamente si riconosca spettante in forza dei rapporti di filiazione correttamente accertati.

La Consulta, come si diceva, partendo dall'analisi del diritto al mantenimento del nome disciplinato dal codice civile, affermava, concordando con il giudice *a quo*, che, nella fattispecie, mentre è assolutamente pacifico che l'atto di nascita dell'interessato debba essere rettificato e che debba indicare l'esatto rapporto di

⁸⁸ Si veda, in proposito, il commento di A. Pace, *Nome, soggettività giuridica e identità personale*, in *Giur. cost.*, n. 1/1994, 103 ss.

filiazione quale risulta dal rispetto delle norme in materia, viene soltanto in discussione il diritto del soggetto stesso a mantenere il cognome, non in quanto derivatogli dal presunto padre, bensì come segno distintivo che ha comunque assunto la rilevanza e l'autonomia proprie di una caratteristica precisa e personalissima della sua identità.

E prosegue: *“Ciò posto, è certamente vero che tra i diritti che formano il patrimonio irrettrabile della persona umana l'art. 2 della Costituzione riconosce e garantisce anche il diritto all'identità personale. Si tratta del diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo. L'identità personale costituisce quindi un bene per sé medesima, indipendentemente dalla condizione personale e sociale, dai pregi e dai difetti del soggetto, di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata. Tra i tanti profili, il primo e più immediato elemento che caratterizza l'identità personale è evidentemente il nome - singolarmente enunciato come bene oggetto di autonomo diritto nel successivo art. 22 della Costituzione - che assume la caratteristica del segno distintivo ed identificativo della persona nella sua vita di relazione. Ora, posto che nella disciplina giuridica del nome confluiscono esigenze di natura sia pubblica che privata, l'interesse pubblico a garantire la fede del registro degli atti dello stato civile è soddisfatto allorché sia rettificato l'atto riconosciuto non veritiero. Una volta certi i rapporti di famiglia della persona, non assume rilevanza ai fini dell'interesse pubblico che questi mantenga il nome precedentemente portato al pari di qualsiasi altro omonimo”*.

In quest'ottica, l'identità personale costituisce, dunque, di per sé stessa, un bene, a prescindere dai pregi e dai difetti che caratterizzano ogni soggetto e indipendentemente da qualsivoglia situazione sociale ed economica. A ciascuno, in altre parole, indipendentemente da tutto e proprio in ragione delle caratteristiche che lo contraddistinguono, è riconosciuto il diritto a che la sua individualità sia preservata.

L'interpretazione della Corte costituzionale conferma che il diritto all'identità non può ridursi al solo diritto al nome o all'immagine. Anzi, la Corte lo spinge ben oltre, al punto che, in quest'ottica, si configura come qualcosa di molto più ampio e diverso e il diritto al nome rimane solo l'occasione per affermarlo.

Alcuni commentatori hanno posto l'accento sulla prospettiva relazionale dell'identità personale a cui si faceva riferimento e che sarebbe valorizzata da questa sentenza: nella fattispecie della sentenza n. 13 del 1994, sarebbe, in quest'ottica, l'essere partecipe alla vita associata che riempie di contenuto tale diritto⁸⁹. Altri hanno valorizzato, commentando la giurisprudenza anche successiva, il fattore tem-

⁸⁹ Cfr. A. Randazzo, *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, cit.

porale: il trascorrere del tempo sedimenta e consolida l'identità della persona, divenendo così giustificazione per il mantenimento del cognome originariamente attribuito rispetto a vicende modificative dello *status* personale capaci di incidere sul cognome stesso.

A parere di alcuni, poi, la definizione ampia della Consulta rischia di essere una “scatola vuota”, anche se, ad uno sguardo a posteriori, ha dimostrato una forza espansiva notevole, “*riuscendo ad attrarre sotto al proprio ombrello protettivo numerosi e a volte eterogenei interessi*”⁹⁰.

Interessante la prospettiva di alcuni autori⁹¹ a parere dei quali la “scoperta” giurisprudenziale dell'identità personale, pur nelle sue tante e diverse implicazioni, risulta, in realtà, pienamente coerente con l'ispirazione personalista della forma di Stato dell'ordinamento italiano. In questo senso, anche se, come anticipato, la Costituzione non contiene riferimenti espliciti al tema e il riconoscimento del diritto all'identità personale ha una matrice giurisprudenziale, in realtà, si tratterebbe di un concetto da sempre presente nel testo costituzionale, risultando, nella connotazione attribuitale dalla giurisprudenza ordinaria citata e da quella costituzionale che si approfondirà a breve, una proiezione del principio personalista di cui è intrisa l'intera Costituzione⁹².

3.2. Il contributo della Corte di Cassazione nell'interpretazione costituzionale.

Ci si vuole soffermare brevemente su una interessante lettura della Costituzione proposta dalla Corte di Cassazione a distanza di soli due anni dalla pronuncia della Consulta appena menzionata.

Si tratta della sentenza n. 978 del 7 febbraio 1996, che affronta un tema di grande rilevanza giuridica: il bilanciamento tra il diritto all'identità personale e la libertà di espressione, in particolare nell'ambito del diritto di cronaca e di creazione artistica.

Il caso vede coinvolti i coniugi Tabocchini, che avevano agito in giudizio per ottenere la distruzione di uno sceneggiato televisivo incentrato sul tragico episodio dell'uccisione del calciatore Luciano Re Cecconi, avvenuta nella gioielleria degli stessi coniugi durante una tentata rapina simulata dalla vittima.

⁹⁰ G. Pino, *Identità personale* cit., 301.

⁹¹ A. Morelli, *Persona e identità personale*, cit., 49.

⁹² Cfr. Corte cost., 29 aprile 1999, n. 167, § 6 del cons. in dir. nel quale si legge che “*il principio personalista, ricavabile dagli artt. 2, 3 e 13 Cost., ma in ultimo, dall'intera trama normativa della Carta repubblicana, pone come fine ultimo dell'organizzazione sociale lo sviluppo di ogni singola persona umana*”. In dottrina cfr. A. Ruggeri, *Il principio personalista e le sue proiezioni*, in *Federalismi.it*, n. 17/2013, 1 ss.

I ricorrenti lamentavano che la rappresentazione dei fatti nello sceneggiato fosse lesiva della loro identità personale, dipingendoli in modo distorto e denigratorio. La Cassazione, chiamata a dirimere la questione, afferma che il diritto all'identità personale, pur trovando fondamento nell'art. 2 della Costituzione, non è assoluto ma va temperato con altri diritti costituzionalmente garantiti, tra cui la libertà di espressione di cui all'art. 21 Cost.

In particolare, la Corte riconosce la prevalenza del diritto di cronaca e di creazione artistica a condizione che: la notizia o l'opera artistica abbiano un'utilità sociale; i fatti narrati siano veri; l'esposizione dei fatti avvenga in forma civile, rispettosa della persona, senza intenti diffamatori o gratuitamente lesivi della reputazione altrui.

Applicando tali principi al caso di specie, la Cassazione ritiene che lo sceneggiato, pur rievocando un fatto privato, avesse una sua utilità sociale in quanto rappresentazione emblematica di un periodo storico, gli anni '70, caratterizzato da una diffusa violenza sociale. Inoltre, la Corte, esaminando il contenuto dello sceneggiato, esclude che la rappresentazione dei coniugi Tabocchini fosse di per sé denigratoria o deformante la loro identità. La Corte rileva come i fatti narrati corrispondessero a verità e che la descrizione dei personaggi, pur non essendo idilliaca, non fosse finalizzata a screditarli. Anzi, la Corte sottolinea come alcuni aspetti della loro caratterizzazione, come il comportamento "impacciato" del Tabocchini dopo la tragedia, fossero preferibili ad un'inverosimile rappresentazione di freddezza o cinismo.

La sentenza, dunque, ribadisce la centralità del bilanciamento tra diritti fondamentali, sottolineando come la libertà di espressione, in ambito giornalistico e artistico, trovi un limite nella tutela della dignità e dell'identità personale. Tale limite è superabile solo quando la rappresentazione dei fatti, pur se critica, sia ancorata alla verità, persegua un interesse pubblico e si mantenga entro i limiti della contenenza formale, evitando gratuiti attacchi personali.

Il caso è emblematico, dunque, dell'apparente conflitto tra due diritti fondamentali - il diritto all'identità personale e il diritto alla libertà di espressione - che la Cassazione ha deciso a favore di quest'ultima. Interessante però, ai fini della presente ricerca, è la ricostruzione effettuata dalla Suprema Corte circa *"la nozione, il fondamento giuridico, la struttura, il contenuto, le forme e i limiti di tutela del "diritto alla identità personale"*.

Dopo una ricostruzione sulla elaborazione storica e dottrinale dell'identità personale, la Corte aderisce alla concezione "monistica" dei diritti della personalità. A tale proposito, afferma, in particolare, che: *"L'«identità personale» è venuta emergendo, nella più recente elaborazione giurisprudenziale, come bene-valore costituito dalla proiezione sociale della personalità dell'individuo, cui si correla un interesse del soggetto ad essere rappresentato, nella vita di relazione, con la sua vera identità, a non vedere quindi, all'esterno, modificato, offuscato o comunque alterato il proprio patrimonio intellettuale, ideologico, etico, professionale"*

(ecc.) quale già estrinsecatosi o destinato, comunque, ad estrinsecarsi, nell'ambiente sociale, secondo indici di previsione costituiti da circostanze obiettive ed univoche [...] La specificità di tale interesse («ad essere se stesso») è stata anche colta in parallelo od in contrappunto ad altri interessi ad esso contermini o collegati [...]. Anche se la utilità, soprattutto didascalica, di tali distinzioni non deve fare velo al carattere solidale di tali interessi, confluenti in un valore unitario, che è quello della persona umana. Quest'ultima puntualizzazione che presuppone l'adesione ad una concezione «monistica» dei diritti della personalità (da questa corte, del resto, già sostanzialmente anticipata nella citata sent. 990/63) aiuta anche a definire, senza perplessità, in termini di diritto soggettivo perfetto, la struttura della situazione soggettiva considerata. E consente, nel contempo, di individuare con maggiore risolutezza (superando le riserve affioranti in qualche tratto della motivazione della pure già citata sentenza 3769/85) il correlativo fondamento giuridico, ancorandolo direttamente all'art. 2 Cost. (cfr. implicitamente su questa linea, anche Corte cost. 13/94, cit.): inteso tale precetto nella sua più ampia dimensione di clausola generale, «aperta» all'evoluzione dell'ordinamento e suscettibile, perciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità in correlazione anche all'obiettivo primario di tutela del «pieno sviluppo della persona umana», di cui al successivo art. 3, cpv. Per cui la concreta disciplina positiva del diritto in esame effettivamente può mutuarsi dalle disposizioni codicistiche e dalle disposizioni sul diritto d'autore, in apertura richiamate: applicabili in via diretta – e non analogica – proprio per l'interpretazione evolutiva ed adeguatrice, di quelle norme che gli indicati precetti costituzionali consentono e, anzi, impongono”.

Interessante anche la precisazione sul fatto che l'identità personale va intesa non in senso soggettivo - come opinione cioè che il soggetto abbia del “proprio io” - bensì in senso oggettivo, in riferimento appunto alla “identità” dell'individuo che, nella realtà sociale generale o particolare, è percepita e conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza o della buona fede soggettiva.

Ebbene, mettendo appunto l'orientamento assunto fino a questo momento, dunque, la Corte - preso atto che i vari diritti della personalità tutelano un unico nucleo, cioè il valore della persona umana - adotta una visione monista dei diritti della personalità. Può essere utile rilevare, per comprendere l'urgenza di questa chiarificazione, che la maggior parte della dottrina si è soffermata negli anni precedenti alla sentenza in oggetto proprio sulla contraddittorietà della pronuncia del 1985 (citato “caso Veronesi”) su questo punto⁹³.

Come esposto, il dibattito in quegli anni si stava concentrando sul fondamento costituzionale del nuovo diritto all'identità personale e sul carattere “chiuso” o “aperto” del catalogo dei diritti e delle libertà fondamentali. Il nodo centrale della

⁹³ Per una ricostruzione del dibattito si veda, ancora, G. Pino, *Il diritto all'identità personale*, cit., 124.

questione riguardava, poi, proprio l'adesione, nella concezione dei diritti della personalità, alla teoria pluralista o monista⁹⁴. Questa scelta influisce direttamente sull'interpretazione del diritto all'identità personale.

In base all'approccio pluralista, infatti, i diritti della personalità sono specifici e chiaramente definiti dal legislatore⁹⁵. Al contrario, l'approccio monista sostiene l'esistenza di un unico diritto generale alla personalità, che può essere declinato in varie manifestazioni⁹⁶.

4. Gli sviluppi successivi della giurisprudenza costituzionale e i corollari del diritto all'identità personale.

In seguito a tale pronuncia, il diritto all'identità personale - entrato definitivamente a far parte della cultura giuridica nazionale e, come si vedrà, anche sovranazionale - è stato sempre più evocato dalla giurisprudenza nelle sue declinazioni più varie.

Già dall'analisi delle sentenze citate emergono almeno due volti dell'identità, uno esterno e uno interno. Il primo è quello delineato - nel 1985 - dalla Corte di Cassazione come diritto a essere rappresentati correttamente nella propria dimensione sociale. Il secondo attiene a una prospettiva più introspettiva ed è quello delineato dalla Corte costituzionale nella sentenza n. 13 del 1994 come diritto a essere sé stessi⁹⁷.

Nell'evoluzione giurisprudenziale e legislativa successiva, in ogni caso, il diritto all'identità personale ha via via assunto una connotazione ancor più "pluridimensionale"⁹⁸.

Considerata l'espansione dell'oggetto di tale diritto, di seguito si proverà - in parte grazie alle classificazioni già proposte dalla dottrina più recente e in parte distaccandosi dalle stesse con ricostruzioni alternative - ad effettuare una sintesi dei diritti che nel tempo sono stati ricondotti all'identità personale.

Si tratta, in particolare del: *diritto al [cog]nome come espressione del diritto all'identità personale; diritto al [cog]nome come espressione dell'ascendenza familiare; diritto alla verità biologica; diritto all'identità sessuale; diritto all'identità di genere; diritto al fine-vita.*

⁹⁴ Per una disamina delle teorie monista e pluralista v. G. Pino, *Teorie e dottrine dei diritti della personalità. Uno strumento di meta-giurisprudenza analitica*, in Aa.Vv., *Materiali per una storia della cultura giuridica*, 2003, 1 ss.

⁹⁵ Si veda, anzitutto, P. Rescigno, voce *Personalità* (diritti della), in *Enc. giur.*, vol. XXIV, Roma, 1991, 6 ss.; nonché A. De Cupis, *I diritti della personalità*, cit., 41 ss.

⁹⁶ Tra i molteplici contributi si ricordino, in particolare, gli studi di P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972; nonché di V. Zeno-Zencovich, *Onore e reputazione nel sistema del diritto civile: uno studio comparato*, Napoli, 1985.

⁹⁷ Sulla distinzione tra le due accezioni v. L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit.; G. Pino, *Identità personale*, cit., 301, ove l'A. si sofferma sulla possibilità di ricondurre questa distinzione a quella tra l'accezione civile e costituzionale del diritto di identità personale.

⁹⁸ A. Morelli, *Persona e identità personale*, cit., 45.

Per completezza, ci si soffermerà anche su diritti ricondotti all'identità personale dal legislatore o dalla dottrina. Ci si riferisce al: *diritto alla protezione dei dati personali* e al *diritto all'oblio*. In questo senso, si parla comunemente di “diritti di identità personale” invece che di “diritto di identità personale”⁹⁹.

Come anticipato, si dedicherà nel prosieguo, invece, un autonomo e più ampio approfondimento al tema dell'identità digitale¹⁰⁰.

Non ci soffermerà, infine, sulla giurisprudenza non costituzionale, anche interessante e copiosa, che ha continuato a svilupparsi negli anni sul tema.

4.1. Il diritto al nome quale manifestazione dell'identità personale.

La relazione tra nome e identità personale attiene alla “genealogia stessa” del concetto di identità personale¹⁰¹ e ciò viene ben presto in rilievo nella dimensione nazionale e sovranazionale¹⁰².

A distanza di due anni e sulla scorta della citata sentenza n. 13 del 1994, la Consulta, con sentenza 23 luglio 1996, n. 297, ha dichiarato l'illegittimità dell'art. 262 del codice civile - per violazione del diritto fondamentale all'identità personale, sempre in riferimento all'art. 2 della Costituzione - nella parte in cui non prevedeva la possibilità per il soggetto di mantenere il cognome attribuitogli dallo stato civile quale segno distintivo della propria identità personale a fronte del riconoscimento della madre naturale intervenuto circa quarant'anni dopo il parto.

Con sentenza 11 maggio 2001, n. 120, poi, la Corte, utilizzando sempre il parametro del diritto all'identità personale ai sensi dell'art. 2 Cost., dichiara l'illegittimità costituzionale del secondo comma dell'art. 299 c.c., nella parte in cui prevedeva che l'adottato figlio naturale non riconosciuto dai propri genitori assumesse

⁹⁹ In questo senso v. F. Modugno, *I “nuovi diritti” nella giurisprudenza costituzionale*, cit.; C. Colapietro, M. Ruotolo, *Diritti e Libertà*, cit. Non si concorda con la diversa lettura del diritto all'identità personale proposta da G. Alpa, *Il diritto di essere sé stessi*, cit., 227. L'Autore, infatti, riduce il dibattito che si è svolto sul tema in ambito costituzionale, concludendo che “*diritto all'identità personale significa “diritto alla propria identità ideale”, il diritto cioè ad essere rappresentati per quel che si è, con i propri valori, le proprie idee, la propria storia*”. Aggiunge, poi, che “*è così facile cadere in errore e scambiare questo specifico diritto con gli altri diritti della personalità che nella raccolta delle massime della Corte di Cassazione effettuata dall'Ufficio del Massimario si equivoca sul punto, scambiando il diritto all'identità personale per l'appunto con il diritto al nome, il diritto a conoscere le proprie origini, il diritto ad affermare la propria identità sessuale, e così via*”. Al contrario, anche a voler attualmente effettuare una distinzione tra diritto all'identità personale e altri diritti della personalità, non può non rilevarsi che storicamente si sono susseguite diverse ricostruzioni di dottrina e giurisprudenza che hanno definito diversamente il diritto all'identità personale. Anche nella giurisprudenza più recente si tratta, più che altro, di diverse declinazioni dello stesso diritto.

¹⁰⁰ Cfr. cap. II.

¹⁰¹ G. Pino, *Identità personale*, cit.

¹⁰² Analogamente a quanto avviene per il diritto all'identità personale, il diritto al nome non è esplicitamente sancito dalla CEDU. Tuttavia, la Corte EDU ha progressivamente ricondotto tale diritto nell'ambito della protezione della vita privata. Si veda, tra le prime pronunce in questo senso, la sentenza di Corte EDU *Burghartz c. Svizzera* del 22 febbraio 1994.

solo il cognome dell'adottante, perdendo, quello originariamente imposto dall'ufficiale di stato civile. In questo caso, la Corte ha inteso il diritto all'identità personale come garanzia del diritto al nome in quanto principale segno distintivo dell'identità della persona. Riscontra, in particolare, una violazione del diritto all'identità personale in ragione del fatto che il soggetto ha sempre utilizzato quel cognome di cui lo si vuole privare, che è divenuto, di conseguenza, un segno distintivo nel contesto sociale in cui opera. Occorre precisare, però, che nel caso deciso con sentenza 120 del 2001, la Corte, nel dichiarare l'illegittimità del secondo comma dell'art. 299 c.c., ha affermato, con riferimento al primo, che *“la precedenza del cognome dell'adottante non appare irrazionale, così come non può costituire violazione del diritto all'identità personale il fatto che il cognome adottivo preceda o segua quello originario. La lesione di tale identità è ravvisabile nella soppressione del segno distintivo, non certo nella sua collocazione dopo il cognome dell'adottante”*.

Si può sintetizzare, dunque, che nei casi appena citati sono stati valorizzati due elementi: quello relazionale (di cui si è detto) e quello temporale. Il trascorrere del tempo - come si è già rilevato con riferimento alla sentenza n. 13 del 1994 - contribuisce a consolidare l'identità della persona e diventa motivo che giustifica l'esigenza di mantenere il cognome che si è sempre utilizzato, nonostante intervengano vicende modificative dello *status* personale capaci di incidere sul cognome stesso¹⁰³.

La Corte è tornata di recente e a distanza di diversi anni sulla questione, pronunciandosi su una vicenda che riguarda il cognome dell'adottato maggiorenne e l'irragionevolezza dell'automatismo nella sua determinazione. Con sentenza n. 135 del 2023, in particolare, dichiara questa volta l'illegittimità costituzionale dell'art. 299, primo comma, del Codice civile, nella parte in cui preclude all'adottando maggiorenne la possibilità di anteporre il suo originario cognome a quello dell'adottante¹⁰⁴.

Nel caso di specie, come rilevato dal giudice rimettente, *“il regime di collocazione dei cognomi riguardava una persona di 39 anni che, nel corso della sua vita, ha avuto modo di stratificare il senso della propria identità nella consapevolezza personale e nei rapporti sociali. Ad avviso del rimettente, dunque, l'ineludibile anteposizione del cognome dell'adottante avrebbe determinato una violazione*

¹⁰³ Cfr. G. Pino, *Identità personale*, cit., 306, rileva che, nella ricostruzione delle sentenze in oggetto, *“Si trattava di fattispecie nelle quali un soggetto, in maniera del tutto indipendente dalla propria volontà e per effetto di una meccanica applicazione di norme di legge si sarebbe trovato ad essere privato del proprio nome, dopo esserne stato titolare per un apprezzabile periodo di tempo”*. Pare opportuno osservare, poi, che l'elemento temporale viene valorizzato anche dalla giurisprudenza della Corte europea dei diritti dell'uomo. Si veda, in proposito, Corte EDU, *Daróczy c. Ucraina*, 1° luglio 2008 e Id., *Künsberg Sarre c. Austria*, 17 gennaio 2023.

¹⁰⁴ Per una ricostruzione approfondita cfr. L. Bartolucci, *L'anteposizione del cognome dell'adottante a quello dell'adottato maggiore d'età. Nota a Corte cost., sentenza n. 135 del 2023*, Osservatorio cost., n. 2/2024, 1 ss.

del diritto all'identità personale e si porrebbe in contrasto con il principio della libertà di scelta, valorizzato dalla più recente giurisprudenza costituzionale”.

La Corte, dopo aver ricostruito l'importanza del cognome e i motivi della sua tutela, nonché l'evoluzione della giurisprudenza fino a quel momento, si sofferma proprio sulle sentenze citate in cui aveva avuto modo di pronunciarsi sull'art. 262 cod. civ. (sentenza n. 297 del 1996) e sull'art. 299, secondo comma, cod. civ. (sentenza n. 120 del 2001).

È interessante che, ad avviso della Corte, il minimo comun denominatore di entrambe sarebbe la valorizzazione di un diritto al nome come espressione del diritto ad essere sé stessi e all'identità negli anni costruita e manifestata nell'ambito della società, anche indipendentemente dalle implicazioni familiari. In particolare, afferma che: *“il diritto al nome, nel divenire autonomo segno distintivo dell'identità personale, attrae una tutela che finisce per poter prescindere dalla correlazione con lo status filiationis. Il cognome originario, intorno al quale si sia venuta a costruire l'identità della persona, va protetto anche ove sia stato assegnato dall'ufficiale di stato civile, in difetto del riconoscimento del figlio da parte dei genitori. E ancora: “se quel cognome si è oramai «radicato nel contesto sociale in cui [l'interessato] si trova a vivere», e magari è stato anche «trasmesso ai [...] figli», precludere «di mantenerlo si risolve in un'ingiusta privazione di un elemento della sua personalità, tradizionalmente definito come il diritto “ad essere sé stessi””.*

La Corte ricorda anche che nel citato caso di cui alla sentenza n. 120 del 2001, la stessa aveva ridimensionato l'incidenza dell'ordine dei cognomi rispetto al diritto all'identità personale ma, a distanza di oltre vent'anni da quella pronuncia, si sente in dovere di riesaminare la questione del contrasto dell'art. 299, primo comma, Cost. con gli artt. 2 e 3 Cost., sia alla luce della diversa questione rimessa al suo scrutinio che dell'evoluzione dell'istituto dell'adozione nel frattempo avvenuta¹⁰⁵.

In questo caso, il giudice *a quo*, in effetti, non mette in discussione la regola di fondo definita dal Legislatore dell'anteposizione del cognome dell'adottante a quello dell'adottando ma ravvisa - ove si tratti dell'adozione della persona maggiore d'età - una irragionevolezza nella automaticità e rigidità del meccanismo, che sacrifica aprioristicamente il diritto all'identità personale dell'adottando. Ebbene, la Corte rileva, contrariamente a quanto fatto nel 2001, che *“l'ordine con cui il cognome dell'adottante si unisce a quello dell'adottato maggiore d'età incide sul diritto all'identità personale di quest'ultimo, che è associato al suo originario co-*

¹⁰⁵ Cfr. § 7.2. della sentenza in esame ove si legge che *“Del resto, che un meccanismo rigido nella determinazione dell'ordine di attribuzione del cognome dell'adottante all'adottato maggiore d'età sia lesivo degli artt. 2 e 3 Cost. è ulteriormente avvalorato dalla considerazione che l'istituto dell'adozione della persona maggiore d'età è in grado attualmente di abbracciare ipotesi varie e differenziate. Risulta allora evidente come proprio la latitudine dell'istituto – esemplificativamente evocata – renda ulteriormente palese l'irragionevolezza di una regola priva di un margine di flessibilità. La rigidità di una previsione insensibile alle esigenze di tutela del diritto alla identità personale dell'adottando rischia di frapporre irragionevoli ostacoli a talune delle funzioni che l'istituto svolge a livello sociale, oltre chiaramente a ledere la stessa identità personale”.*

gnome”. Aggiunge che *“il medesimo ordine condiziona il rilievo attribuito al frammento di identità dell’adottante – il suo cognome – che viene assunto dall’adottato, onde rappresentare il nuovo vincolo giuridico”*.

Ne consegue che *“se l’adottato maggiore d’età ha esigenza di veder tutelato il suo diritto all’identità personale attraverso l’aggiunta, in luogo della anteposizione, del cognome dell’adottante al proprio e se anche l’adottante è favorevole a tale ordine, che non incide sul suo consenso all’adozione, è irragionevole non consentire che la sentenza di adozione possa disporre il citato effetto”*.

La Corte conclude, dunque, che è irragionevole e lesivo dell’identità personale, e, dunque, contrario agli artt. 2 e 3 Cost., non consentire al giudice – con la sentenza che fa luogo all’adozione – di aggiungere, anziché di anteporre, il cognome dell’adottante a quello dell’adottato maggiore d’età, se entrambi nel manifestare il consenso all’adozione si sono espressi a favore di tale effetto.

4.2. Il diritto al nome quale espressione dell’ascendenza familiare.

Con sentenza 28 novembre 2002, n. 494, la Corte costituzionale ha dichiarato l’illegittimità costituzionale degli artt. 278 comma 1 e 251 comma 1 c.c., nella parte in cui escludevano il riconoscimento dei figli nati da rapporti incestuosi.

Come anticipato, si ritrova in questa pronuncia un’ennesima declinazione dell’identità personale in quanto, nel caso di specie, non si tratta tanto della modifica o eliminazione di un elemento che nel tempo è divenuto un tratto identificativo nel contesto sociale, quanto dell’esigenza di allineare l’identità reale dei figli incestuosi e l’identità giuridica. La mancanza del riconoscimento incide sul profilo dell’identità, privando il minore di un aspetto fondamentale della sua personalità. Per dirlo con le parole della Corte, il figlio ha diritto *“al riconoscimento formale di uno status filiationis il quale è un elemento costitutivo dell’identità umana”*.

C’è chi ha ricondotto questo filone a quello appena esposto relativo al diritto al cognome come espressione del diritto all’identità personale (cfr. § 4.1.)¹⁰⁶.

Si ritiene, però, più condivisibile l’orientamento secondo il quale la Corte, nel caso di specie, non ha definito l’identità personale come il diritto ad essere sé stesso e al rispetto di quello che è il proprio patrimonio di idee, di esperienze e di convinzioni, proteggendone di conseguenza – come fatto nelle altre sentenze – il primo e

¹⁰⁶ Cfr. G. Pino, *Identità personale*, cit., 307, in cui, secondo una ricostruzione diversa, si legge *“Non troppo dissimili, infine, le censure di incostituzionalità che hanno dato luogo alle successive pronunce della Corte costituzionale 11 maggio 2001, n. 120, e 28 novembre 2002, n. 494. In tali casi, la variazione sul tema della titolarità del nome dipendeva dalla condizione di figlio adottivo in un caso, e di figlio «incestuoso» nell’altro”*.

più immediato segno distintivo, il nome, in quanto segno identificativo della personalità¹⁰⁷; ha utilizzato, invece, l'identità personale per enucleare il diritto, la garanzia ad un "status filiationis", che implica un diritto al nome identificativo non della personalità dell'individuo ma dell'ascendenza familiare¹⁰⁸.

Diversa vicenda in cui però si fa riferimento alla tutela dell'identità personale del figlio per il tramite del diritto al nome è quella che ha riguardato l'attribuzione allo stesso anche del cognome materno. In realtà, è utile precisare che, come rilevato da autorevole dottrina, la questione della trasmissione del cognome materno racchiude in sé due distinte pretese: l'uguaglianza dei coniugi nella trasmissione del proprio cognome e il diritto all'identità personale del minore che si sostanzia nel vedersi attribuito il cognome di entrambi i genitori¹⁰⁹.

Con riferimento a quest'ultimo profilo, secondo la Corte, la selezione della sola linea parentale paterna oscura unilateralmente il rapporto genitoriale con la madre, provocando – nel riconoscimento contemporaneo del figlio – l'invisibilità della donna. Pertanto, l'automatismo imposto si traduce in una diseguaglianza fra i genitori, che si riverbera e si imprime sull'identità del figlio, così determinando la contestuale violazione degli artt. 2 e 3 Cost.

In questo senso, la Corte, da ultimo, con sentenza n. 131 del 2022, ha affermato che il figlio - nel caso in cui ci sia stato il riconoscimento contemporaneamente di entrambi i genitori - assume sia il cognome del padre che quello della madre, salvo accordo diverso degli stessi.

4.3. Il diritto alla "verità biologica" nella costruzione della identità individuale.

Ancora diversa è l'accezione utilizzata dalla Corte in altre occasioni.

Nella sentenza n. 170. del 10 maggio 1999, prima di una lunga serie sul tema, la Consulta afferma, in particolare, che "*la verità biologica*¹¹⁰ *della procreazione si*

¹⁰⁷ Cfr. E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit., 50.

¹⁰⁸ Cfr. D. Tega, *La giurisprudenza costituzionale sul diritto al nome e all'identità personale. Il caso dei figli incestuosi*, in C. Honorati (a cura di), *Diritto al nome e all'identità personale nell'ordinamento europeo*, Milano, 2010, 75 ss.; G. Di Lorenzo, *La dichiarazione giudiziale di paternità e maternità naturale dei figli nati da rapporto incestuoso*, in *Giur. cost.*, 2003, 1 ss.

¹⁰⁹ Si veda in proposito L. Santoro, *L'attribuzione del cognome ai figli: dalla discrezionalità del legislatore...alla discrezionalità dei genitori (considerazioni controcorrente a partire dalla ord. n. 18/2021 della Corte costituzionale)*, in *Consulta online*, n. 2/2021, 548 ss.

¹¹⁰ E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit., 53, parla più che di "verità" di "identità biologica", come quella "idonea a identificare e distinguere la persona dagli altri individui" e come "diritto a conoscere le alle proprie origini in base ai propri dati genetici". Similarmente cfr. G. Alpa in *Il diritto a essere sé stessi*, cit., 244, ove parla di "identità genetica", declinandola nella duplice accezione di: *i*) il diritto dell'individuo a conoscere il proprio patrimonio genetico (diritto all'informazione); *ii*) diritto dell'individuo alla conservazione del proprio patrimonio genetico, e quindi alla prevenzione delle manipolazioni genetiche.

*è ritenuta una componente essenziale dell'interesse del medesimo minore, riconoscendosi espressamente l'esigenza di garantire al figlio il diritto alla propria identità e precisamente all'affermazione di un rapporto di filiazione veridico*¹¹¹.

Qui, come è evidente, non si tratta solo del diritto ad essere sé stessi o ad essere correttamente rappresentati ma a sapere chi si è e da dove si viene, oltre a poterlo affermare pubblicamente.

Come rilevato da autorevole dottrina, in altre parole, mentre con riferimento ai casi citati relativi al diritto al cognome, *“la Corte ha utilizzato il paradigma dell'identità personale con sguardo, per così dire, rivolto al futuro, ossia rivolto all'esigenza che un soggetto continui ad utilizzare un nome ritenuto ormai stabilmente evocativo della sua identità (come complesso di esperienze di vita, ecc.), in questo tipo di casi invece il paradigma dell'identità personale è, per così dire, rivolto al passato, cioè alla possibilità per una persona di ricostruire le proprie origini biologiche (che certo non appartengono al suo patrimonio di esperienze culturali ecc., visto che fino a quel momento non ne era nemmeno a conoscenza: la biologia non è biografia)*¹¹².

La Corte costituzionale, dunque, si spinge a riconoscere un concetto di identità personale che si configura in termini soggettivi, ponendo l'accento sulla formazione dell'identità psico-fisica dell'individuo. Questo approccio sembra prescindere, in parte, anche dalla dimensione relazionale, concentrandosi primariamente sull'accurata costruzione del sé e della propria storia¹¹³.

Del resto, in questi casi non si discute del segno distintivo esterno per antonomasia cioè il cognome e, peraltro, come correttamente rilevato dalla Corte, la dimensione sociale dell'identità spesso viene sacrificata a favore della verità. In questo senso, nella citata sentenza, si legge che *“certamente il perseguimento del valore verità determina il sacrificio della posizione familiare, affettiva e socio-economica acquisita medio tempore dal figlio; tuttavia, la sofferenza del figlio legittimo consapevole dell'apparenza solo formale del proprio status, contro la quale nessuno dei soggetti legittimati abbia reagito, non è meno grave e profonda rispetto a quella di chi sia posto innanzi alla verità della procreazione”*.

Questa impostazione sottolinea la rilevanza della verità biologica e storica nella costruzione dell'identità personale, attribuendo al singolo individuo il potere di conoscere e comprendere le proprie radici come parte integrante e inalienabile del suo sviluppo e della sua realizzazione personale.

¹¹¹ Cfr. anche Corte cost., 9 aprile 1997, n. 112 e 19 giugno 1997, n. 216.

¹¹² G. Pino, *Identità personale* cit.

¹¹³ Anche I. Carlotto, *La ricerca delle proprie origini nel bilanciamento dei diritti*, Napoli, 2020, XII, parla, in proposito, di “identità biologica”.

In questo senso, va anche la nota sentenza n. 278 del 2013, con cui la Corte costituzionale ha dichiarato l'illegittimità dell'art. 28, comma 7, della legge sull'adozione n. 184 del 1983, nella parte in cui non prevedeva la possibilità per il giudice d'interpellare la madre che avesse dichiarato di non voler essere nominata, ai fini di un'eventuale revoca di tale dichiarazione. In tale pronuncia afferma che *“il diritto del figlio a conoscere le proprie origini – e ad accedere alla propria storia parentale – costituisce un elemento significativo nel sistema costituzionale di tutela della persona, come pure riconosciuto in varie pronunce della Corte europea dei diritti dell'uomo. E il relativo bisogno di conoscenza rappresenta uno di quegli aspetti della personalità che possono condizionare l'intimo atteggiamento e la stessa vita di relazione di una persona in quanto tale”*.

La giurisprudenza nazionale e sovranazionale¹¹⁴ che si è sviluppata negli anni su questo specifico profilo, però, è piuttosto variegata, in quanto, a fronte dell'indubbio valore della verità biologica, spesso emergono, in questo tipo di situazioni, anche altri interessi costituzionalmente garantiti e la Corte si è trovata, di volta in volta, a fare un bilanciamento¹¹⁵.

A tale proposito, con sentenza n. 272 del 2017, la Consulta, riaffermando che *“la verità biologica costituisce una componente essenziale dell'identità personale del minore, la quale concorre, insieme ad altre componenti, a definirne il contenuto”*, ha precisato che *“pur dovendosi riconoscere un accentuato favore dell'ordinamento per la conformità dello status alla realtà della procreazione, va escluso che quello dell'accertamento della verità biologica e genetica dell'individuo costituisca un valore di rilevanza costituzionale assoluta, tale da sottrarsi a qualsiasi bilanciamento”*¹¹⁶.

¹¹⁴ Cfr., in particolare, Corte EDU, *Gaskin c. Regno Unito*, 7 luglio 1989.

¹¹⁵ Cfr., L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 34; nonché, G. Matucci, *La dissoluzione del paradigma della verità della filiazione innanzi all'interesse concreto del minore* (Nota a Corte cost., 18 dicembre 2017, n. 272), in *Forumcostituzionale.it*, 15 febbraio 2018.

¹¹⁶ La questione di costituzionalità in esame è sorta nell'ambito di un procedimento di impugnazione di una sentenza emessa dal Tribunale di Milano ove il giudice ordinario, accogliendo la domanda avanzata dal curatore speciale di un minore nominato dal Tribunale per i minorenni, aveva stabilito che il minore, nato tramite surrogazione di maternità con ovodonazione, non fosse figlio della donna che lo aveva riconosciuto. A seguito di tale decisione, la Corte d'Appello di Milano sollevava questione di legittimità costituzionale relativa all'art. 263 c.c., che disciplina l'impugnazione del riconoscimento per difetto di veridicità. La Corte d'Appello ha contestato la mancata previsione, nella norma, che tale azione potesse essere accolta solo allorquando rispondente all'interesse del minore. Nel dichiarare infondata la questione, la Corte costituzionale n. 278/2013 ha precisato che l'interesse del minore è già considerato dalla normativa vigente e che, nell'ambito dell'azione prevista dall'art. 263 c.c. (ad eccezione di quella proposta dal figlio stesso), il giudice è tenuto a svolgere una valutazione complessa, in cui l'interesse del minore potrebbe risultare secondario rispetto ad altri interessi di rilievo nel caso concreto. La Corte ha ulteriormente sottolineato che le variabili da considerare sono “molto più complesse della rigida alternativa vero o falso”. Tra queste, rivestono particolare rilievo, oltre alla durata del rapporto instauratosi con il minore e alla condizione identitaria acquisita, le modalità del concepimento e della gestazione, nonché la disponibilità di strumenti legali che permettano la costituzione di un legame giuridico con il genitore contestato, come l'adozione in casi particolari, che possa garantire al minore un'adeguata tutela.

Anche con successiva sentenza n. 127 del 2020 la Corte afferma che il bilanciamento tra il *favor veritatis* e l'interesse del minore non possa essere condotto in astratto, sacrificando a priori uno dei due valori. Il giudice deve operare in ciascun caso una concreta valutazione degli interessi in gioco, tenendo in considerazione che il diritto all'identità personale non si sostanzia solamente nella verità biologica, ma anche nei legami affettivi e personali sviluppatisi all'interno della famiglia.

Rilevanti sul tema sono anche le sentenze nn. 32 e 33 del 2021. In questi diversi casi la Corte afferma che la mancanza di meccanismi volti a riconoscere il vincolo di filiazione nei confronti del genitore non biologico per i minori nati all'estero da tecniche di procreazione medicalmente assistita o da gestazione per altri comportamenti una lesione dell'identità del minore, che emerge e si forma dalla relazione quotidiana e dal rapporto di cura.

4.4. Il diritto all'identità sessuale e il diritto all'identità di genere.

Una storia più tortuosa ha avuto il diritto all'identità sessuale, intesa come il diritto al riconoscimento della propria caratterizzazione sessuale¹¹⁷. Si tratta di una componente molto importante della persona, della sua identità, della sua verità, anche al di là delle apparenze fisiche¹¹⁸.

Proprio dal disallineamento tra apparenza estetica e percezione sostanziale di sé stessi emerge l'ulteriore declinazione “dell'identità di genere”¹¹⁹. Il concetto si fonda sulla distinzione tra sesso e genere: il sesso riguarda le caratteristiche biologiche, mentre il genere rimanda alla percezione del proprio essere sessuato, modellata da elementi culturali, storici e sociali. In questa prospettiva, l'identità di genere corrisponde alla percezione che ogni individuo ha di sé e del proprio ruolo di genere; di conseguenza, il diritto all'identità di genere comporta la richiesta di un riconoscimento giuridico di tale percezione¹²⁰.

Come affermato da Guido Alpa, il “*diritto al gender va al di là del diritto all'identità personale (cioè all'identità ideale) perché demistifica l'idea di natura*

¹¹⁷ Diversa è, invece, la “libertà sessuale”, qualificata da Corte cost. 10 dicembre 1987, n. 561 quale diritto fondamentale riconducibile all'art. 2 Cost. in quanto essenziale modo di espressione della persona umana. Ad avviso della Corte, dunque, “il diritto di disporre liberamente è senza dubbio un diritto soggettivo assoluto, che va ricompreso tra le posizioni soggettive direttamente tutelate dalla Costituzione ed inquadrato tra i diritti inviolabili della persona umana che l'art. 2 Cost. impone di garantire”.

¹¹⁸ E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit., 52. In ordine alla tesi che avvalorata una trattazione congiunta delle tematiche dell'identità sessuale e di quella personale v. anche G. Pino, *Identità personale*, cit., spec. 300 ss.

¹¹⁹ Per un approfondimento sul tema cfr. G. Mingardo, *Il riconoscimento delle nuove soggettività e il limite del binarismo di genere nella prospettiva costituzionale*, in *GenIUS*, 24 settembre 2024, 1 ss. Sul fondamento costituzionale dell'identità di genere v. A. Astone, *Il controverso itinerario dell'identità di genere*, in *Nuova giur. civ. comm.*, 2016, 315 ss.

¹²⁰ Così F. Bilotta, *Transessualismo* voce, in *Dig. disc. priv.*, VIII Agg., Torino, 2013, 732 ss.; nonché, A. Lorenzetti, *Diritti in transito*, Milano, 2013, 19 ss.; A.C. Visconti, *Oltre la logica binaria...L'identità di genere tra vecchie e nuove prospettive*, in *Federalismi.it*, n. 15/2023, 240 ss.

*che per millenni i giuristi hanno codificato e considera la persona come un unicum composto di corpo e psiche, dando prevalenza all'atto di autodeterminazione del singolo che, assecondando le sue inclinazioni naturali, manifesta la volontà di cambiare il sesso corporeo-anagrafico nell'altro sesso psicologicamente più consono*¹²¹.

Tanto era codificata la “natura” che tale diritto è stato inizialmente espressamente negato. Con sentenza n. 98 del 1 agosto 1979, in particolare, la Corte aveva escluso l'illegittimità delle norme che non riconoscevano il diritto alla rettificazione dell'atto di nascita e - nel caso di specie - alla attribuzione del sesso femminile “*nell'ipotesi di modificazioni artificiali di un sesso che facciano perdere ad un individuo le caratteristiche peculiari maschili ed acquistare quelle femminili esterne, qualora le modificazioni stesse trovino corrispondenza in una originaria, indiscutibile, personalità psichica di natura femminile*”. In quella occasione, aveva affermato, infatti, che “*così delimitata la materia, la Corte ritiene che le norme costituzionali invocate non pongano fra i diritti inviolabili dell'uomo quello di far riconoscere e registrare un sesso esterno diverso dall'originario, acquisito con una trasformazione chirurgica per farlo corrispondere a una originaria personalità psichica*”¹²².

Qualche anno dopo, però, è intervenuto il Legislatore con Legge 14 aprile 1982, n. 164, rubricata, “*Norme in materia di rettificazione di attribuzione di sesso*”. L'art. 1, tutt'ora vigente, recita che “*La rettificazione si fa in forza di sentenza del tribunale passata in giudicato che attribuisca ad una persona sesso diverso da quello enunciato nell'atto di nascita a seguito di intervenute modificazioni*”.

¹²¹ G. Alpa, *Il diritto di essere sé stessi*, cit., 248.

¹²² In proposito pare di interesse il ragionamento di Corte cost. 1° agosto 1979, n. 98, che aderisce all'interpretazione dell'art. 2 come norma a “*fattispecie chiusa*”. Nella pronuncia si legge, in particolare, che “*Posto, infatti, nei suoi termini reali, e perciò impropriamente definito come relativo al riconoscimento della “identità sessuale”, il problema, che non coinvolge, come si è detto, la libertà del comportamento sessuale, può suscitare in Italia, come in altri Paesi, l'attenzione del legislatore sulle sue possibilità di soluzione e i relativi limiti in ordine al matrimonio, che la Costituzione definisce fondamento della famiglia come “società naturale”, ma non può essere risolto in termini di costituzionalità delle norme impugnate. Infatti, nella costante interpretazione della Corte, l'invocato art. 2 della Costituzione, nel riconoscere i diritti inviolabili dell'uomo, che costituiscono patrimonio irretrotrattabile della sua personalità, deve essere ricollegato alle norme costituzionali concernenti singoli diritti e garanzie fondamentali (sentenze nn. 11/1956, 29/1962, 1, 29 e 37/1969, 102 e 238/1975), quantomeno nel senso che non esistono altri diritti fondamentali inviolabili che non siano necessariamente conseguenti a quelli costituzionalmente previsti. Ora dalla Costituzione non è possibile desumere una tutela di quel diritto cui richiamavasi l'attore in giudizio e che il giudice a quo - riconoscendolo sprovvisto di tutela nella legge ordinaria - ha ritenuto potesse essere compreso fra i diritti inviolabili dell'uomo. Ne consegue la infondatezza del richiamo non solo all'art. 2, ma anche all'art. 24 della Costituzione: il quale ultimo garantisce la possibilità di agire in giudizio per la tutela dei diritti e interessi legittimi e non può quindi essere utilmente invocato dove si tratti, come nella specie, non della (incontestata) possibilità di azione, ma dell'esistenza o inesistenza del diritto sostanziale.*”

dei suoi caratteri sessuali". Molto si è discusso sul significato della locuzione "*intervenute modificazioni dei suoi caratteri sessuali*". Ciò che è certo è che tale novella normativa fornisce un appiglio per il riconoscimento del fatto che l'identità sessuale è il risultato della commistione tra la componente fisica e psicologica.

Ebbene, questa novità normativa, dunque, porta la Corte a un cambio di rotta anche più radicale di quanto ci si aspettasse alla luce dell'orientamento assunto giusto pochi anni prima.

La Corte, infatti, ha il pregio di accogliere - con un approccio più lungimirante - anche i casi di c.d. "transessualismo", nei quali, sulla base di una dichiarata psico-sessualità in contrasto con la presenza di organi dell'altro sesso, si intervenga con operazioni demolitorie e ricostruttive per consentire al soggetto l'appartenenza al sesso opposto, in riferimento agli artt. 2 e 32 Cost.

Con sentenza n. 161 del 1985, la Corte ha rilevato, infatti, che il Legislatore ha previsto, con l'introduzione della predetta disciplina, "*un concetto di identità sessuale nuovo e diverso rispetto al passato, nel senso che, ai fini di una tale identificazione, viene conferito rilievo non più esclusivamente agli organi genitali esterni, quali accertati al momento della nascita ovvero "naturalmente" evolutisi, sia pure con l'ausilio di appropriate terapie medico-chirurgiche, ma anche ad elementi di carattere psicologico e sociale. Presupposto della normativa impugnata è, dunque, la concezione del sesso come dato complesso della personalità determinato da un insieme di fattori, dei quali deve essere agevolato o ricercato l'equilibrio, privilegiando – poichè la differenza tra i due sessi non è qualitativa, ma quantitativa – il o i fattori dominanti*".

Ciò porta la Corte a far rientrare a pieno titolo nel patrimonio irretrotrattabile della personalità "*il diritto di realizzare, nella vita di relazione la propria identità sessuale, da ritenere aspetto e fattore di svolgimento della personalità*". Nella stessa occasione, aggiunge anche che, peraltro, "*gli altri membri della collettività sono tenuti a riconoscerlo per dovere di solidarietà sociale*"¹²³.

Si rileva che parte della dottrina, ritiene tale diritto all'identità sessuale emblematico del fatto che la Corte non accoglierebbe la tesi "della fattispecie aperta" e che ciò sarebbe dimostrato dal fatto che, quando invoca l'art. 2, "*si preoccupa di non ricostruire i diritti della persona senza specifici agganci - per lo più esplicitati ma sempre rinvenibili - ai diritti enumerati*"¹²⁴.

Fino a questo momento, comunque, il diritto all'identità di genere era stato ricondotto a quello di identità sessuale. Solo a partire dal 2015 tale diritto è ritenuto *species* del *genus* diritto all'identità personale, anche in linea con l'orientamento assunto dalla Corte europea dei diritti dell'uomo¹²⁵.

¹²³ Cfr., in generale, le annotazioni di P. Stanzione, *Transessualità* voce, in *Enc. dir.*, vol. XLIV, Milano, 1992, 874 s.

¹²⁴ Cfr. F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, cit., 54.

¹²⁵ Cfr., *ex multis*, Corte EDU, *Y. c. Francia*, 31 gennaio 2023; Id., *A.D. e altri c. Georgia*, 1° dicembre 2022; Id., *X. e Y. c. Romania*, 19 gennaio 2021; Id., *S.V. c. Italia*, 11 ottobre 2018; Id.,

Si aggiunge che la Corte, più di recente, si è spinta ad affermare, prima con sentenza n. 221 del 2015¹²⁶ e poi con sentenze nn. 180 e 185 del 2017, che - ai fini della rettifica anagrafica dell'attribuzione di sesso - un'interpretazione costituzionalmente orientata della Legge n. 164 del 1982 porta ad escludere la necessità del ricorso a intervento chirurgico¹²⁷.

In questa prospettiva, dunque, in tali occasioni, ha precisato che la mancanza, nella disciplina legislativa, “di un riferimento testuale alle modalità (chirurgiche, ormonali, ovvero conseguenti ad una situazione congenita), attraverso le quali si realizzi la modificazione, porta ad escludere la necessità, ai fini dell'accesso al percorso giudiziale di rettificazione anagrafica, del trattamento chirurgico, il quale costituisce solo una delle possibili tecniche per realizzare l'adeguamento dei caratteri sessuali”.

Sembra, sul tema, che l'ordinamento italiano sia orientato a un'evoluzione graduale verso il riconoscimento del principio di autodeterminazione nell'ambito delle scelte di genere. In diversi aspetti, in effetti, esso prosegue la traiettoria tracciata dalla sentenza n. 221 del 2015, valorizzando le specificità del percorso individuale della persona e attenuando alcuni degli elementi più autoritativi della disciplina¹²⁸.

A.P., *Garçon e Nicot c. Francia*, 6 aprile 2017; Id., *Y. Y. c. Turchia*, 10 marzo 2015; Id., *Van Kuck c. Germania*, 12 giugno 2003.

¹²⁶ A commento della pronuncia cfr., fra gli altri, A. Nocco, *La rettificazione di attribuzione di sesso tra Corte Costituzionale n. 221/2015 e fonti sovranazionali*, in *Questione Giustizia*, 30 novembre 2015; A. Lorenzetti, *Corte costituzionale e transessualismo: ammesso il cambiamento di sesso senza intervento chirurgico ma spetta al giudice la valutazione*, in *Quad. cost.*, 2015, 1006 ss.; L. Ferraro, *La Corte costituzionale e la primazia del diritto alla salute e della sfera di autodeterminazione*, in *Giur. cost.*, 2015, 2054 ss. C.M. Reale, *Corte costituzionale e transgenderismo: l'irriducibile varietà delle singole situazioni*, in *BioLaw Journal*, n. 1/2016, 283 ss.; A. Spangaro, *Anche la Consulta ammette il mutamento di sesso senza il previo trattamento chirurgico*, in *Fam. dir.*, 2016, 639 ss.; C. Meoli, *La correzione dell'interpretazione sulla correzione del sesso: brevi note a Corte cost., sent. n. 221 del 2015*, in *Giustamm.it*, n. 6/2016, 1 ss.; I. Rivera, *Le suggestioni del diritto all'autodeterminazione personale tra identità e diversità di genere. Note a margine di Corte cost. n. 221 del 2015*, in *Consulta online*, n. 1/2016, 175 ss.; L. Ferraro, *Il giudice nel procedimento di rettificazione del sesso: una funzione ormai superata o ancora attuale?*, in *Questione giustizia*, 2016; P.I. D'Andrea, *La sentenza della Corte costituzionale sulla rettificazione anagrafica del sesso: una risposta e tanti nuovi interrogativi*, in *Giur. cost.*, 2016, p. 263 ss.; P.C. Guarini, *«Maschio e femmina li creò» ... o, forse, no. La Corte costituzionale ancora sulla non necessità di intervento chirurgico per la rettificazione anagrafica di attribuzione di sesso*, in *Federalismi.it*, n. 8/2018, 1 ss.

¹²⁷ Nello stesso senso, da ultimo, la Corte costituzionale si è espressa con le pronunce 10 febbraio 2021 nn. 30 e 31. In dottrina cfr. M. D'Amico, *I diritti dei “diversi”*. Saggio sull'omosessualità, in *Oss. cost.*, 2021, 164 ss.; nonché M.E. Ruggiano, *Il diritto all'identità di genere: preoccupazioni per la decisione della Corte costituzionale nella sentenza n. 180 del 2017*, in *Stato, Chiese e pluralismo confessionale*, n. 41/2017, 1 ss.; I. Rivera, *Le suggestioni del diritto all'autodeterminazione personale tra identità e diversità di genere*, cit., 181.

¹²⁸ Cfr. Corte cost. 23 luglio 2024, n. 143 e, in proposito, il commento di di P. Mezzanotte, *Identità di genere non binaria e altre questioni in una recente pronuncia della Corte costituzionale*, in *Nomos*, 2024, 1 ss.

4.5. L'identità personale nel dibattito sul fine vita.

Un'ulteriore declinazione del diritto all'identità personale emerge in riferimento alla fase finale della vita¹²⁹.

In particolare, in quelle situazioni in cui un soggetto - pur trovandosi ad affrontare sofferenze insopportabili causate da malattie terminali o condizioni di vita gravemente debilitanti e mantenendo le proprie capacità cognitive - non sia nelle condizioni materiali di autodeterminarsi in merito alle modalità e ai tempi di cessazione della sua stessa esistenza¹³⁰.

In effetti, proprio le diverse visioni sui profili legali, etici e religiosi che emergono in siffatte situazioni hanno dato vita ad un acceso dibattito - in varie parti del mondo - sulla legittimità e opportunità di ammettere e regolamentare ipotesi di eutanasia¹³¹. Come in altre vicende della vita, ci troviamo nel campo del biodiritto¹³² nel quale si deve bilanciare il diritto ad autodeterminarsi¹³³ con i valori dell'ordinamento e condivisi dalla collettività di cui si fa parte.

¹²⁹ Per una ricostruzione delle principali tappe storiche e dei profili filosofici che hanno segnato il dibattito sul fine vita e sulla liceità delle condotte eutanasiche cfr. G. Razzano, *Dignità nel morire, eutanasia e cure palliative nella prospettiva costituzionale*, Torino, 2014, 13 ss.; Id., *Sulla sostenibilità della dignità come autodeterminazione*, in *BioLaw*, n. 2/2019, 95 ss.; A. Giubilei, *Discrezionalità legislativa e garanzia della Costituzione*, Roma, 2023, 243 ss.

¹³⁰ A. Morelli, *Persona e identità personale*, cit., 54; nonché, G. Alpa, *Il diritto di essere sé stessi*, cit., 240.

¹³¹ Dal punto di vista etimologico il termine deriva dal greco antico εὐθανασία (euthanasía), che significa “buona morte” o “morte dolce”. L'eutanasia può essere distinta in diverse forme: *i*) eutanasia attiva: Comporta un'azione diretta per causare la morte di una persona, come la somministrazione di un farmaco letale. È considerata eutanasia volontaria se la persona ha espresso il desiderio di morire, oppure involontaria se viene praticata senza il consenso esplicito del paziente (per esempio, perché il paziente è incapace di esprimersi); *ii*) eutanasia passiva: consiste nel rifiuto o nella sospensione di trattamenti medici necessari per mantenere in vita una persona, come la sospensione di un respiratore o la non somministrazione di farmaci salvavita. In questo caso, la morte sopraggiunge per il naturale decorso della malattia o della condizione da cui il paziente è affetto; *iii*) suicidio assistito: In questa pratica, una persona, solitamente un medico, fornisce a un paziente i mezzi necessari per mettere fine alla propria vita, ma è il paziente stesso a compiere l'atto finale. Il suicidio assistito è distinto dall'eutanasia attiva, poiché nel primo caso l'azione decisiva è compiuta dal paziente stesso. Mentre alcuni paesi come i Paesi Bassi, il Belgio e il Canada hanno legalizzato forme di eutanasia, in altri, come l'Italia, rimane illegale, sebbene il suicidio assistito sia stato depenalizzato in determinate circostanze in seguito alla emblematica pronuncia di Corte cost. 25 settembre 2019, n. 242.

¹³² Per una trattazione ad ampio raggio v. G. Alpa, *Il diritto di essere sé stessi*, cit., 239 ss., che analizza le principali pronunce in tema di procreazione assistita e tutela dell'embrione, maternità surrogata, accanimento terapeutico, transessualità, rapporti tra genere, sesso e fisico, espressione delle credenze religiose attraverso la loro rappresentazione simbolica.

¹³³ Sulla possibilità di configurare un diritto costituzionalmente garantito alla morte medicalmente assistita, fondato sul principio di autodeterminazione dell'individuo v. anche D. Neri, *Eutanasia. Valori, scelte morali, dignità delle persone*, Roma-Bari, 1995; H. Jonas, *Il diritto di morire* (1978), *Il Nuovo Melangolo*, Genova, 1997; G. Gemma, *Vita (diritto alla)* voce, in *Dig. IV disc. pubbl.*, vol. XV, Torino, 1999, 671 ss.; S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, 254 ss.; U. Veronesi, *Il diritto di morire. La libertà del laico di fronte alla sofferenza*, Mondadori, Milano, 2005; A. Santosuosso, *Eutanasia, in nome della legge*, in *Micromega*, n. 1/2007, 28 ss.; S. Rodotà, *Nuovi soggetti, nuovi diritti, nuovi conflitti*, in F.G. Pizzetti, M. Rosti (a

Il dibattito sull'eutanasia in Italia ha avuto uno sviluppo lungo e complesso, caratterizzato da una serie di eventi chiave, casi giudiziari emblematici e interventi significativi della Corte costituzionale.

Alcuni casi giudiziari, in particolare, hanno attirato l'attenzione dell'opinione pubblica e hanno messo in luce le lacune della legislazione italiana sul tema del fine-vita¹³⁴.

Con riferimento al noto "caso Englaro", a valle di numerose sentenze emanate da diverse giurisdizioni, è intervenuta la Corte di Cassazione con sentenza n. 21748 del 2007. La Suprema Corte ha statuito che il giudice può autorizzare l'interruzione del trattamento soltanto in presenza di due circostanze concorrenti, cioè: l'irreversibilità della condizione di stato vegetativo della paziente, scientificamente fondata in modo che non vi sia, in base agli standard scientifici internazionalmente riconosciuti, alcuna possibilità di recupero della coscienza e delle capacità di percezione; l'accertamento univoco della volontà della paziente, sulla base di elementi tratti dal vissuto della medesima, dalla sua personalità e dai convincimenti etici, religiosi, culturali e filosofici, circa il rifiuto alla continuazione del trattamento.

Per quanto di interesse in questa sede, si riporta di seguito un passaggio della sentenza in cui la Corte si sofferma sull'art. 2, come fondamento del "consenso informato". Nella pronuncia, si legge, in particolare, che "*Occorre premettere che*

cura di), *Soggetti, diritti, conflitti: percorsi di ridefinizione*, Milano, 2007; G.U. Rescigno, *Dal diritto di rifiutare un determinato trattamento sanitario secondo l'art. 32, comma 2, Cost., al principio di autodeterminazione intorno alla propria vita*, in *Dir. pubbl.*, 2008, 102 ss.; M. Donini, *Antigiuridicità e giustificazione oggi. Una "nuova" dogmatica, o solo una critica per il diritto penale moderno?*, in *Riv. it. dir. proc. pen.*, 2009, 1658 ss.; Id., *La necessità di diritti infelici. Il diritto di morire come limite all'intervento del legislatore penale*, in *Riv. it. med. legale*, 2016, 554 ss.; Id., *Libera nos a malo. I diritti di disporre della propria vita per neutralizzare il male*, in G. D'Alessandro, O. Di Giovine (a cura di), *La Corte costituzionale e il fine vita. Un confronto interdisciplinare sul caso Cappato-Antoniani*, Torino, 2020, 221 ss.; M. Villone, *Il diritto di morire*, Napoli, 2011; S. Staiano, *Legiferare per dilemmi sulla fine della vita: funzione del diritto e moralità del legislatore*, in *Federalismi.it*, n. 9/2012, 9 ss.; G. Gemma, *Dignità ed eutanasia: non c'è antitesi. Note a margine di un'opera recente di una costituzionalista cattolica*, in *Materiali per una storia della cultura giuridica*, n. 1/2016, 253 ss.; G. Maniaci, *Perché abbiamo un diritto costituzionalmente garantito all'eutanasia e al suicidio assistito*, in *Riv. AIC*, n. 2019, 262 ss.; G. Rolla, *Il valore normativo del principio di dignità umana. Brevi considerazioni alla luce del costituzionalismo iberoamericano*, in *DPCE*, 2003, 1880 ss.

¹³⁴ Ci si riferisce, in particolare, a due casi specifici. Viene in rilievo, anzitutto, quello di Eluana Englaro, risalente al 2009. Eluana Englaro era in stato vegetativo permanente dal 1992 a seguito di un grave incidente stradale. Dopo una lunga battaglia legale, nel 2009, il padre ottenne dal Tribunale il permesso di interrompere le pratiche di alimentazione e idratazione artificiali. Questo caso ha aperto un dibattito profondo e divisivo in Italia sul diritto alla morte e sull'autodeterminazione, mettendo in evidenza la mancanza di una legge chiara sul fine vita. Su di un piano non dissimile si colloca, invece, il c.d. caso di DJ Fabo del 2017. Fabiano Antoniani, noto come "DJ Fabo", rimase tetraplegico e cieco a causa di un incidente stradale. Dopo aver espresso ripetutamente il desiderio di porre fine alle sue sofferenze, DJ Fabo si recò in Svizzera, dove la pratica del suicidio assistito è consentita dalla legge, così riaccendendo il dibattito sull'eutanasia in Italia e portando alla luce l'assenza di opzioni legali per coloro che vogliono porre fine alla propria vita in modo dignitoso. Giova evidenziare che è diversa la questione giuridica che si è posta nell'altrettanto noto "caso Welby". In questo caso, il Tribunale di Roma ha dichiarato il non luogo a procedere nei confronti del medico curante, invocando il principio di autodeterminazione, alla luce del fatto che il paziente era, fino alla fine, cosciente e in grado di esprimere la propria volontà.

il consenso informato costituisce, di norma, legittimazione e fondamento del trattamento sanitario: senza il consenso informato l'intervento del medico è sicuramente illecito, anche quando è nell'interesse del paziente; la pratica del consenso libero e informato rappresenta una forma di rispetto per la libertà dell'individuo e un mezzo per il perseguimento dei suoi migliori interessi. Il principio del consenso informato – il quale esprime una scelta di valore nel modo di concepire il rapporto tra medico e paziente, nel senso che detto rapporto appare fondato prima sui diritti del paziente e sulla sua libertà di autodeterminazione terapeutica che sui doveri del medico – ha un sicuro fondamento nelle norme della Costituzione: nell'art. 2, che tutela e promuove i diritti fondamentali della persona umana, della sua identità e dignità; nell'art. 13, che proclama l'invulnerabilità della libertà personale, nella quale "è postulata la sfera di esplicazione del potere della persona di disporre del proprio corpo" (Corte cost., sentenza n. 471 del 1990); e nell'art. 32, che tutela la salute come fondamentale diritto dell'individuo, oltre che come interesse della collettività, e prevede la possibilità di trattamenti sanitari obbligatori, ma li assoggetta ad una riserva di legge, qualificata dal necessario rispetto della persona umana e ulteriormente specificata con l'esigenza che si prevedano ad opera del legislatore tutte le cautele preventive possibili, atte ad evitare il rischio di complicanze"¹³⁵.

Nel 2019, poi, è intervenuta la Corte costituzionale con una storica pronuncia sul tema¹³⁶.

La Corte, in particolare, era chiamata a pronunciarsi sulla questione di legittimità costituzionale dell'art. 580 c.p., relativo al reato di istigazione o aiuto al suicidio. La questione è stata sollevata dalla Corte d'Assise di Milano nel corso di un processo a carico di un uomo accusato di aver aiutato un soggetto tetraplegico e cieco, a seguito di un grave incidente stradale, a recarsi in Svizzera per porre fine alla sua vita tramite suicidio assistito¹³⁷.

In quella occasione, la Corte costituzionale ha dichiarato l'illegittimità costituzionale dell'articolo 580 del c.p. nella parte in cui non esclude la punibilità di chi agevola l'esecuzione del suicidio di una persona che si trovi in condizioni specifiche e a determinate condizioni.

In particolare, le condizioni del richiedente che rendono lecita la prestazione dell'aiuto al suicidio, per come ricostruite dalla Corte, sono: essere tenuto in vita da trattamenti di sostegno vitale; essere affetto da una patologia irreversibile; soffrire di sofferenze fisiche o psicologiche che reputa intollerabili; essere pienamente capace di prendere decisioni libere e consapevoli.

¹³⁵ Cass. civ., sez. I, 16 ottobre 2007, n. 21748, § 6.

¹³⁶ Cfr., ancora, Corte cost. n. 242/2019.

¹³⁷ Per un approfondimento sulla vicenda e sull'ordinanza di remissione, v. A Giubilei, *Discrezionalità legislativa e garanzia della Costituzione*, Roma, 2023, 243 ss.

Le condizioni di liceità dell'aiuto al suicidio, inoltre, sono: la verifica delle condizioni del paziente, da effettuarsi da parte di una struttura pubblica del servizio sanitario nazionale, previo parere del comitato etico territorialmente competente; la presenza di una richiesta esplicita, libera, informata da parte del paziente; che sia stata offerta al paziente la possibilità di accedere a cure palliative, laddove possibile, e che il paziente sia stato adeguatamente informato sulle possibili alternative al suicidio assistito; la scelta delle modalità di esecuzione dell'aiuto, che dovranno essere tali da garantire la minore sofferenza possibile per il paziente.

La Corte ha precisato che tale sentenza non obbliga il personale sanitario a praticare il suicidio assistito, lasciando al singolo medico la libertà di coscienza di scegliere se prestare o meno aiuto al paziente. Ha stabilito, inoltre, che, per i fatti anteriori alla pubblicazione della sentenza, la non punibilità è applicabile solo se l'aiuto al suicidio, pur prestato in assenza delle verifiche e delle procedure ora indicate, sia comunque avvenuto con modalità equivalenti, idonee a offrire garanzie sostanzialmente analoghe e la cui sussistenza dovrà essere verificata dal giudice caso per caso.

Infine, la Corte ha esortato il Parlamento a disciplinare in maniera organica la materia del suicidio assistito, in conformità ai principi enunciati nella sentenza.

Da ultimo, le pronunce n. 135/2024 e n. 66/2025 hanno chiarito e precisato i requisiti per l'accesso al suicidio medicalmente assistito, ribadendo che la non punibilità è condizionata alla sofferenza irreversibile, alla capacità decisionale e, nei casi di dipendenza da trattamenti vitali, alla valutazione medica. Infine, la sentenza n. 132/2025 ha consolidato questa impostazione, confermando che l'ordinamento può accompagnare il paziente nell'esercizio del suicidio assistito senza legittimare l'omicidio del consenziente. Complessivamente, queste decisioni mostrano come la Corte riconosca l'autodeterminazione come componente essenziale dell'identità personale, pur inserendola in un quadro normativo che contempera libertà individuale e valori fondamentali della vita, evidenziando la centralità della scelta consapevole e della dignità del soggetto¹³⁸.

4.6. La protezione dei dati personali e il diritto all'oblio.

Come anticipato, diversa è la storia del diritto alla protezione dei propri dati personali, qui preso in esame esclusivamente come ulteriore declinazione del diritto all'identità personale.

Come visto, infatti, in Italia, si deve alla normativa in materia di protezione dei dati la prima codificazione, pur senza definizioni giuridiche, della nozione di "identità personale".

¹³⁸ Per un approfondimento sulle ultime pronunce cfr. F.G. Campodonico, *Fine vita e suicidio medicalmente assistito: dalla sentenza n. 242 del 2019 alla recentissima sentenza n. 132 del 2025*, in *Federalismi.it*, n. 30/2025, 78 ss.

Tornando più indietro, va rilevato, in realtà, che esistono diverse sentenze che provano a delineare un interesse alla riservatezza, inteso come diritto alla “non rappresentazione” all’esterno di proprie vicende personali, che contribuiscono a definire in negativo l’identità personale, a fronte della nozione della stessa intesa come fedeltà della rappresentazione¹³⁹, che, come si è visto, connota l’identità personale all’inizio della sua storia.

In particolare, in quei primi casi, addirittura precedenti alla citata pronuncia della Pretura di Roma del 1974, la Suprema Corte, facendo riferimento al “*diritto assoluto alla personalità*”, afferma che, “*sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità di uomo come singolo, la divulgazione di notizie relative alla vita privata in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell’attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza*”¹⁴⁰.

Tale giurisprudenza, peraltro, risulta pienamente in linea proprio con la prima accezione di “*privacy*”. Come noto, nata come “*diritto ad essere lasciati soli*”¹⁴¹, si è poi progressivamente trasformata nella possibilità delle persone fisiche di controllare l’uso e la circolazione delle informazioni che le riguardano¹⁴².

Da un punto di vista normativo, come anticipato, la tutela legislativa dell’identità personale si manifesta espressamente proprio nella protezione dei dati

¹³⁹ Si veda già Cass. civ., sez. I, 22 giugno 1985, n. 3769; nonché, Id., 7 febbraio 1996, n. 978.

¹⁴⁰ Si veda già Cass. civ., 20 aprile 1963, n. 990.

¹⁴¹ Cfr. S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, vol. IV, 1890, 1 ss. Gli autori teorizzano il c.d. “*the right to be let alone*”, cioè il diritto ad essere lasciati soli nella propria sfera privata e a non subire ingerenze nella propria sfera domestica. Gli Autori evidenziano che tale diritto consiste “*nell’esigenza di riservatezza dei “thoughts, emotions, sentiments and sensations*”. La divulgazione indesiderata dei pensieri, degli stati d’animo e dei sentimenti degli individui è “*wrongful in itself*”, quindi indipendentemente dalle conseguenze sulle loro relazioni sociali, sul loro patrimonio o sui loro affari. La formula è ripresa anche da T.M. Clooley, *Treatise on the Law of Torts*, 1879.

¹⁴² Cfr. S. Rodotà, *Il diritto di avere diritti*, cit., 24. L’Autore, con un’espressione efficace, ci ricorda che “*nata come diritto dell’individuo borghese a escludere gli altri da ogni forma di invasione della propria sfera privata, la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano*”. Per una ricostruzione delle origini a partire da epoche ancora più risalenti si veda S. Nìger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

personali, inizialmente codificata nell'ambito della Legge n. 675 del 1996¹⁴³ e successivamente nel D.lgs. n. 196 del 2003, recante come “*Codice in materia di protezione dei dati personali*”¹⁴⁴.

All'introduzione di tali testi normativi viene ricondotto sia un cambiamento profondo dell'assetto generale del sistema di tutela civile della persona che la trasformazione del significato complessivo dell'identità personale¹⁴⁵.

Le nuove connotazioni del diritto all'identità hanno comportato, a parere di alcuni, anche il cambiamento dell'apparato rimediale con l'arricchimento qualitativo della tutela attraverso l'interazione tra tecniche privatistiche e pubblicistiche. L'obiettivo sarebbe quello di “*apprestare una serie di strumenti idonei ad agevolare, in via preventiva e indipendentemente dal rischio di danno, la libera costruzione della propria sfera privata*”¹⁴⁶.

Il Codice, come anticipato, è stato poi aggiornato dal d.lgs. n. 101 del 2018, che ha allineato la normativa italiana al Regolamento europeo 2016/679/UE¹⁴⁷. Il Regolamento europeo nasce con l'intento di armonizzare le normative degli Stati membri sulla protezione dei dati personali, introducendo una visione dinamica della protezione dei dati personali, che non si limita più a una difesa passiva della sfera privata, ma coinvolge attivamente il trattamento e la circolazione dei dati¹⁴⁸. Non a caso il Regolamento è relativo alla protezione delle persone fisiche con riguardo tanto al “trattamento dei dati personali” quanto alla “libera circolazione” degli stessi.

Alla luce dell'evoluzione normativa avvenuta negli ultimi anni, dunque, il trattamento dei dati personali all'interno dell'ordinamento italiano oggi avviene secondo le norme del Regolamento e del Codice.

Come ricordato dal Regolamento, in realtà, la protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale sancito

¹⁴³ L. 31 dicembre 1996, n. 675 recante «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali che ha recepito la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».

¹⁴⁴ Sul tema cfr. S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e diritto privato*, n. 1/2004, 1 ss.

¹⁴⁵ Cfr. G. Resta, *Identità personale e identità digitale*, cit., 522; S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss.; V. Zeno-Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, 1 ss.

¹⁴⁶ Cfr. G. Resta, *Identità personale e identità digitale*, cit., 522-523; nonché, M. Federico, *Protezione dei dati personali e tutela collettiva Itinerari di comparazione tra Europa e Stati Uniti*, Venezia, 2024, *passim*.

¹⁴⁷ Ai sensi del cons. n. 8 del Regolamento n. 2016/679/UE “*Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale*”.

¹⁴⁸ Cfr. C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, n. 22/2018, 1 ss.

all'art. 8, par. 1 della Carta dei diritti fondamentali dell'Unione Europea e dall'art. 16, par 1 del trattato sul funzionamento dell'Unione europea, i quali stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano¹⁴⁹.

Il trattamento dei dati personali deve essere finalizzato al benessere dell'essere umano. Il diritto alla protezione dei dati di carattere personale non costituisce una prerogativa assoluta, ma deve essere interpretato alla luce della sua funzione sociale e armonizzato con altri diritti fondamentali, nel rispetto del principio di proporzionalità. Il Regolamento, in questo senso “*rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*”¹⁵⁰.

La normativa europea di armonizzazione è intesa a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche¹⁵¹.

Nel Regolamento particolare attenzione è dedicata al tema delle tecnologie che, come noto e come anticipato, comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. In questo contesto, “*la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*”¹⁵².

Come rilevato da autorevole dottrina, è evidente, anche alla luce della digitalizzazione, che la libera costruzione dell'identità può essere concretamente messa in pericolo non soltanto nelle ipotesi di travisamento o decontestualizzazione ma anche qualora il flusso delle informazioni che riguardano la persona non avvenga attraverso canali trasparenti e all'interno di un ben preciso quadro di garanzie¹⁵³.

¹⁴⁹ Cfr. cons. 1 del Regolamento n. 2016/679/Ue.

¹⁵⁰ Cfr. cons. 4 del Regolamento n. 2016/679/Ue.

¹⁵¹ Cfr. cons. 2 del Regolamento n. 2016/679/Ue.

¹⁵² Cfr. cons. 6 del Regolamento n. 2016/679/Ue.

¹⁵³ Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, *passim*.

Proprio tale evoluzione ha comportato l'esigenza di un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. L'obiettivo non è solo che le persone fisiche abbiano il controllo dei dati personali che le riguardano ma anche garantire un quadro giuridico e operativo chiaro a operatori economici e autorità pubbliche¹⁵⁴.

A tale proposito, come condivisibilmente rilevato dalla dottrina già in un'epoca in cui non esisteva ancora tale regolazione sovranazionale, il contenuto del diritto all'identità personale come tutelato da questo tipo di normativa (la normativa in materia di protezione dei dati personali), consiste nell'interesse che i propri dati personali¹⁵⁵ – oggetto di “trattamento”¹⁵⁶ da parte di terzi – siano aggiornati, corretti e completi¹⁵⁷.

Ebbene, tali riflessioni risultano quanto mai attuali. I diritti degli interessati – anche in ragione della sempre più pervasiva digitalizzazione – sono stati, infatti, sensibilmente valorizzati e rafforzati dal Regolamento europeo¹⁵⁸.

¹⁵⁴ Cfr. cons. 7 del Regolamento n. 2016/679/Ue.

¹⁵⁵ L'art. 4 del Regolamento n. 2016/679/Ue definisce “dato personale” come qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera così la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

¹⁵⁶ *Ibidem*, si definisce “trattamento” come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

¹⁵⁷ G. Pino, *Identità personale*, cit., 304.

¹⁵⁸ Si consideri che i diritti degli “interessati” persone fisiche rispetto al controllo sui “trattamenti” dei propri “dati personali”, peraltro, sono stati da ultimo ulteriormente rafforzati dal richiamato Regolamento n. 2016/679/Ue. In particolare, i diritti conoscitivi dell'interessato includono attualmente: *i*) il diritto ad avere l'informativa per ogni trattamento svolto (artt. 13 e 14), sicché tale documento deve includere le informazioni sull'identità e i dati di contatto del titolare e del responsabile, sulle finalità del trattamento, sugli eventuali destinatari a cui sono comunicati i dati e se il titolare del trattamento sia intenzionato a comunicare tali dati a paesi terzi non appartenenti all'Unione europea; il titolare deve indicare il periodo di conservazione (o i criteri per determinare tale periodo), il diritto dell'interessato di chiedere l'accesso, il diritto di revocare il consenso, le possibili conseguenze della mancata comunicazione dei dati quando questi siano raccolti per dare esecuzione a un contratto, se è eventualmente svolta attività di profilazione; *ii*) il diritto di accesso, di ottenere dal titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso diritto di ottenere l'accesso a una serie di informazioni indicate dall'art. 15 del Regolamento; *iii*) il diritto alla comunicazione (art. 34) in caso di violazione dei dati personali che lo riguardano. Invece, i diritti di controllo dell'interessato includono: *i*) il diritto a esprimere liberamente e in modo espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità: si noti che il consenso non è richiesto quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o per adempiere un obbligo di legge (art. 6 par. 1 lett. a), b), c); *ii*) il diritto alla revoca del consenso in qualsiasi momento (art. 7 par. 3); *iii*) il diritto di opposizione al trattamento: infatti, l'art. 21 prevede che l'interessato ha il diritto di opporsi in

Sebbene, il rafforzamento dei diritti degli interessati abbia rallegrato i più, c'è chi ci ricorda, con un approccio molto meno ottimista, che, in questo scenario e in un generale contesto di “*ripiegamento individualistico negato dagli ingenui i quali s'illudono che l'agorà telematica sia davvero una piazza civica in cui si matura coscienza collettiva e non una selva in cui ogni singolo si perde, senza riuscire ad allacciare alcuna relazione realmente “politica” con gli altri c'è chi ci ricorda*”, quella all'autogoverno dei dati digitalizzati che compongono la nostra identità negli archivi pubblici e privati o nella rete sembra essere diventata la massima (e agiungo illusoria) aspirazione possibile¹⁵⁹.

In ogni caso, risulta, assolutamente condivisibile la conclusione a cui è pervenuta parte della dottrina secondo la quale tutta, o quasi tutta, la casistica sul diritto all'identità personale che si è sviluppata nella giurisprudenza italiana a partire dalla metà degli anni Settanta, sembra adesso traducibile, nella stragrande maggioranza dei casi, nel linguaggio e nei rimedi sostanziali e procedurali previsti dalla normativa sulla protezione di dati personali¹⁶⁰. Rimarrebbero esclusi, a parere degli stessi autori, esclusivamente i casi in cui non c'è alcun trattamento di dati personali. A riprova di ciò, in effetti, oggi gran parte della casistica è attratta nella giurisdizione delle Autorità indipendenti competenti in materia di dati personali¹⁶¹.

Si pensi, a titolo di esempio, al primo provvedimento dell'Autorità garante per la protezione dei dati personali del 19 aprile 1999¹⁶² che si registra sul tema. In quell'occasione, l'Autorità ha statuito che i comportamenti segnalati costituissero violazione del diritto all'identità personale così come previsto dall'art. 1 della l. n. 675 del 1996. Dalla motivazione esposta si evinceva che tale diritto si sostanziava nel diniego di vedersi attribuita un'immagine sociale differente¹⁶³. Si tornerà sul

qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano; *iii*) il diritto alla portabilità dei dati ex art. 20, a mente del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento; *iv*) il diritto di rettifica e integrazione, ai sensi dell'art. 16 in base al quale l'interessato ha il diritto a ottenere la rettifica dei dati personali inesatti che lo riguardano o l'integrazione dei dati personali incompleti; *v*) il diritto alla cancellazione e oblio, sicché ai sensi dell'art. 17 l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano quando non sono più necessari per le finalità per le quali sono stati raccolti, quando l'interessato revoca il consenso o quando i dati personali sono stati trattati illecitamente; *vi*) il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato: in tal caso, infatti, l'art. 20 riconosce all'interessato il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo significativamente sulla sua persona.

¹⁵⁹ M. Luciani, *Quale identità?*, in Aa.Vv., *Dialoghi con Guido Alpa*, Roma, 2018, 343 ss.

¹⁶⁰ Cfr. G. Pino, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 257 ss.

¹⁶¹ Per una disamina sulla giurisprudenza dell'Autorità garante per la protezione dei dati personali, in cui emerge la rilevanza del controllo dei propri dati rispetto alla costruzione dell'identità personale, cfr. G. Resta, *Identità personale e identità digitale*, cit., spec. 524 ss.

¹⁶² Cfr. provvedimento del 19 aprile 1999 consultabile sul sito istituzionale dell'Autorità.

¹⁶³ Si trattava della richiesta di rettifica dei dati personali rivolta da una donna all'editore e al direttore del giornale in seguito alla pubblicazione di alcuni articoli.

tema nel prosieguo della presente trattazione, in particolare con riferimento ai minori di età¹⁶⁴.

Si aggiunge, infine, che ci troviamo in un'epoca in cui fenomeni di c.d. "patrimonializzazione"¹⁶⁵ o "monetizzazione" dei dati personali ci impongono di svolgere ulteriori riflessioni. Se si sposa il diritto alla protezione dei dati come collegato all'identità personale, la logica conclusione di alcuni autori, infatti, è che, essendo i diritti fondamentali indisponibili, la cessione di dati che potrebbero essere utilizzati per procurare danno alla persona non dovrebbe essere consentita, neppure con il consenso dell'interessato¹⁶⁶.

Quanto al diverso tema del c.d. "diritto all'oblio", anche tale diritto viene trattato spesso come declinazione di quello di identità personale¹⁶⁷.

Non è pacifica la sua collocazione, in quanto, come efficacemente sintetizzato da alcuni autori, il diritto all'oblio si colloca al crocevia del bilanciamento tra il diritto di essere lasciato in pace e il diritto-dovere di informazione; tra la pretesa dell'individuo a vedersi rappresentato correttamente e l'interesse pubblico; tra la riservatezza del singolo e la memoria collettiva.

Si tratta, come noto, del diritto a che certe vicende appartenenti all'esistenza passata di una persona non siano oggetto di immotivata riproposizione nel tempo, in modo da continuare ad essere associate alla stessa, che, magari, se ne vuole liberare¹⁶⁸.

Parte della dottrina ha rilevato come tale diritto sia rappresentativo, in particolare, di precise caratteristiche della identità, come il suo essere "diacronica" e dinamica o anche "liquida"¹⁶⁹.

¹⁶⁴ Cfr. *infra* cap. III.

¹⁶⁵ I dati personali, secondo tale orientamento, possono costituire "un *asset*" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto come nel caso oggetto della sentenza appena richiamata.

¹⁶⁶ In questo senso si veda G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723 ss.; nonché, M. Luciani, *Quale identità?*, cit., 351.

¹⁶⁷ Sul tema cfr. A. Cerri, *Identità personale* voce, in *Enc. giur.*, IV Agg., Roma, 1995, 1 ss.; G. Finocchiaro, *Identità personale (diritto alla)* voce, cit.; E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine cui prodest?*, in *Riv. AIC*, 2016, 22 s.; C. Colapietro, A. Iannuzzi, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 85 ss. Si vedano, altresì, le riflessioni raccolte in M. Bianca (a cura di), *Memoria versus oblio*, Torino, 2019.

¹⁶⁸ G. Pino, *Identità personale*, cit., 303.

¹⁶⁹ Cfr. F. Di Ciommo, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo: il regolamento generale 2016/479 (e le direttive sul trattamento dei dati in ambito penalistico)*, Torino, 2019, 351 ss.

In questo senso, il diritto all'identità non riguarda più solamente la corretta rappresentazione dell'immagine sociale, ma la rappresentazione integrale della persona, intesa come il rispetto della reale identità di un soggetto in un determinato contesto spaziale e temporale¹⁷⁰.

Peraltro, anche con riferimento a tale diritto, vale quanto si diceva sul fatto che gran parte della casistica sul tema è attratta oggi nella giurisdizione dell'Autorità garante per la protezione dei dati personali¹⁷¹.

La casistica è varia perché lo stesso diritto all'oblio si è evoluto¹⁷². Da una prima accezione più legata alla dimensione analogica, oggi tale diritto viene rivendicato soprattutto nell'ambito della dimensione digitale, assumendo forme differenziate che spaziano dal diritto a non vedere più ripubblicate informazioni superate, al diritto alla contestualizzazione dei dati online, fino alla facoltà di ottenere la deindicizzazione dei contenuti personali. Internet, infatti, nelle sue varie declinazioni, che vanno dai siti ai social network e agli archivi storici, è in grado di riproporre in un "presente continuo" dati personali, informazioni e notizie presenti in rete¹⁷³.

Si rileva, infine, che, nel momento in cui si scrive, l'Autorità garante per la protezione dei dati personali è impegnata in una serie di attività che riguardano il c.d. "oblio oncologico"¹⁷⁴. Si tratta del diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica¹⁷⁵.

Con riguardo a questa tematica è, in realtà, il Legislatore che, in attuazione degli artt. 2, 3 e 32 della Costituzione, ha adottato la l. 7 dicembre 2023, n. 193, recante "*Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti*

¹⁷⁰ Cfr. S. Rodotà, *Persona, riservatezza, identità*, cit., 587.

¹⁷¹ G. Resta, *Identità personale e identità digitale*, cit., 522.

¹⁷² G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. Resta, V. Zeno Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, 29 ss. Tale ricostruzione è stata fatta propria anche da Cass. civ., sez. un., 22 luglio 2019, n. 19681.

¹⁷³ Cfr. M.R. Morelli, *Oblio (diritto all')* voce, in *Enc. dir.*, Agg. VI, Milano, 2002, 848 ss.; B. Meo, *Il "diritto a essere dimenticati e l'oblio su internet"*, in E. Belisario, G. Scorza, G.M. Riccio (a cura di), *Commentario GDPR e normativa privacy*, Padova, 2022.

¹⁷⁴ Cfr. art. 2, comma 7, ove si prevede che il Garante è chiamato a definire le modalità di attuazione del comma 1 della medesima disposizione. Quest'ultimo prevede che "*Ai fini della stipulazione o del rinnovo di contratti relativi a servizi bancari, finanziari, di investimento e assicurativi nonché nell'ambito della stipulazione di ogni altro tipo di contratto, anche esclusivamente tra privati, quando, al momento della stipulazione del contratto o successivamente, le informazioni sono suscettibili di influenzarne condizioni e termini, non è ammessa la richiesta di informazioni relative allo stato di salute della persona fisica contraente concernenti patologie oncologiche da cui la stessa sia stata precedentemente affetta e il cui trattamento attivo si sia concluso, senza episodi di recidiva, da più di dieci anni alla data della richiesta. Tale periodo è ridotto della metà nel caso in cui la patologia sia insorta prima del compimento del ventunesimo anno di età. Le informazioni di cui al presente comma non possono essere acquisite neanche da fonti diverse dal contraente e, qualora siano comunque nella disponibilità dell'operatore o dell'intermediario, non possono essere utilizzate per la determinazione delle condizioni contrattuali*".

¹⁷⁵ Cfr. legge 7 dicembre 2023, n. 193.

delle persone che sono state affette da malattie oncologiche”, che contiene previsioni in materia di parità di trattamento, non discriminazione e garanzia del diritto all’oblio delle persone guarite da patologie oncologiche.

5. Focus: l’identità anagrafica tra tradizione e evoluzione.

Dopo aver approfondito in quante e quali direzioni, da un punto di vista giuridico, si è spinta l’identità personale e continua a diramarsi, si intende tornare brevemente alla prima e più tradizionale accezione della stessa, quella “anagrafica”. Come si approfondirà, del resto, è il profilo da cui si intende prendere le mosse per sondare la connessione con il tema dell’identità digitale come strumento di identificazione a cui è dedicata la presente trattazione.

Partendo dall’etimologia dell’identità anagrafica, è noto che il termine “anagrafe” viene dal greco ἀναγραφή “registro” (der. di ἀναγράφω “registrare”). Da secoli, in diverse parti del mondo, l’identificazione delle persone si fonda, prima nella prassi e poi nel diritto, sull’attribuzione di un “nome” in senso giuridico¹⁷⁶, su altri segni distintivi o su metodi oggettivi idonei a garantire che un soggetto sia riconoscibile e distinto da un altro.

Si può definire l’“identità anagrafica” come l’insieme dei dati personali ufficiali che identificano una persona presso lo Stato o un ente pubblico, registrati nell’anagrafe della popolazione residente e necessari per esercitare diritti, adempiere obblighi e distinguere legalmente un individuo dagli altri. Questi dati oggi includono principalmente nome, cognome, data e luogo di nascita, sesso, residenza e codice fiscale¹⁷⁷. Prima della costituzione di sistemi di registrazione delle persone, la funzione di identificazione veniva perseguita con l’utilizzo di ritratti, stemmi, sigilli, armi di famiglia¹⁷⁸.

L’identificazione delle persone nella società persegue innanzitutto finalità pubblicistiche, poiché regola i rapporti tra cittadini e Stato. Essa consente allo Stato di esercitare un controllo sul territorio e sulla popolazione, sia per finalità di sicurezza sia per garantire un’organizzazione efficiente dei servizi amministrativi. Tali esigenze trovano riflesso anche nel diritto privato, dove una precisa identificazione costituisce una garanzia fondamentale per i rapporti tra i consociati.

Nell’ordinamento italiano, gli strumenti fondamentali per la registrazione dell’identità previsti espressamente dalla Costituzione sono rappresentati dai registri dello stato civile e dal registro anagrafico. Tali strumenti costituiscono la documentazione ufficiale della vita di una persona e del suo legame con una specifica comunità.

¹⁷⁶ Per una disamina storica sulla funzione del nome cfr. G. Alpa, *Il diritto di essere sé stessi*, cit., 133-146.

¹⁷⁷ G. Falco, *Identità personale* voce, cit., 652.

¹⁷⁸ Per un approfondimento storico sul tema cfr. V. Groebner, *Storia dell’identità personale e della sua certificazione, Scheda segnaletica, documento d’identità e controllo nell’Europa moderna*, trad. it A. Michler (a cura di), Bellinzona, 2008, 101 ss.

In particolare, il concetto di stato civile designa l'insieme delle posizioni giuridiche spettanti all'individuo all'interno della famiglia, dello Stato e della comunità giuridica. Gli atti dello stato civile sono disciplinati, nei principi generali, dal Titolo XIV del codice civile¹⁷⁹, mentre la regolazione di dettaglio è affidata al d.P.R. 3 novembre 2000, n. 396. Ai sensi dell'art. 1 del richiamato d.P.R., ogni Comune è dotato di un ufficio dello stato civile, i cui ufficiali — il sindaco e i funzionari delegati — svolgono anche funzioni di rilascio di estratti e certificati.

Gli atti dello stato civile, redatti secondo formule specifiche approvate con decreto del Ministro dell'Interno, hanno lo scopo di documentare pubblicamente non tutti gli eventi ma quelli ritenuti rilevanti per lo stato delle persone, quali nascita, matrimonio, unione civile, morte e cittadinanza. Questi atti sono raccolti in registri appositi, dove vengono iscritti gli atti contenenti le dichiarazioni rese all'ufficiale dello stato civile, nonché trascritti gli atti provenienti da altri pubblici ufficiali e annotate eventuali modifiche successive alla prima iscrizione.

Gli atti dello stato civile sono di natura pubblica, come sancito dall'articolo 450 del Codice civile e la loro pubblicità si manifesta attraverso il rilascio di estratti e certificati.

Gli estratti di tali atti di stato civile possono essere rilasciati in forma riassuntiva, riportando le informazioni contenute nell'atto e nelle relative annotazioni, oppure in copia integrale; quest'ultima opzione è possibile solo su esplicita richiesta degli interessati e qualora non sia vietata dalla legge.

Gli atti dello stato civile costituiscono prova, fino a querela di falso, di quanto l'ufficiale pubblico attesta essere avvenuto alla sua presenza o da lui compiuto, come previsto dall'articolo 451 del Codice civile.

Chiunque intenda promuovere la rettifica di un atto dello stato civile, la ricostituzione di un atto smarrito o la formazione di un atto registrato indebitamente, deve presentare ricorso al tribunale, che decide in camera di consiglio con decreto motivato¹⁸⁰.

Il registro dell'anagrafe, invece, ha la funzione di tenere traccia della popolazione residente sia nel territorio italiano che all'estero.

L'Anagrafe in Italia svolge una funzione cruciale nel sistema amministrativo e giuridico, rappresentando un elemento cardine dell'ordinamento pubblico. Non si tratta solo di uno strumento di raccolta dati, ma di una componente essenziale per il funzionamento dello Stato e per la regolazione dei rapporti tra cittadini e pubblica amministrazione. La disciplina normativa che regola l'Anagrafe è articolata, trovando il suo fondamento principale nella Legge 24 dicembre 1954, n. 1228 e nel successivo Decreto del Presidente della Repubblica 30 maggio 1989, n. 223, i quali

¹⁷⁹ Nel codice civile del 1865 gli atti dello stato civile erano disciplinati negli artt. 350-405.

¹⁸⁰ Per un inquadramento generale si veda, anzitutto, il R.D. 9 luglio 1939, n. 1239, recante l'Ordinamento dello stato civile. In dottrina cfr. A. Santoro Passarelli, *Stato civile* voce, in *Dig. disc. pubbl.*, vol. XV, Torino, 1999, 44 ss.; nonché, F. Scardullo, *Stato civile* voce, in *Enc. dir.*, vol. XLIII, 1990, 1 ss.

stabiliscono la base dell'ordinamento delle anagrafi della popolazione residente e le modalità operative per la gestione delle relative informazioni.

L'Anagrafe è l'istituto attraverso il quale i Comuni italiani tengono un registro costantemente aggiornato della popolazione residente. Questo registro, che ha carattere di continuità, è strutturato in modo tale da garantire una precisa identificazione dei cittadini, raccogliendo informazioni fondamentali quali nome, cognome, data e luogo di nascita, cittadinanza, stato civile, indirizzo di residenza e composizione del nucleo familiare. Tali informazioni non sono mere annotazioni, ma assumono un valore probatorio rilevante, in quanto costituiscono la base per il rilascio di certificati anagrafici aventi efficacia legale, come i certificati di residenza, di stato di famiglia, e di cittadinanza.

In questo contesto, particolarmente significativa per il tema in esame, e soprattutto in relazione alle considerazioni che saranno sviluppate nel prosieguo della trattazione¹⁸¹, è la più recente evoluzione normativa, che, con l'obiettivo di promuovere la modernizzazione e la digitalizzazione dei registri anagrafici, ha introdotto l'istituzione dell'Anagrafe Nazionale della Popolazione Residente (c.d. "ANPR")¹⁸². Si rileva, peraltro, che negli ultimi mesi il Legislatore sta lavorando altresì anche alla progressiva digitalizzazione dello dei registri dello Stato civile.

Posto che si tornerà più avanti sulla digitalizzazione dell'anagrafe, si anticipa sin da ora che l'art. 62 del d.lgs. n. 82 del 2005, recante "Codice dell'amministrazione digitale" (di seguito anche "CAD") prevede l'istituzione di ANPR presso il Ministero dell'interno, "quale base di dati di interesse nazionale", e che, ferme restando le attribuzioni del sindaco, l'ANPR subentra alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni.

In particolare, ANPR è un sistema integrato che consente ai Comuni di svolgere i servizi anagrafici e di consultare o estrarre dati, monitorare le attività, effettuare statistiche. Dovrebbe diventare un punto di riferimento unico per l'intera pubblica amministrazione e per tutti coloro che sono interessati ai dati anagrafici, in particolare i gestori di pubblici servizi.

Le modalità di attuazione, il funzionamento e il progressivo piano di subentro dei Comuni è stato definito dal DPCM n. 194 del 10 novembre 2014. Allo stato, si rileva che tutti i comuni italiani hanno proceduto al subentro in ANPR e che sono oltre 700 i Comuni che hanno già aderito alla piattaforma informatizzata dell'Archivio Nazionale dello Stato Civile (ANSC).

¹⁸¹ Per un approfondimento, cfr. cap. III.

¹⁸² DPCM del 10 novembre 2014, n.194, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente. Per un inquadramento sul servizio di anagrafe e sulla digitalizzazione dello stesso v. E. Jona, *Il servizio di anagrafe alle soglie della digitalizzazione*, in *Federalismi.it*, n. 18/2020, 182 ss. e ivi l'ulteriore bibliografia citata.

Con le modifiche apportate all'art. 62 del CAD, è stato previsto che ANPR contenga, oltre ai dati anagrafici, anche l'archivio nazionale informatizzato dei registri di Stato civile e i dati delle liste di leva. Da ultimo, per effetto delle modifiche all'art. 62 del CAD apportate dal D.L. n. 76/2020, è stata prevista l'attribuzione ad ogni cittadino di un codice identificativo unico in ANPR al fine di facilitare l'interoperabilità e l'integrazione con le altre banche dati della PA e dei gestori di servizi pubblici. È stata prevista, inoltre, la possibilità per i cittadini di ottenere direttamente certificazioni anagrafiche digitali tramite l'accesso ad ANPR e l'emissione di certificati digitali muniti di sigillo elettronico qualificato (a decorrere dall'attivazione del relativo servizio da parte del Ministero dell'interno e di Sogei S.p.a.).

Dunque, l'anagrafe, come regolata dalla normativa vigente, riveste una funzione di garanzia all'interno del sistema giuridico italiano. Le informazioni anagrafiche costituiscono infatti la base per numerosi atti amministrativi e giuridici, dai procedimenti elettorali alla concessione di benefici sociali, dal calcolo dei tributi locali alla gestione delle politiche abitative. Inoltre, l'anagrafe svolge un ruolo cruciale nella tutela dei diritti civili, poiché consente allo Stato di verificare l'identità e la residenza dei cittadini, elementi fondamentali per l'esercizio di diritti e doveri, come il diritto di voto, l'accesso al sistema sanitario, e la partecipazione alla vita pubblica.

Alcuni autori hanno provato a ricostruire le caratteristiche giuridiche principali dell'identità anagrafica per come emergono dal quadro normativo appena ricostruito. Tali caratteristiche sarebbero obbligatorietà, indisponibilità, stabilità, immutabilità relativa, oggettività e staticità¹⁸³.

Quanto all'obbligatorietà dell'identità anagrafica, non sembrano porsi particolari dubbi. In effetti, la citata L. 24 dicembre 1954, n. 1228, principale riferimento normativo in materia di anagrafe, stabilisce l'obbligo per ogni cittadino di iscriversi nell'anagrafe del Comune in cui stabilisce la propria dimora abituale e prevede che ogni cambiamento di residenza o di stato civile debba essere prontamente comunicato alle autorità competenti. L'importanza di questa precisazione risiede proprio nel fatto che essa sancisce il principio secondo cui l'iscrizione anagrafica non è soltanto un diritto, ma un dovere giuridico di ogni cittadino. Tale obbligo di iscrizione e aggiornamento anagrafico è finalizzato non solo a garantire la correttezza e la veridicità delle informazioni registrate, ma anche a facilitare la pianificazione delle politiche pubbliche e l'erogazione dei servizi da parte dello Stato e degli enti locali.

Si ritiene, nell'ottica di provare ad elaborare ulteriori caratteristiche da attribuire all'identità anagrafica, che, contrariamente alle identità molteplici che, come

¹⁸³ Cfr. G. Mingardo, *Il riconoscimento delle nuove soggettività e il limite del binarismo di genere nella prospettiva costituzionale*, cit., 23, ove l'A., con riferimento all'identità anagrafica, parla di obbligatorietà, indisponibilità, stabilità, immutabilità, oggettività e staticità della stessa.

si esponeva all'inizio della trattazione, possono abitare ogni individuo, una caratteristica della identità della stessa sia quella dell'“unicità”. L'identità anagrafica è unica per ciascun individuo. Ogni persona ha un'identità anagrafica distinta e non duplicabile, che è garantita dall'attribuzione di un codice fiscale e da una serie di dati identificativi specifici. Questo principio di unicità assicura che ogni cittadino possa essere identificato in modo inequivocabile all'interno del sistema anagrafico.

Altre due caratteristiche dell'identità anagrafica sono, inoltre, l'“ufficialità” e la “pubblicità”. Le informazioni che costituiscono l'identità anagrafica hanno carattere ufficiale, in quanto sono registrate e certificate da pubblico ufficiale. Questo conferisce all'identità anagrafica un valore giuridico probatorio, utilizzabile in atti pubblici e privati. Gli atti e i certificati rilasciati dall'Anagrafe (come il certificato di residenza o lo stato di famiglia) hanno piena efficacia giuridica e costituiscono prova fino a querela di falso. Le informazioni relative all'identità anagrafica, poi, sono soggette a pubblicità legale, il che significa che possono essere accessibili non solo agli interessati, ma anche a terzi, nei limiti e con le modalità previste dalla legge. Questo principio è funzionale alla trasparenza e alla certezza dei rapporti giuridici, consentendo alle autorità e agli enti pubblici di verificare l'identità delle persone in maniera ufficiale.

Qualche dubbio sorge, poi, con riferimento alle caratteristiche di “indisponibilità”, “stabilità”, “immutabilità”, “oggettività” e “staticità”. Se tali categorie possono essere accostate all'identità anagrafica, infatti, ciò può essere fatto solo in senso relativo e non assoluto. L'identità personale non è del resto “dinamica” e “fluida”? Se alcune delle informazioni contenute nell'anagrafe rimangono, in generale ma non sempre, immutate nel tempo (come la data di nascita), altre possono essere soggette a variazioni e aggiornamenti (come l'indirizzo di residenza o lo stato civile). Certo è che ogni modifica che riguarda l'identità anagrafica deve essere prontamente registrata e aggiornata nell'anagrafe, per garantire che le informazioni siano sempre attuali e corrette.

Si ritiene corretto, infine, attribuire all'identità anagrafica le caratteristiche della “completezza”, anche se non di “esaustività”. L'identità anagrafica, infatti, è composta da un insieme completo di informazioni che identificano la persona sia dal punto di vista personale che familiare e territoriale. Gli elementi tipici dell'identità anagrafica, come esposto, comprendono nome e cognome, data e luogo di nascita, stato civile (celibe/nubile, coniugato/a, vedovo/a, separato/a, divorziato/a), cittadinanza, residenza (indirizzo esatto), composizione del nucleo familiare, codice fiscale. Se queste informazioni danno un quadro completo di una persona, ciò che si coglie è comunque un'immagine stilizzata che, inevitabilmente, può fornire solo un'idea sfocata e generica dell'identità di un individuo¹⁸⁴. Del resto, non potrebbe essere altrimenti quando si parla di identità anagrafica in contrapposizione alla identità sostanziale. L'identità anagrafica, intesa quale complesso di

¹⁸⁴ In generale sul tema cfr. i contributi raccolti in M. Ladu, N. Maccabiani, *L'individuo e la realtà digitale. Una questione costituzionale e democratica oltre la virtualità*, Napoli, 2023.

dati oggettivi formalmente riconosciuti che permettono l'individuazione di un soggetto, non può mai esaurire la molteplicità e la complessità della persona nella sua dimensione sociale, culturale e psicologica.

6. Prime conclusioni sull'identità personale.

Ebbene, nell'ambito del presente capitolo si è tentato di offrire una ricostruzione dell'identità personale nella sua accezione giuridica, dalla sua emersione in dottrina e nella prima giurisprudenza fino alla codificazione e agli sviluppi più recenti.

Ponendo a fondamento tutto quanto esposto, è a questo punto possibile formulare alcune prime conclusioni, che rappresentano la base per la trattazione dei capitoli successivi.

Si è visto, con riferimento alla nozione "sostanziale" dell'identità personale, che si è sviluppata in dottrina e poi nella prima giurisprudenza come diritto ad essere correttamente rappresentati e solo successivamente, nella giurisprudenza costituzionale, come diritto ad essere sé stessi. Più precisamente, si è analizzata la genesi di entrambi i volti dell'identità "sostanziale", che potremmo definire "esterno" e civilistico ed "interno" e costituzionalistico. Il primo è quello delineato – nel 1985 – dalla Corte di Cassazione come diritto a essere rappresentati correttamente nella propria dimensione sociale. Il secondo attiene a una prospettiva più introspettiva ed è quello delineato dalla Corte costituzionale nella sentenza n. 13 del 1994 come diritto a essere sé stessi.

Con specifico riferimento a quest'ultimo, quando si parla di "identità" da un punto di vista costituzionale, si fa riferimento, il più delle volte, ai "nuovi diritti", elaborati dalla Corte costituzionale e ricondotti dalla stessa, attraverso il combinato disposto degli art. 2, 3 (secondo comma) e 13 Cost., ai diritti fondamentali della persona. Analoga attività è stata fatta dalla Corte EDU a partire dalla Convenzione.

Considerata l'espansione dell'oggetto di tale diritto, si è provato, poi, – in parte grazie alle classificazioni già proposte dalla dottrina più recente e in parte distaccandosi dalle stesse con ricostruzioni alternative – ad effettuare una sintesi dei diritti che nel tempo sono stati ricondotti all'identità personale soprattutto in via giurisprudenziale. Ci si è soffermati altresì su diritti ricondotti all'identità personale dal legislatore o dalla dottrina. In questo senso, si parla comunemente di "diritti di identità personale" invece che di "diritto di identità personale".

Quanto all'effettività della tutela dell'identità personale nella nozione della corretta rappresentazione della persona, non c'è dubbio che, oltre alle varie Corti a livello nazionale e sovranazionale, un ruolo molto importante sia stato progressivamente assunto dalla normativa in materia di protezione personali e dalla Autorità garante competente in materia e che gran parte della casistica sia ormai assorbita dalla giurisprudenza di quest'ultima.

Dopo aver approfondito in quante e quali direzioni, da un punto di vista giuridico, si è spinta l'identità personale e continua a diramarsi, si è tornati alla prima e più tradizionale accezione della stessa, quella "anagrafica". Si tratta, infatti, del profilo da cui si intende prendere le mosse per sondare la connessione con il tema dell'identità digitale come strumento di identificazione a cui è dedicata la presente trattazione.

Come emerge dal quadro normativo, che si è tentato di ricostruire nel presente capitolo, l'identità anagrafica è un concetto giuridico e amministrativo che si riferisce all'insieme delle informazioni fondamentali che identificano un individuo all'interno del sistema anagrafico di uno Stato. Tali informazioni, appuntate all'interno dei registri, costituiscono la base giuridica per l'identificazione della persona nei rapporti con lo Stato e con i terzi¹⁸⁵.

È evidente che nel sistema delineato nei precedenti paragrafi si rinviene una catena logica e giuridica in cui ogni passaggio genera e legittima il successivo, garantendo certezza e tracciabilità dell'identità di ogni cittadino. Infatti, lo stato civile definisce lo *status* giuridico della persona e registra gli eventi fondamentali della sua vita e l'anagrafe registra e aggiorna le informazioni provenienti dagli atti di stato civile, creando un *database* ufficiale della popolazione. I documenti di identità, infine, attestano concretamente l'identità della persona, sulla base dei dati anagrafici e di stato civile, e permettono il riconoscimento legale in ambito pubblico e privato.

Per la presente trattazione è di estremo rilievo la circostanza per cui, in determinati contesti, l'identificazione anagrafica si configura come presupposto abilitante, essendo propedeutica all'esercizio di diritti o all'accesso a servizi pubblici o privati, quali la fruizione di prestazioni sanitarie, l'iscrizione a istituzioni educative o l'apertura di rapporti bancari. In altre circostanze, essa svolge una funzione di tutela, assicurando che l'accesso a diritti e servizi avvenga esclusivamente in capo al soggetto titolare dell'identità, garantendo così la correttezza e la sicurezza dei rapporti giuridici e amministrativi. L'identità anagrafica, intesa come l'insieme di informazioni ufficialmente riconosciute che permettono di riconoscere un individuo, è funzionale alla sua identificazione rispetto agli altri e storicamente collegata al territorio di riferimento, sia per nascita sia per residenza.

Tradizionalmente, come esposto, ogni cittadino era registrato presso un Comune o un ente locale, che fungeva non solo da archivio amministrativo, ma anche da punto di riferimento per l'esercizio dei diritti civili, sociali e politici. In questo quadro, la territorialità non costituiva un semplice vincolo formale, bensì un principio organizzativo fondamentale: essa determinava l'accesso ai servizi pubblici, definiva la partecipazione alla vita politica locale e costituiva il presupposto per la tassazione e la tutela giuridica dei cittadini. L'identità, in questa prospettiva, si configurava come un attributo ancorato a uno specifico contesto comunale o regionale

¹⁸⁵ Per un approfondimento cfr. C. Bassu, *Il diritto alla identità anagrafica. Il cognome materno tra personalità individuale e principio di eguaglianza*, Napoli, 2021, *passim*.

e la sua funzione principale era quella di garantire la certezza giuridica e amministrativa all'interno di confini definiti e riconoscibili. A ben vedere, si tratta, da sempre, di una percezione più che di una realtà, se si considera che l'anagrafe è, in realtà, un servizio nazionale la cui gestione è attribuita ai comuni¹⁸⁶ e che lo Stato ha legislazione esclusiva su cittadinanza, stato civile e anagrafi¹⁸⁷. La scelta del Legislatore di includere il servizio anagrafico tra le funzioni che richiedono un rapporto di prossimità con i cittadini è stata ulteriormente consolidata attribuendo al comune – e al sindaco, quale organo di vertice dell'ente locale più vicino ai cittadini e nella sua qualità di ufficiale di governo, cioè come organo statale e non del comune¹⁸⁸ – l'esercizio e la responsabilità della gestione dei servizi anagrafici. Resta comunque fermo che la titolarità del servizio rimane in capo al Ministero dell'Interno.

Ebbene, con l'istituzione dell'Anagrafe Nazionale della Popolazione Residente, come si è visto, il paradigma esposto, basato nella prassi su una grande decentralizzazione, subisce una trasformazione radicale poiché non comporta esclusivamente una riorganizzazione della gestione del servizio grazie all'utilizzo di strumenti informatici ma un profondo mutamento dello stesso. La centralizzazione dei dati anagrafici a livello nazionale comporta il superamento dei confini comunali come elemento vincolante dell'identità: le informazioni relative a ciascun cittadino sono ora registrate una sola volta, in un sistema integrato e uniformemente accessibile su tutto il territorio nazionale. Questo processo non solo semplifica la gestione amministrativa e l'accesso ai servizi pubblici, ma modifica profondamente la concezione e soprattutto la percezione stessa di identità anagrafica, che da dimensione

¹⁸⁶ Cfr. art. 14, d.lgs. 18 agosto 2000, n. 267, recante «Testo unico delle leggi sull'ordinamento degli enti locali» (TUEL). La disposizione annovera, tra i servizi di competenza statale gestiti dal comune, oltre a leva militare e statistica, anche stato civile e anagrafe. Il comma 2 dell'art. 14 precisa che le funzioni derivanti da questi servizi sono esercitate dal sindaco quale ufficiale del Governo, ai sensi dell'art. 54. Sul tema cfr. l'analisi commentata all'art. 14 in R. Cavallo Perin, A. Romano, *Commentario breve al testo unico sulle autonomie locali*, Padova, 2006.

¹⁸⁷ Cfr. art. 117 Cost. In particolare, il comma 2, lett. i) prevede che lo Stato ha legislazione esclusiva, tra le altre, nelle materie di «cittadinanza, stato civile e anagrafi». La stessa disposizione precisa, al comma 6, che i Comuni, le Province e le Città metropolitane hanno, in ogni caso, potestà regolamentare in ordine alla disciplina dell'organizzazione e dello svolgimento delle funzioni loro attribuite. Il Ministero dell'interno svolge, in materia, funzioni di indirizzo, coordinamento e supporto all'azione degli enti locali e delle Prefetture. In questo senso, al momento, nell'ambito degli obiettivi di *e-government* svolge, inoltre, un fondamentale ruolo nei processi di semplificazione dell'azione amministrativa, tra i quali: la realizzazione di un sistema per la circolarità e l'integrazione delle anagrafi attraverso la infrastruttura dell'Ina-Saia; il rilascio della Carta d'Identità Elettronica (CIE) quale strumento di identificazione e di accesso ai servizi in rete nazionali e locali; la gestione informatizzata dell'Aire centrale per l'esercizio del diritto al voto degli italiani residenti all'estero; l'informatizzazione degli atti e dei registri di stato civile.

¹⁸⁸ Sul punto si veda Corte cost., 30 giugno 1988, n. 730, ove la Consulta afferma che «*Il servizio anagrafico è una funzione dello Stato, che la esercita per mezzo di un organo proprio, e cioè il sindaco, nella sua veste di ufficiale di governo. Esso ha per oggetto la registrazione delle vicende attinenti alla composizione delle popolazioni considerata nel suo aspetto complessivo in un dato momento (censimento), ovvero nelle singole modificazioni (operazioni di registrazione anagrafica). Il censimento e, dunque, null'altro che una particolare, periodica, esplicazione di tale funzione*».

locale assume dimensione nazionale, caratterizzata da un'unicità e da una riconoscibilità uniformi. La centralizzazione implica inoltre un mutamento simbolico e concettuale: l'identità non è più esclusivamente definita dalla residenza fisica, ma diventa un'entità digitale, riconosciuta e certificata attraverso strumenti informatizzati, il cui valore giuridico non dipende più dal contesto comunale di appartenenza.

Questa evoluzione comporta, oltre che l'evoluzione dell'identità anagrafica, quella della anagrafe stessa, che, come si vedrà, si evolve da registro a piattaforma che attesta attributi per la semplificazione dell'accesso ai servizi.

L'espansione della identità anagrafica oltre ai confini locali per il tramite della digitalizzazione dell'anagrafe, come si approfondirà nei capitoli successivi, trova una naturale prosecuzione nel contesto europeo, in cui l'identità digitale unica promossa dall'Unione Europea mira a una transfrontalierità che si estende anche oltre i confini nazionali. L'introduzione di strumenti come l'identità unica europea e il relativo portafoglio dovrebbe consentire ai cittadini europei di accedere a servizi pubblici e privati in qualsiasi Stato membro, consolidando un modello di identità che non è più limitato né al territorio comunale né a quello nazionale, ma che si estende a una dimensione sovranazionale, oltre che digitale¹⁸⁹. La territorialità, in questo senso, viene progressivamente disarticolata: l'identità digitale europea permette di preservare la certezza giuridica e l'efficienza amministrativa, pur svincolando l'individuo dai confini geografici tradizionali.

In conclusione, il passaggio dall'identità anagrafica percepita come locale a quella nazionale, e successivamente a quella europea, rappresenta una trasformazione profonda del concetto stesso di cittadinanza e di riconoscimento giuridico. La territorialità, un tempo principio costitutivo dell'identità, viene sostituita da un paradigma digitale e interoperabile, che garantisce la continuità dei diritti e dei servizi in una dimensione sempre più estesa e sovranazionale. Questo processo non solo ridefinisce la relazione tra individuo e Stato, ma apre anche nuove prospettive rispetto ad alcune funzioni centrali dell'identificazione nell'ordinamento giuridico.

¹⁸⁹ Cfr. M. Ladu, N. Maccabiani, *L'autodeterminazione popolare nell'era digitale: tra opportunità normative e tecnologiche*, in *Consulta online*, 2023, 415 ss.

CAPITOLO II

Il diritto all'identità digitale: profili nazionali e prospettive europee

SOMMARIO: 1. Introduzione: l'identità digitale tra rappresentazione soggettiva e funzione identificativa – 2. L'identità digitale come diritto fondamentale - 3. La disciplina dei diritti digitali nella normativa di rango primario e prime riflessioni sulle tecniche di regolazione - 3.1. Il Codice dell'amministrazione digitale e la Carta della cittadinanza digitale - 3.2. Il diritto all'identità digitale per l'accesso ai servizi - 3.3. Il Sistema pubblico di identità digitale (SPID), la Carta di identità elettronica (CIE) e la Carta nazionale dei servizi (CNS) - 3.4. Il punto di accesso telematico e l'applicazione "Io" - 3.5. Il diritto a servizi digitali semplici, sicuri e integrati - 3.6. L'Anagrafe nazionale della popolazione residente (ANPR) come piattaforma che attesta attributi - 3.7. Gli strumenti di garanzia e tutela dei diritti digitali - 4. La dimensione sovranazionale del diritto all'identità digitale nella sua funzione identificativa - 4.1. Il Regolamento (UE) 910/2014 (eIDAS) - 4.2. Il Regolamento (UE) 2024/1183 (eIDAS2) e la costruzione dell'identità digitale europea - 4.3. L'European Digital Identity Wallet (EUDI Wallet) - 5. Il portafoglio italiano (IT Wallet) e i portafogli digitali sviluppati negli altri Stati membri: una prospettiva comparatistica - 6. Prime conclusioni sullo stato dell'arte e prospettive dell'identità digitale nella sua funzione identificativa.

1. Introduzione: l'identità digitale tra rappresentazione soggettiva e funzione identificativa.

L'identità digitale¹ ha la stessa duplice natura dell'identità personale², potendo essere intesa, in modo più sostanziale, come *alter ego* virtuale della persona

¹ In ordine alla fase di transizione in cui la nozione di identità personale viene progressivamente declinata alla luce delle trasformazioni digitali cfr. i contributi di G. Resta, *Identità personale e identità digitale*, in *Dir. inform. inf.*, 2007, 511 ss.; G. Finocchiaro, *Identità personale (diritto alla)*, in *Dig. disc. priv.*, Agg., 2010, 721 ss., nonché Id., *Identità personale su internet. Il diritto alla contestualizzazione dell'informazione*, in *Dir. inform. inf.*, 2012, 383 ss.; C. Sullivan, *Digital Identity: An Emergent Legal Concept. The role and legal nature of digital identity in commercial transactions*, University of Adelaide Press, South Australia, 2011, *passim*. Con riferimento specifico alla dimensione dell'identità digitale si veda M.A. Cocuccio, *Il diritto all'identità personale e l'identità digitale*, in *Dir. fam. e pers.*, 2016, 949 ss.; i contributi raccolti in O. Pollicino, V. Lubello, M. Bassini (a cura di), *Identità ed eredità digitali. Stato dell'arte e possibili soluzioni al servizio del cittadino*, Roma, 2016; S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. industriale*, 2017, 180 ss.; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. e impr.*, 2017, 723 ss.; T. Pasquino, *Identità digitale della persona, diritto all'immagine e reputazione*, in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 93 ss.; nonché, in prospettiva comparata, A.M. Manago, *Identity development in the digital age: The case of social networking sites*, in K.C. McLean & M. Syed (a cura di), *The Oxford Handbook of Identity Development*, Oxford University Press, 2015, 508 ss.

² Per un approfondimento si rinvia al cap. I. Sul tema la letteratura è, in ogni caso, assai ampia. Per quanto riguarda l'identità personale nella sua dimensione classica, si vedano, tra gli altri, G.

nel mondo digitale, una sorta di proiezione della persona fisica³. D'altro canto, può essere intesa, in maniera più tecnica, come un insieme di informazioni utili all'identificazione di un individuo nell'ambito dei sistemi virtuali⁴.

Quando si evoca l'identità digitale quale *alter ego* virtuale, si allude a una dimensione che trascende la mera sommatoria di dati oggettivi, configurandosi piuttosto come proiezione immateriale della personalità dell'individuo. Essa si atteggiava a "doppio virtuale", capace di inglobare non soltanto i tratti caratteristici del soggetto, ma altresì l'intreccio delle sue relazioni, l'orizzonte delle opinioni e la trama delle attività dispiegate nello spazio cibernetico. In tale prospettiva, l'identità virtuale si rivela come costruzione eminentemente narrativa e rappresentazionale elaborata negli ambienti digitali e suscettibile di assumere forme molteplici: essa, infatti, può riprodurre fedelmente la realtà individuale oppure offrirne una versione rielaborata o idealizzata, ovvero, ancora, trasfigurarsi in *avatar* o maschere prive di qualsiasi immediata corrispondenza con la persona fisica da cui traggono origine⁵.

La riflessione dottrinale ha più volte sottolineato l'intrinseca fluidità e pluralità come tratto dell'identità ancor più evidente nella dimensione digitale, nella misura in cui un singolo individuo può dar vita a proiezioni identitarie eterogenee, modellate sui diversi contesti d'uso, sugli scopi perseguiti e sulle interazioni intraprese⁶. Ne deriva un processo in perenne divenire, costantemente rimodulato dai comportamenti digitali e dalle dinamiche relazionali, che veicola istanze di natura

Bavetta, *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, 1970, 953 ss.; G. Ferrando, *Diritto all'informazione e tutela dell'identità personale: note in margine ad un recente convegno*, in *Giust. civ.*, 1980, 581 ss.; A. Cataudella, *Dignità, decoro e identità personale*, in *Dir. inform. inf.*, 1985, 575 ss.; R. Tommasini, *Identità personale tra immagine e onore: autonomia del valore ed utilità dello schema*, in *Rass. dir. civ.*, 1985, 84 ss.; V. Zeno Zencovich, *Identità personale*, in *Dig. disc. priv.*, vol. IX, Torino, 1993, 294 ss.; S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, spec. 298 ss.; G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003; nonché G. Marini, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, 359 ss.

³ In questo senso, S. Rodotà, *Prefazione alla Relazione annuale dell'Autorità Garante per la protezione dei dati personali*, 1997. Sullo stesso tema, v. anche Id., *Tecnologia e diritti*, Bologna, 1995; Id., *Trasformazioni del corpo*, in *Pol. dir.*, 2006, 3 ss.; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., 723 ss., che ci parla della dimensione digitale quale prolungamento della dimensione umana; nonché, Id., *Il diritto di essere sé stessi*, cit., 258, ove l'A. afferma, appunto, che "l'informatica ha trasformato l'individuo, affiancando alla sua dimensione corporea la dimensione virtuale, la prima nota nella cerchia in cui vive, la seconda proiettata nell'infinito del mondo informatico".

⁴ In questo senso, v. G. Resta, *Identità personale e identità digitale*, cit., 516, ove l'A. rileva che la stessa relazione tra statuto dell'identità personale e tecniche di identificazione del soggetto oggi sono al centro dell'intera riflessione sull'identità in rete. Sottolinea, in questo senso, come anche nel mondo virtuale tendano a riproporsi, sia pur con altri presupposti ed implicazioni, temi e problemi già più volte affrontati dal sistema giuridico nel contesto dei rapporti *off-line*. Per un approfondimento sul tema cfr. anche M. Luciani, *Quale identità?*, in *Aa.Vv.*, *Dialoghi con Guido Alpa*, Roma Tre-Press, 2018, 343 ss.; G. Alpa, *Il diritto di essere sé stessi*, cit., 253-272.

⁵ Cfr. G. Finocchiaro, *Identità personale su internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf.*, 2012, 383 ss.

⁶ G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., 726.

psicologica, sociale e comunicativa non sempre coincidenti con le forme istituzionalizzate dell'identità giuridicamente riconosciuta. Si pensi al "profilo" in un *social network*, che, lungi dal limitarsi a identificare il titolare, ne restituisce un'immagine pubblica intessuta di preferenze, inclinazioni e passioni; ovvero ai mondi virtuali e alle piattaforme videoludiche, ove l'identità si incarna in figure simboliche o *avatar*, strumenti iconici, che amplificano e talora trasfigurano le modalità con cui il soggetto sceglie di manifestarsi agli altri.

Il nodo centrale, come rilevato dalla più autorevole dottrina, risiede nel fatto che la persona fisica, quando si proietta nello spazio digitale assumendo i tratti di "*digital person*", si manifesta attraverso processi inevitabilmente riduttivi e frammentari, che isolano e rendono visibili soltanto porzioni della sua identità. Tale rappresentazione si ricava dall'analisi di singoli atti o comportamenti puntuali – come l'ascolto di un brano musicale, la visione di un contenuto audiovisivo in rete o l'acquisto di un bene tramite piattaforme di e-commerce – i quali, se considerati isolatamente, restituiscono solo un'immagine parziale del soggetto. La capacità attuale delle tecnologie di aggregare e correlare tali tracce consente di ricostruire profili complessivi molto più ampi, ma senza garanzia di accuratezza né di effettiva corrispondenza con la realtà personale. Anzi, quanto più l'identità reale risulta sfuggente, mutevole e "liquida"⁷, tanto più la sua traduzione digitale rischia di risultare distorta o deformata⁸. La versione virtuale potrebbe essere, inoltre e per stesso volere del titolare, falsata o non autentica.

Nello stesso senso, già alla fine degli anni Novanta, Stefano Rodotà rilevava che l'evoluzione tecnologica ha profondamente inciso sul concetto di identità personale, introducendo una vera e propria "*frammentazione della persona*"⁹. L'unità del soggetto, tradizionalmente considerata elemento costitutivo dell'identità, viene infatti spezzata e sostituita da una molteplicità di proiezioni elettroniche: addirittura, a parere dell'Autore, non si tratta di un unico "clone digitale", ma di tante "persone elettroniche" quante sono le esigenze informative e gli interessi economici che ne determinano la raccolta e l'elaborazione dei dati. L'individuo contemporaneo appare così "moltiplicato", scisso in rappresentazioni plurime e talvolta incoerenti tra loro. A ciò si aggiunge la possibilità offerta dalla rete di celarsi dietro l'anonimato o di adottare identità alternative, variabili e continuamente rinegoziabili. L'"Io diviso", per riprendere le parole dell'Autore, "esplode sullo schermo", consentendo a ciascuno di incarnare simultaneamente molteplici identità secondo la

⁷ G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., 726; ripreso da M. Luciani, *Quale identità?*, cit., 353. Quest'ultimo Autore rileva, in particolare, che la digitalizzazione comporta l'attribuzione di un numero alla persona con una conseguente semplificazione informativa. Una volta disumanizzata l'informazione, però, si disumanizza anche il suo oggetto, non più immediatamente percepibile appunto come essere umano,

⁸ M. Luciani, *Quale identità?*, cit., 353.

⁹ Come rilevato già da S. Rodotà, *Elaboratori elettronici e controllo sociale*, rist. anast., Napoli, 2018, all'inizio degli anni Settanta erano nati gli "elaboratori di terza generazione", dotati di grande capacità di elaborazione e capacità di trattare elevati flussi di informazioni.

celebre formula di Pirandello: “uno, nessuno e centomila”. In questa prospettiva, le molteplici “finestre” aperte sullo schermo del computer si configurano come una metafora potente della soggettività digitale, rappresentata non più come un’unità coerente, bensì come un sistema multiplo e distribuito¹⁰.

Proprio per questo, la facoltà di autodeterminare e governare l’uso dei propri dati digitali si colloca al cuore stesso dei diritti della personalità, costituendone un presidio essenziale¹¹.

A tale proposito, può essere utile notare che, in un contesto in cui la compagine sociale-digitale tende a farsi un’idea tramite ciò che è condiviso sul *web* nonostante i contenuti online siano solo parzialmente rappresentativi di chi ne è protagonista, molto spesso le informazioni sono fornite volontariamente dall’individuo a cui le stesse appartengono¹².

L’identità digitale, in questa prospettiva, si caratterizza altresì per la sua autonomia rispetto alla dimensione corporea e temporale dell’esistenza individuale, potendo anticiparla o, anche, sopravvivere. Non è raro, infatti, che le tracce digitali di un soggetto — profili di *social network* o archivi *cloud* — permangano anche dopo la morte biologica, continuando a produrre effetti giuridici, relazionali e simbolici. Si pensi, ad esempio, alla gestione degli *account* appartenenti a persone defunte, che pone questioni delicate non solo sul piano della memoria e della rappresentazione, ma anche in relazione alla titolarità e alla trasmissibilità dei dati digitali.

¹⁰ S. Rodotà, *Prefazione alla Relazione annuale dell’Autorità Garante per la protezione dei dati personali*, cit. Sul punto cfr. anche M. Bianca, *La filter bubble e il problema dell’identità digitale*, in Riv. dir. media, 2/2019, 1 ss., 12, la quale osserva come la digitalizzazione abbia determinato un distacco tra identità reale e identità digitale, consentendo la creazione di profili virtuali che possono divergere da quello effettivo e moltiplicarsi (si pensi ai diversi profili che un medesimo soggetto può gestire su Facebook o altri social network). Ciò secondo un paradigma riconducibile all’“identità di Zelig” o alla formula pirandelliana dell’“uno, nessuno e centomila”. L’A. aggiunge, inoltre, che non è soltanto la natura poliedrica dell’identità – già paragonata ai frammenti di uno specchio – a mettere in crisi la sua tradizionale connotazione ontologica; è soprattutto la consapevolezza della formazione di un contenuto nuovo della nozione stessa di identità, che non si limita più alla dimensione fisica o morale della persona, ma deve confrontarsi con la sua rappresentazione nel mondo digitale. In questo contesto, l’identità assume una connotazione dinamica: essa non coincide solo con l’interesse a una rappresentazione fedele di sé, ma comprende anche l’interesse alla sua costante attualizzazione, attraverso la modifica o la cancellazione di dati che, pur veritieri in passato, oggi non sono più considerati significativi dal titolare.

¹¹ Sull’evoluzione del diritto alla privacy da ancorato ai diritti di proprietà a una prospettiva fondata sulla persona, sulla sua inviolabilità e sulla tutela della sfera di libertà individuale, cfr. *supra* cap. I. Giova evidenziare, inoltre, che S. Rodotà, nella bozza di dichiarazione dei diritti in Internet (o *Internet bill of rights*) redatta dalla commissione da lui presieduta afferma che le persone non possono essere ridotte ad oggetti sottoposti a poteri esterni, ad essere deve essere restituita la sovranità sulla loro esistenza digitale. L’identità è questione chiave, riguarda il diritto a costruire liberamente la personalità. In dottrina cfr., altresì, A. Baldassarre, *Privacy e Costituzione. L’esperienza statunitense*, Roma, 1974, spec. 33 ss.; E. Cremona, *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in Riv. it. inf. dir., 2024, 111 ss.

¹² Efficace, in proposito, è l’espressione di A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, Milano, 2019, 7, la quale afferma che “Al contempo c’è un innegabile desiderio sociale di mostrarsi ed è proprio la persona stessa, che tende, sempre di più, ad esporsi mediaticamente, rendendo sottile il limen che distingue il personaggio pubblico dal commoner”.

Tanto premesso sulla prima accezione, dall'altra parte, l'identità digitale può essere intesa, in modo più tecnico e funzionale, come l'insieme di informazioni necessarie a identificare un individuo. Questo approccio si concentra sul ruolo più concreto e pratico dell'identità digitale, nel momento in cui può essere utilizzata per accedere a servizi, autenticarsi *online* o proteggere le proprie interazioni virtuali. Qui, l'attenzione si sposta su dati oggettivi e verificabili, come il nome, il cognome, il codice fiscale, l'indirizzo e-mail o, in contesti più avanzati, le impronte digitali e altre caratteristiche biometriche.

Tale ultima dimensione, essendo collegata alla identità personale c.d. "anagrafica" su cui ci si è soffermati nel primo capitolo, è quella che più ci si propone di approfondire nel prosieguo della presente trattazione.

Si può affermare, dunque, che la prima nozione attiene maggiormente alla rappresentazione, mentre la seconda alla identificazione¹³. In sintesi, da un punto di vista giuridico, l'identità digitale è il complesso dei dati e delle rappresentazioni riconducibili a un individuo nello spazio digitale, la cui gestione e protezione incidono direttamente sull'esercizio dei diritti fondamentali.

Le due principali accezioni di identità digitale – quella come profilo tecnico di identificazione e quella come rappresentazione personale nella dimensione virtuale – risultano, pur nella loro differenza concettuale, strutturalmente interdipendenti. La costruzione dell'alter ego digitale, con la sua componente dinamica e relazionale, presuppone infatti un'infrastruttura di identificazione univoca e verificabile che ne garantisca l'autenticità e la legittimazione nelle interazioni online. Parallelamente, i sistemi tecnico-strumentali di identificazione assumono rilevanza crescente in quanto non si limitano a certificare l'identità dell'utente, ma ne ampliano le possibilità d'azione, consentendogli accesso a servizi, transazioni e relazioni nella dimensione digitale. L'identità digitale, in altre parole, non solo rappresenta la persona, ma la estende nella misura in cui ne permette l'effettiva partecipazione allo spazio virtuale, con ricadute giuridiche, sociali ed economiche¹⁴.

Questa duplice natura riflette le attuali sfide e opportunità connesse alla digitalizzazione dell'identità. Da un lato, la rappresentazione virtuale può divergere dalla persona fisica, generando ambiguità, manipolazioni, disinformazione o fenomeni di impersonificazione. Dall'altro lato, l'identità digitale come strumento tecnico richiede sistemi di gestione, tutela e controllo sempre più sofisticati, atti a prevenire abusi, garantire l'integrità dei dati personali e assicurare adeguati livelli di sicurezza informatica, preservando così l'affidabilità dell'identificazione e la protezione della persona nella sua proiezione digitale.

¹³ G. Resta, *Identità personale e identità digitale*, cit., 516, evidenzia che "Già da questi rilievi emerge chiaramente come qualsiasi discorso sull'identità digitale dovrebbe toccare necessariamente due aspetti: quello della tutela dell'identità personale in rete (specie nei suoi profili reputazionali) e quello delle tecniche di identificazione del soggetto a mezzo di strumenti informatici".

¹⁴ Cfr. le riflessioni di S. Rodotà svolte nell'ambito della Conferenza internazionale sulla protezione dei dati tenutasi a Parigi nel settembre 2001, ove affermava che "l'identità personale, diventando "elettronica", assume una dimensione planetaria".

2. L'identità digitale come diritto fondamentale.

La trasformazione digitale sembra oggi delineare le condizioni per l'affermazione di diritti di “quinta generazione”¹⁵, con relative opportunità e rischi inediti¹⁶.

Se parte della dottrina ricorre – anche con riferimento ai diritti digitali – alla concettualizzazione dei cc.dd. “nuovi diritti”¹⁷, altri autori preferiscono trattare gli stessi alla stregua di attuali manifestazioni di diritti fondamentali già codificati, per cui non si richiede alcuna altra previsione positiva a livello costituzionale¹⁸.

Se si adotta la tesi secondo cui i diritti digitali – o almeno alcuni di essi – costituiscono diritti nuovi, infatti, potrebbe rendersi necessaria, in taluni casi, una puntuale revisione costituzionale finalizzata all'introduzione di specifiche tutele. Viceversa, se si privilegia l'interpretazione secondo la quale essi rappresentano semplicemente una nuova declinazione dei diritti fondamentali tradizionali, l'esigenza di modifiche costituzionali viene inevitabilmente meno.

L'idea di qualificare i diritti digitali come nuove espressioni dei diritti inviolabili già riconosciuti dalla Costituzione appare particolarmente persuasiva, in quanto, in effetti, anche a parere della scrivente, maggiormente idonea a cogliere le peculiarità del contesto dinamico della trasformazione digitale, che ha comportato la creazione di una “*copia virtuale del mondo*”¹⁹.

¹⁵ Sull'evoluzione dei diritti fondamentali, cfr. N. Bobbio, *L'età dei diritti*, Torino, 1990, 7; nonché, A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in *Dir. cost.*, 2023, 12 ss.; S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014, spec. 13 ss., ove l'A. rileva che “*attraverso la considerazione dei diritti fondamentali, già previsti o di cui si chiede il riconoscimento, si giunge al tema della “cittadinanza digitale”, per molti versi ancora nebuloso ma che consente di ricondurre alla persona un insieme di situazioni che concorrono a definirne la condizione nel cyberspazio*”.

¹⁶ Cfr. M. Olivetti, *Diritti fondamentali e nuove tecnologie*, in *Revista Estudos Institucionais*, vol.6, n. 2/2020, 395 ss.

¹⁷ Per taluni approfondimenti sulle questioni che ruotano attorno ai c.d. “nuovi diritti” si rinvia all'analisi svolta nel cap I.

¹⁸ Per una ricostruzione del dibattito sul tema cfr. T.E. Frosini, *Il Costituzionalismo nella Società tecnologica*, in Aa.Vv., *Liber amicorum per Pasquale Costanzo*, in *Consulta Online*, I, 2020, p. 1 ss.; A. Morelli, O. Pollicino, *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Riv. AIC*, 2018, 12 ss.; A. Iannuzzi - F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, cit., 12; A. Iannuzzi, *La qualificazione dei diritti fondamentali nell'ecosistema digitale. Relazione di sintesi del Tavolo n. 3 «Le democrazie costituzionali nella transizione digitale»*, in *Riv. Gruppo di Pisa*, n. spec. 11/2025, 347 ss.

¹⁹ In questo senso cfr., ancora, A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, cit., 16; nonché, M. Luciani, *Quale identità?*, cit., 354, ove l'A., richiamando l'insegnamento di Guido Alpa sul tema dell'identità e dell'indisponibilità di alcuni diritti, afferma che “*Questo significa, a me pare, che anche le grandi trasformazioni del mondo contemporaneo possono essere disciplinate sulla scorta di principi antichi e che non sempre c'è necessità di inventarne di nuovi o di elaborare categorie analitiche originali. Certo, le technicalities regolatorie sono indispensabili e l'intervento del legislatore, per quanto in ritardo possa arrivare,*

Del resto, come già rilevato dalla dottrina, anche qualora si tenti di individuare singoli nuovi diritti emergenti in conseguenza della trasformazione digitale, non si giunge comunque a delineare situazioni autonome che non possano in qualche modo essere ricondotte ai diritti fondamentali già riconosciuti dalla Costituzione²⁰.

L'orientamento appena evocato sembra, peraltro, quello patrocinato anche dalla giurisprudenza costituzionale, che si è trovata di recente ad esprimersi sulla relazione tra la dimensione analogica e quella digitale dei diritti con specifico riferimento all'art. 15 della Costituzione²¹.

In particolare, la Corte costituzionale, con la nota sentenza n. 170 del 2023, ha delineato un principio fondamentale sui diritti digitali, affermando con decisione che la dimensione digitale sta avvolgendo l'esperienza umana, modificando e ampliando la sede di manifestazione dei diritti costituzionali. Questo principio si manifesta in particolare nell'interpretazione evolutiva del diritto alla libertà e segretezza della corrispondenza tutelato dall'art. 15 della Costituzione e, per i parlamentari, dall'art. 68, comma 3.

Il punto cardine di tale pronuncia risiede nell'estensione del concetto di "corrispondenza". La Corte, infatti, ha stabilito che tale nozione è ampiamente comprensiva, idonea ad abbracciare "*ogni comunicazione di pensiero umano tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza*". Questo significa che la tutela costituzionale prescinde dal mezzo tecnico utilizzato, includendo a pieno titolo gli strumenti elettronici e informatici come la posta elettronica e i messaggi scambiati tramite applicazioni di messaggistica istantanea (ad esempio, *WhatsApp*), che sono assimilabili a "*lettere o biglietti chiusi*". La riservatezza, che nella corrispondenza tradizionale era garantita dall'involucro fisico, nel digitale è assicurata dai codici personali di accesso e dai meccanismi di protezione dei dispositivi.

Un aspetto rilevante è che la tutela si estende anche alla corrispondenza già ricevuta e letta dal destinatario, purché essa conservi un carattere di attualità in rapporto all'interesse alla sua riservatezza. La Corte ha respinto l'idea che una volta non più "in itinere" (in transito), la comunicazione degradi a mero documento, poiché ciò svuoterebbe di fatto la garanzia per le forme di comunicazione digitale più diffuse, la cui ricezione è quasi istantanea. Tale "attualità" deve presumersi, salvo prova contraria, quando i messaggi sono scambiati in un lasso di tempo non signi-

non può essere omissa. Ma il presidio dei paradigmi fondamentali della civiltà giuridica occidentale è sempre disponibile, e lo è in tempo reale (se si vuole impiegare quest'espressione ormai abusata)".

²⁰ A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, cit., 17.

²¹ Sul "fondamentale rilievo sistemico della sentenza n. 170 del 2023 della Corte costituzionale" cfr. A. Iannuzzi, C. Colapietro, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, *Riv. it. inf. dir.*, 2024, 333 ss.

ficativo e sono ancora custoditi in dispositivi protetti. Questa interpretazione è fondamentale per salvaguardare l'autonomia e l'indipendenza decisionale delle Camere, evitando che la conoscenza di messaggi già pervenuti possa generare condizionamenti sul mandato parlamentare.

Inoltre, la garanzia costituzionale si estende anche ai dati esteriori delle comunicazioni (i cosiddetti metadati), come i tabulati telefonici. Se questi dati, che rivelano il fatto storico di una comunicazione, il suo autore, tempo e luogo, godono di protezione per la loro capacità intrusiva, a maggior ragione deve goderne il sequestro di messaggi elettronici, che rivela il contenuto stesso delle comunicazioni, avendo un'attitudine intrusiva tendenzialmente maggiore.

Per quanto riguarda i membri del Parlamento, la Corte ha stabilito un meccanismo procedurale specifico: nel caso di acquisizione di messaggi intercorsi con un parlamentare da dispositivi di terzi, gli organi inquirenti devono sospendere l'estrazione di tali messaggi e chiedere l'autorizzazione preventiva alla Camera di appartenenza del parlamentare. Questa autorizzazione è necessaria a prescindere dal fatto che l'acquisizione sia "mirata" o "occasionale", poiché non si tratta di "intercettazioni" (comunicazioni in corso e captate occultamente), ma di acquisizione di messaggi già avvenuti, quindi in una fase "statica".

Tuttavia, la Corte ha operato una distinzione significativa per l'estratto conto bancario. Sebbene quest'ultimo contenga dati riservati, esso non rientra nella nozione di "corrispondenza" ai fini della prerogativa parlamentare, quando acquisito tramite interrogazione di banche dati e non come corrispondenza *in itinere* spedita dalla banca. Questo perché l'estratto conto è considerato un documento contabile interno all'ente creditizio con funzione autonoma, e le prerogative parlamentari, essendo deroghe al principio di parità di trattamento, devono essere interpretate restrittivamente per evitare estensioni improprie. La protezione generica della riservatezza del parlamentare, in questi casi, è affidata ad altre norme, non alla specifica garanzia costituzionale della corrispondenza.

Ebbene, volendo provare a trarre un principio dalla sentenza appena ricordata e dal dibattito dottrinale richiamato, si può sostenere che la Corte costituzionale promuove una visione dinamica ed espansiva dei diritti fondamentali in risposta all'evoluzione tecnologica. In tal modo, tenta di assicurare che la tutela della libertà e della segretezza delle comunicazioni resti pienamente efficace anche nel contesto digitale, prevenendo lo svuotamento di tali garanzie in un'epoca in cui le comunicazioni elettroniche assumono un ruolo predominante e allo stesso tempo scoraggiando la necessità di una revisione costituzionale mirata a colmare presunti vuoti normativi.

Si potrebbe eccepire il fatto che, nella fattispecie esaminata dalla Corte, si trattava di una libertà espressamente prevista in Costituzione, quale quella alla corrispondenza. Tuttavia, si ritiene che il ragionamento alla base della decisione non cambierebbe se si facesse riferimento all'identità digitale. Pur non essendo l'iden-

tà personale direttamente menzionata dalla Costituzione, l'identità digitale potrebbe comunque ricevere una tutela indiretta attraverso quella dei diritti fondamentali: l'approccio della Corte costituzionale, infatti, si orienta chiaramente a garantire una protezione ampia e dinamica dei diritti nel contesto digitale. Ne consegue, che qualsiasi aspetto dell'identità digitale che rifletta la personalità, la riservatezza o la libertà di autodeterminazione dell'individuo nel mondo digitale - verosimilmente - godrebbe di una solida tutela costituzionale, tramite l'interpretazione dei principi esistenti adattati alle nuove realtà tecnologiche, così da preservare l'efficacia delle garanzie fondamentali in un'epoca sempre più digitalizzata.

Alla luce delle considerazioni sin qui svolte, è possibile formulare alcune ulteriori osservazioni.

In primo luogo, come già sostenuto in dottrina, la tutela dell'identità digitale intesa come rappresentazione di sé nello spazio virtuale²² risulta oggi in larga parte assorbita, nella pratica, dalla normativa di livello primario e dalla giurisprudenza in materia di protezione dei dati personali²³ o, secondo alcuni, di riservatezza²⁴. Si profila peraltro un'epoca in cui la tutela dell'identità digitale in questo senso intesa potrebbe diventare oggetto di tutela della normativa in materia di proprietà intellettuale e diritto d'autore. In questo senso, in Danimarca, il Ministro della Cultura Jakob Engel-Schmidt ha recentemente annunciato un disegno di legge che propone l'introduzione di una nuova sezione 73a nel Copyright Act danese, con l'obiettivo di riconoscere ai cittadini diritti esclusivi sui propri tratti facciali, sulla voce e sulle caratteristiche corporee, includendo una tutela per cinquant'anni dopo la morte. Al momento, si tratta di una misura in fase di definizione e non ancora approvata dal Parlamento danese. Se adottata, rappresenterebbe il primo intervento normativo eu-

²² Sul punto cfr. la *Dichiarazione dei diritti di internet*, elaborata dalla Commissione per i diritti e i doveri relativi ad Internet della Camera dei deputati. L'art. 9, rubricato, appunto, "Diritto all'identità" recita che "1. Ogni persona ha diritto alla rappresentazione integrale e aggiornata delle proprie identità in Rete. 2. La definizione dell'identità riguarda la libera costruzione della personalità e non può essere sottratta all'intervento e alla conoscenza dell'interessato. 3. L'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano. 4. Ogni persona ha diritto di fornire solo i dati strettamente necessari per l'adempimento di obblighi previsti dalla legge, per la fornitura di beni e servizi, per l'accesso alle piattaforme che operano in Internet. 5. L'attribuzione e la gestione dell'Identità digitale da parte delle Istituzioni Pubbliche devono essere accompagnate da adeguate garanzie, in particolare in termini di sicurezza".

²³ Cfr. S. Rodotà, *Una costituzione per Internet?*, in *Pol. dir.*, 2010, 337 ss., 344, ove l'A. afferma che nel contesto digitale, il diritto alla protezione dei dati personali si configura quale presidio giuridico essenziale attraverso il quale l'individuo esercita il potere di autodeterminarsi selezionando gli elementi della propria identità da rendere conoscibili alla collettività e ricomponendo, in tal modo, un'immagine unitaria e coerente della propria persona, idonea a rifletterne l'integrità. Cfr. anche S. Rodotà, *Presentazione della relazione per l'anno 2001*, cit., ove rilevava come la nozione di privacy si fosse evoluta e parlava dell'importanza dell'"*habeas data, non solo per respingere invasioni illegittime o indesiderate, ma anche per evitare di essere "costruiti" dagli altri*". Cfr., ancora, G. Alpa, *L'identità digitale e la tutela della persona*, cit.; S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 605-606.

²⁴ Cfr. M. Luciani, *Quale identità?*, cit., 349.

ropeo a concettualizzare l'identità personale come una forma di proprietà intellettuale, superando i tradizionali approcci penalistici adottati da Francia e Regno Unito e aprendo a un paradigma in cui lo sfruttamento economico e la protezione dell'identità digitale trovano una disciplina specifica nel diritto d'autore²⁵. Anche il caso recentemente emerso in Italia riguardante il noto attore Raoul Bova, che non a caso è stato oggetto anche di intervento da parte dell'Autorità per la protezione dei dati personali²⁶, evidenzia come elementi privati della comunicazione digitale possano essere oggetto di protezione mediante strumenti propri del diritto industriale²⁷.

Quanto poi all'identità digitale intesa come diritto al possesso di attributi personali idonei all'identificazione, la stessa può essere più facilmente ricostruita – anche sulla base dell'orientamento della Corte costituzionale poc'anzi richiamato – come la trasposizione in chiave digitale degli strumenti tradizionali di riconoscimento (quali il documento di identità). Come si approfondirà nel presente Capitolo e in continuità con le riflessioni già sviluppate in dottrina, essa peraltro non assolve soltanto alla funzione di identificazione del soggetto, ma, alla luce del processo di digitalizzazione che ha portato all'imposizione di specifici obblighi soprattutto alla

²⁵ Nello stesso senso in California sono state di recente approvate due leggi per limitare l'utilizzo dell'IA per impersonificare persone e reprimere il fenomeno delle cc.dd. “digital replica”, vale a dire repliche digitali realizzate con l'IA di persone fisiche esistenti o decedute. La Bill 2602, approvata dal Governatore della California lo scorso 17 settembre, stabilisce che non sono efficaci le clausole contenute nei contratti che prevedano tra le prestazioni la concessione o la realizzazione di una replica digitale di un individuo “in sostituzione dell'opera dell'individuo”. La Bill 1836, approvata nella stessa data, invece, stabilisce il divieto di diffondere la replica digitale della voce o dell'immagine di una persona deceduta senza previo consenso specifico, pena il pagamento a colui detiene i diritti sull'immagine della persona defunta di 10.000 dollari a titolo di risarcimento. Entrambe le leggi definiscono “replica digitale” una rappresentazione elettronica altamente realistica, generata al computer, facilmente identificabile come la voce o l'immagine di un individuo, incorporata in una registrazione sonora, immagine, opera audiovisiva o trasmissione in cui l'individuo reale non ha effettivamente recitato o è apparso, oppure ha recitato o è apparso, ma il carattere fondamentale della recitazione o dell'aspetto è stato materialmente alterato. Per un approfondimento, cfr. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2602 e https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1836.

²⁶ Con il provvedimento del 4 agosto 2025, n. 467, l'Autorità garante per la protezione dei dati personali è intervenuta sull'illecita diffusione sui social di un file audio contenente la conversazione privata tra un noto attore e una modella, avvertendo i potenziali utilizzatori dell'audio dell'illiceità del comportamento (che potrà essere sanzionato).

²⁷ Nella fattispecie, in seguito alla diffusione non autorizzata di messaggi vocali WhatsApp, contenenti tra l'altro la locuzione “occhi spaccanti”, l'attore ha depositato presso l'Ufficio Italiano Brevetti e Marchi due domande di registrazione di marchio - una relativa alla locuzione e l'altra alla frase integrale “Buongiorno essere speciale, dal sorriso meraviglioso e dagli occhi spaccanti” - con l'obiettivo dichiarato di impedire la circolazione illecita dei contenuti audio. Come noto, il ricorso al marchio consente di acquisire un titolo di esclusiva opponibile a terzi, funzionale a impedire usi non autorizzati dei contenuti digitali, e pertanto nella vicenda in oggetto è stato utilizzato quale strumento integrativo rispetto alla tutela tradizionale della persona e della privacy della stessa. La registrazione preventiva, infatti, consente di esercitare un controllo diretto sulla diffusione dei contenuti, mitigando le problematiche derivanti dalla viralità dei mezzi digitali e dalla difficoltà di esercitare rimedi risarcitori efficaci *ex post*.

pubblica amministrazione, costituisce oggi anche il presupposto necessario per l'accesso ai servizi, in particolare a quelli digitali. In tale prospettiva, l'identità digitale può altresì configurarsi come diritto prodromico al diritto alla fruizione dei servizi digitali²⁸.

In questo senso, le tecnologie che saranno esaminate nell'ambito della presente analisi (tra le altre, siti web, Sistema pubblico di identità digitale o "SPID", applicazione "IO" e "IT Wallet"), le quali, *prima facie*, potrebbero apparire come meri strumenti informatici privi di rilievo giuridico, si rivelano invece fondamentali mezzi abilitanti alla fruizione di servizi²⁹, rispetto ai quali tanto l'accesso quanto l'utilizzo si configurano come diritti connessi all'identità digitale.

Del resto, la gestione semplificata in mobilità delle carte fisiche si configura quale elemento strategico nel processo di digitalizzazione dell'identità e delle credenziali personali, volto a favorire la piena interoperabilità tra sistemi informativi pubblici e privati in conformità ai principi di semplificazione amministrativa e di *once only*. L'eliminazione dell'obbligo di esibizione e custodia di documenti in formato cartaceo, unitamente al superamento della necessità di presenza fisica dell'utente, dovrebbe consentire un accesso più tempestivo ai procedimenti e ai servizi, incidendo positivamente sull'efficienza amministrativa e sulla riduzione degli oneri a carico del cittadino. Tale modello, basato su strumenti digitali sicuri e riconosciuti dall'ordinamento, contribuisce altresì al rafforzamento della tutela dei dati personali e alla tracciabilità delle operazioni, delineando un rapporto più diretto, trasparente e tecnologicamente avanzato tra amministrazione e utenza, in linea con le finalità di modernizzazione del settore pubblico.

Alla luce di tutto quanto esposto, sin da ora può affermarsi che si deve propendere, al momento, per la non necessità di una revisione costituzionale. Del resto, con specifico riferimento all'identità digitale – anche nella sua dimensione eminentemente identificativa – si ritiene che il relativo diritto, oltre a trovare già fonda-

²⁸ In questo senso, da ultimo, cfr. anche la recente delega di riforma del CAD prevista dal disegno di legge recante "*Misure per la semplificazione normativa e il miglioramento della qualità della normazione e deleghe al Governo per la semplificazione, il riordino e il riassetto in determinate materie*" e sulla quale ci si soffermerà nel prosieguo, che prescrive proprio "*l'aggiornamento della disciplina dei mezzi di identificazione elettronica e dei servizi fiduciari in coerenza con il quadro regolatorio europeo, al fine di semplificare l'accesso e la fruizione dei servizi in rete erogati dalle pubbliche amministrazioni*".

²⁹ Si veda la nozione di "piattaforma abilitante" già contenuta nel par. 4.2. del primo piano triennale per l'informatica nella pubblica amministrazione dell'Agenzia per l'Italia digitale. In quella sede vengono definite come "*soluzioni che offrono funzionalità fondamentali, trasversali e riusabili nei singoli progetti, uniformandone le modalità di erogazione. Esse sollevano le amministrazioni dalla necessità di dover acquistare e/o realizzare funzionalità comuni a più sistemi software, semplificando la progettazione, riducendo i tempi e i costi di realizzazione di nuovi servizi e garantendo maggiore sicurezza informatica. Alcuni esempi rivolti ai cittadini e alle imprese sono i servizi di identificazione, di fatturazione e di pagamento. Altre piattaforme sono rivolte in via principale alla PA ma sono ugualmente abilitanti, come ad esempio l'Anagrafe nazionale della popolazione residente (ANPR). In questo modo sarà più facile per le amministrazioni offrire al cittadino e alle imprese un modo uniforme e più semplice di interazione e collaborazione*".

mento nella lettera della Costituzione, allo stato, benefici di una solida tutela riconducibile tanto alla normativa primaria quanto a quella di matrice sovranazionale. Stessa cosa può dirsi, come si vedrà, con riferimento al diritto collegato alla fruizione di servizi digitali.

3. La disciplina dei diritti digitali nella normativa di rango primario e prime riflessioni sulle tecniche di regolazione.

Soffermandosi sull'identità digitale nella sua configurazione di strumento di identificazione del soggetto, come già evidenziato, pur in assenza di un esplicito riferimento in sede costituzionale e della possibile ricostruzione nei termini sopra esposti, la stessa ha ricevuto un riconoscimento espresso in varie discipline di settore³⁰ e una tutela specifica nell'ambito della normativa di rango primario, oltre che della normativa sovranazionale.

Ciò ha portato, evidentemente, a percepire come meno urgente l'esigenza di una revisione costituzionale. In effetti, indipendentemente dall'orientamento che si vuole sposare tra quelli che si sono sviluppati in dottrina, è pacifico che, parallelamente alla codificazione di alcuni diritti digitali nell'ambito della normativa di rango primario, ha, di fatto, perso vigore, in quanto evidentemente percepito di minor urgenza, il dibattito sulla necessità di inserire gli stessi, *in primis* il diritto di accesso ad internet, in Costituzione³¹.

³⁰ Giova menzionare anche il riferimento all'identità digitale contenuto nel codice penale e in particolare nell'art. 640-ter che disciplina il reato di "frode informatica" e prevede una specifica aggravante in caso di "furto di identità digitale". In particolare, la disposizione prevede che "*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o ((la circostanza prevista)) dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età". Per un inquadramento generale si vedano in dottrina, *ex multis*, F. Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n. 93* (conv. con modif. dalla L. 15 ottobre 2013, n. 119), in *Cass. penale*, 2014, 1094 ss.; nonché, C. Crescioli, *La tutela penale dell'identità digitale*, in *Dir. pen. contemp.*, 2018, 265 ss. e ivi gli ulteriori riferimenti bibliografici.*

³¹ Cf. A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, cit., 21. A parere degli Autori, a distanza di anni, si può affermare che non v'è più un problema di accesso alla tecnologia in Italia ma più che altro permane un problema legato al *digital divide*. In particolare, si legge che "*La questione incide, infatti, più che altro sulla capacità di servirsi degli strumenti informatici, vale a dire sulle necessarie competenze digitali che i cittadini devono avere per poter fruire pienamente delle nuove tecnologie. Infatti, è proprio la mancanza di una diffusa alfabetizzazione al digitale che comporta delle vere e proprie limitazioni di fatto della*

I diritti codificati dalla normativa di rango primario, pur non potendo essere qualificati quali diritti costituzionali in senso stretto, si configurino quali espressioni dirette e specificazioni applicative dei principi sanciti dalla Costituzione, dei quali costituiscono l'attuazione nell'ambito digitale. È infatti la legislazione ordinaria a tradurre in prassi il disegno tracciato dalla Carta fondamentale, garantendo che il programma in essa contenuto mantenga effettività e attualità di fronte al rapido mutamento dei fenomeni sociali indotto dall'accelerazione tecnologica.

In tale prospettiva, considerati i tempi fisiologici richiesti per l'approvazione di una revisione costituzionale e la velocità esponenziale dello sviluppo tecnologico, la normativa primaria si rivela sovente lo strumento più idoneo per disciplinare in maniera tempestiva la materia.

Oltre che i principi costituzionali sui diritti, può essere utile prendere in considerazione in questa sede anche quanto previsto in Costituzione sulla innovazione della pubblica amministrazione. Le basi dell'organizzazione e del funzionamento della pubblica amministrazione trovano radici, infatti, nei principi costituzionali, a partire dal principio di buon andamento previsto dall'art. 97 Cost., e nei principi di sussidiarietà, differenziazione e adeguatezza sanciti dal primo comma dell'art. 118 Cost³². A questi si affiancano valori di rilevanza costituzionale come la trasparenza, nonché principi fondamentali che guidano in modo sistematico le politiche di innovazione digitale, primo fra tutti il principio di interoperabilità. La digitalizzazione delle attività amministrative è inoltre richiamata indirettamente nella Costituzione attraverso due specifiche previsioni relative alla competenza legislativa esclusiva dello Stato: da un lato, nel coordinamento informativo, statistico e informatico dei dati dell'amministrazione statale, regionale e locale (art. 117, secondo comma, lettera r)); dall'altro, nei livelli essenziali delle prestazioni da garantire uniformemente su tutto il territorio nazionale (art. 117, secondo comma, lettera m)). Questi riferimenti evidenziano sin da ora come la digitalizzazione non sia solo una questione tecnica, ma un principio di ordine costituzionale che contribuisce all'efficienza, alla trasparenza e all'uniformità dei servizi pubblici.

Fermo restando tale presupposto, concentrandosi per un momento sulle modalità di regolazione dei diritti digitali, l'analisi della normativa mostra come l'intervento più incisivo in questo ambito provenga dall'Esecutivo e dalle Autorità indipendenti o Agenzie tramite regolazione tecnica³³, con una progressiva e parallela

libertà e dell'uguaglianza dei cittadini e impedisce il pieno sviluppo della persona umana nell'ambiente digitale. È, pertanto, proprio in questo senso che lo Stato deve intervenire per adempiere ai compiti affidatigli dall'art. 3, comma 2 della Costituzione”.

³² Cfr. A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 1 ss.

³³ Per quanto riguarda la normativa tecnica si veda, tra gli altri, gli studi di A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018; A. Zei, *Tecnica e diritto tra pubblico e privato*, Milano, 2008; M. Cecchetti, *La produzione pubblica del diritto dell'ambiente: tra expertise tecnico-scientifico, democrazia e responsabilità politica*, in *DPCE online*, 2020, 1 ss.; i contributi raccolti in S. Grassi, M. Cecchetti (a cura di), *Governo*

marginalizzazione del Parlamento³⁴. In altre parole, la codificazione e la tutela dei diritti digitali sono state realizzate prevalentemente nell'ordinamento italiano attraverso atti aventi forza di legge, piuttosto che mediante la legge ordinaria. Tale dinamica, con le sue implicazioni e i suoi limiti, sarà oggetto di approfondimento anche nel prosieguo della presente tesi, nella parte dedicata all'identità digitale dei minori³⁵.

Come si approfondirà nel prosieguo, del resto, il principale riferimento normativo italiano sul tema è il d.lgs. n. 82/2005, recante “Codice dell'amministrazione digitale” (di seguito anche “CAD”)³⁶.

Lo stesso Codice, in effetti, è il risultato della delega contenuta nell'art. 10 della legge 29 luglio 2003, n. 229, recante “*Interventi in materia di qualità della regolazione, riassetto normativo e codificazione - legge di semplificazione 2001*”³⁷. Tra le idee alla base della redazione del Codice c'era proprio il principio della “*inevitabile necessità di un frequente futuro aggiornamento delle singole disposizioni*”³⁸. Per lo stesso motivo, nella redazione del Codice, si è cercato di realizzare un delicato equilibrio tra principi, contenuti nel testo principale e regole tecniche, elaborate secondo il procedimento di cui all'art. 71 CAD. Si noti, peraltro, che quest'ultima disposizione è stata riscritta nel tempo, per passare, sempre per ragioni

dell'ambiente e formazione delle norme tecniche, Milano, 2006; nonché, più di recente, F. Pacini, *Ai confini della normatività. Hard law e soft law in “tempi difficili”*, Relazione al Convegno annuale dell'Associazione “Gruppo di Pisa”, *Modello costituzionale e trasformazione del sistema delle fonti nelle crisi economica e pandemica. Emergenza e persistenza*, Firenze, 17-18 giugno 2022.

³⁴ Cfr. G. Silvestri, *La ridefinizione del sistema delle fonti: osservazioni critiche*, in *Pol. dir.*, 1987, 149 ss.; L. Carlassare, *Fonti del diritto (diritto costituzionale)* voce, in *Enc. dir.*, Annali, vol. II, Milano, 2008, 536 ss.; E. Longo, *La legge precaria. Le trasformazioni della funzione legislativa nell'età dell'accelerazione*, Torino, 2017; F. Modugno, *È possibile parlare ancora di un sistema delle fonti?*, in *Riv. AIC*, 2008, 1 ss.; A. Pizzorusso, *Sistematica giuridica e sistema delle fonti del diritto*, in *Aa.Vv.*, *Scritti in onore di Lorenza Carlassare*, I, Napoli, 2009, 281 ss.; B. Tonoletti, *Fuga dal regolamento e confini della normatività nel diritto amministrativo*, in *Dir. amm.*, 2015, 371 ss.; N. Lupo, *La normazione secondaria e il fenomeno della fuga dalla legge n. 400 del 1988 al vaglio del Comitato per la legislazione*, in *Federalismi.it*, n. 3/2017, 1 ss.; A. De Crescenzo, *Le “sunset rules” come strumenti di better regulation. Un possibile equilibrio tra centralità parlamentare in periodi emergenziali e obiettivo di semplificazione normativa*, in *DPCE online*, n. 2/2020, 1 ss.; A. Ruggeri, *Ha ancora un futuro la legge quale strumento primario di normazione e di direzione politica*, in *Oss. fonti*, 2021, 567 ss.

³⁵ Cfr. *infra* cap. III.

³⁶ V. E. De Giovanni, *Il Codice dell'amministrazione digitale: genesi, evoluzione. Principi costituzionali e linee generali*, in C. Boccia, C. Contessa, E. De Giovanni (a cura di), *Codice dell'Amministrazione digitale. D.L.gs 7 marzo 2005, n. 82 commentato e annotato per articolo*, Piacenza, 2018, 20 ss.

³⁷ Per un approfondimento sulla tecnica di redazione del Codice e delle professionalità diversificate coinvolte nella stessa cfr. E. De Giovanni, *Il Codice dell'amministrazione digitale: genesi, evoluzione. Principi costituzionali e linee generali*, cit., 22.

³⁸ *Ibidem*, cit., 23, ove l'A. afferma che il CAD è stato concepito come un “work in progress”, in quanto, alla luce della materia disciplinata avrebbe richiesto aggiornamenti frequenti.

legate al forte rischio di obsolescenza delle regole in questa materia, dalle “regole tecniche” alle “linee guida”³⁹.

Numerosi interventi normativi, poi, sono stati successivamente adottati mediante decretazione delegata e d’urgenza. La più rilevante riforma del CAD è stata realizzata mediante la legge n. 124/2015, cd. “legge Madia”, che ha conferito delega legislativa al Governo, da cui sono scaturiti due decreti legislativi, il d.lgs n. 179/2016 e il d.lgs. n. 217/2017, Correttivo al primo.

Un’ulteriore e significativa stagione riformatrice si è registrata all’indomani della pandemia da Covid-19, con la modifica sostanziale del Codice mediante due decreti-legge, entrambi successivamente convertiti in legge, il d.l. n. 76/2020 (di seguito anche decreto “Semplificazioni”), convertito con modificazioni in legge n. 120/2020 e il d.l. n. 77/2021 (di seguito, anche decreto “Semplificazioni bis”), convertito con modificazioni in legge n. 108/2021.

Da ultimo, il d.l. 2 marzo 2024, n. 19, recante “Ulteriori disposizioni urgenti per l’attuazione del Piano nazionale di ripresa e resilienza” (c.d. “Decreto PNRR 4”), convertito con modificazioni dalla l. 29 aprile 2024, n. 55, ha introdotto, nel Capo V rubricato “Disposizioni urgenti in materia di digitalizzazione”, rilevanti innovazioni in materia di digitalizzazione e dematerializzazione documentale. Tra queste si segnala, in particolare, l’inserimento di una disciplina dedicata all’IT Wallet, sulla quale si tornerà nel prosieguo.

Si aggiunge che è stato il citato d.l. n. 77 del 2021 ad attribuire all’Agenzia per l’Italia digitale (di seguito anche “AGID”) un potere sanzionatorio in caso di inadempimento degli obblighi in materia di digitalizzazione tramite l’introduzione dell’art. 18-bis CAD. Tale disposizione che, come si approfondirà, riveste un rilievo sistematico fondamentale in relazione all’effettività dei diritti digitali.

Preme aggiungere, infine, le recentissime modifiche al Codice dell’amministrazione digitale previste dal già citato disegno di legge recante “Misure per la semplificazione normativa e il miglioramento della qualità della normazione e deleghe al Governo per la semplificazione, il riordino e il riassetto in determinate materie”⁴⁰.

Tale disegno di legge, all’art. 11, prevede una delega al Governo per l’adozione - entro dodici mesi - di uno o più decreti legislativi di semplificazione, aggiornamento e riassetto del Codice dell’amministrazione digitale. La rivisitazione

³⁹ Per un approfondimento su genesi, *ratio* ed evoluzione della disposizione cfr., ancora, C. Boccia, C. Contessa, E. De Giovanni, *Codice dell’Amministrazione digitale. D.lgs. 7 marzo 2005, n. 82 commentato e annotato per articolo*, cit., 297.

⁴⁰ Il disegno di legge, collegato alla manovra di finanza pubblica, è stato presentato dal Governo al Senato il 15 luglio 2024 (S. 1192). L’esame in sede referente presso la I Commissione Affari costituzionali del Senato è stato avviato nella seduta del 18 settembre 2024, per concludersi, apportando modifiche al testo, nella seduta del 30 aprile 2025. L’esame da parte dell’Assemblea del Senato si è svolto nelle sedute del 7 e 8 maggio 2025. Trasmesso alla Camera (C. 2393), la I Commissione Affari costituzionali ne ha avviato l’esame in sede referente nella seduta del 9 luglio 2025, per concluderlo, senza apportare modifiche al testo, nella seduta del 28 ottobre 2025. Cfr. Dossier del Servizio studi del 28 ottobre 2025.

del Codice così autorizzata concerne: la disciplina dei mezzi di identificazione elettronica e dei servizi fiduciari; l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori dei servizi pubblici⁴¹.

Per quanto di interesse in questa sede, con riferimento ai mezzi di identificazione elettronica, come si evince dalla formulazione della delega, lo scopo è probabilmente solo quello di "aggiornare" la disciplina nazionale al mutato quadro sovranazionale. Come si esporrà nel prosieguo, a valle dell'entrata in vigore del Regolamento (UE) 2024/1183 (c.d. Regolamento eIDAS2), che istituisce il quadro europeo relativo a un'identità digitale (EUDI) nel maggio 2024, emergono diversi profili di disallineamento.

3.1. Il Codice dell'amministrazione digitale e la Carta della cittadinanza digitale.

Come noto, il già citato Codice dell'amministrazione digitale è stato adottato in modo da definire il quadro normativo in materia di informatizzazione della pubblica amministrazione⁴², dettando fundamentalmente un triplice ordine di

⁴¹ Come rilevato nel Dossier del Centro Studi del 28 ottobre 2025, il Comitato per la legislazione della Camera, con parere reso nella seduta del 29 luglio 2025, ha raccomandato di approfondire il principio di delega previsto dal disegno di legge, alla luce del paragrafo 2, lettera d), della circolare sulla formulazione tecnica dei testi legislativi del 20 aprile 2001 del Presidente della Camera, che prescrive di evitare la sovrapposizione tra oggetti e principi di delega. Nelle premesse, il principio di delega in esame sembra indicare più un oggetto di delega che un vero e proprio principio direttivo, suggerendo una necessaria precisazione tecnica per conformità alla prassi parlamentare.

⁴² Sul più ampio tema della trasformazione digitale della pubblica Amministrazione cfr., tra le fonti più risalenti, le riflessioni raccolte in E. Zampetti (a cura di), *Lo stato verso l'automazione. L'informatica al servizio della Pubblica Amministrazione*, in *Concretezza*, 1970; S. Buscema, *Prospettive per la meccanizzazione integrale*, in *Riv. informazione*, 1970, 110 ss.; A. Predieri, *Gli elaboratori elettronici nell'amministrazione dello Stato*, Bologna, 1971; A. Loiodice, *Informatica, banche dati e diritto all'informazione*, in Aa.Vv., *Scritti in onore di Costantino Mortati. Aspetti e tendenze del diritto costituzionale*, vol. III, Varese, 1977, 637 ss.; V. Bachelet, *Evoluzione del ruolo delle strutture della pubblica amministrazione*, Milano, 1977; G. Duni, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. amm. republ. It.*, 1978, 407 ss.; M.G. Losano, *L'automazione delle procedure gestionali e le banche di dati*, in *L'elaborazione elettronica. Principi di calcolo automatico*, Milano, 1979; Id., *Il diritto pubblico dell'informatica*, Torino, 1986; A. Usai, *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. informazione*, 1993, 163 ss.; U. Fantigrossi, *Automazione e pubblica amministrazione. Profili giuridici*, Bologna, 1993. Tra le fonti più recenti cfr., nell'ambito di una vasta dottrina, E. Belisario, *La nuova pubblica amministrazione digitale: guida al Codice dell'Amministrazione Digitale dopo la legge n. 69/2009: diritti digitali, strumenti, obblighi, sanzioni e responsabilità*, Santarcangelo di Romagna, 2009; E. Belisario, F. Ricciulli, *Legalità algoritmica e vizi procedurali*, in E. Belisario, G. Cassano (a cura di), *Intelligenza Artificiale per la Pubblica Amministrazione. Principi e regole del procedimento amministrativo algoritmico*, Pisa, 2023, 159 ss.; I. Macri, U. Macri, G. Pontevolpe, *Il nuovo codice dell'Amministrazione digitale*, Milano, 2011; A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 2019, 1149 ss.; L. Musselli, *La decisione amministrativa nell'età degli algoritmi: primi spunti*, in *Riv. dir. media*, 2020, 20 ss.; C. Colapietro, *Digitalizzazione e Costituzione*, in *Riv. giur. on-line-ISSiRFA*, n. 1/2025, 1 ss.; L. Torchia, *Lo Stato digitale*, Bologna, 2025.

norme: diritti digitali di cittadini e utenti; disposizioni sul valore giuridico - probatorio del documento informatico; obblighi a contenuto informatico per le pubbliche amministrazioni⁴³.

Come anticipato, il Codice, entrato in vigore il 1° gennaio 2006, è stato oggetto di ripetuti interventi di riforma da parte del Legislatore. Tali modifiche hanno riguardato – oltre alle singole previsioni – lo stesso impianto del testo normativo, con specifico riferimento ai soggetti destinatari delle previsioni in esso contenute (e quindi dei relativi obblighi).

Ci si sofferma esclusivamente sui profili rilevanti ai fini della presente trattazione.

Anzitutto, con riferimento all’ambito di applicazione soggettivo del Codice, se la versione originaria lo limitava solo alle pubbliche amministrazioni di cui all’art. 1, comma 2, d.lgs. n. 165/2001 e alle società e enti inseriti nel conto economico consolidato dello stato redatto da Istat, a seguito del d.lgs. n. 179/2016 e del 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 a cui si fa rinvio nell’ambito dell’art. 2, comma 2, lett. a), anche:

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

c) alle società a controllo pubblico, come definite nel D.lgs. 19 agosto 2016 n. 175, escluse le società quotate di cui all’articolo 2, comma 1, lett. p), del medesimo decreto che non rientrino nella lettera b)⁴⁴.

Con riferimento alla *ratio* della novella legislativa, si ritiene che debba essere rinvenuta, oltre naturalmente al migliore investimento di risorse pubbliche, proprio 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. A conferma di ciò, si ritiene utile ricordare che la Relazione illustrativa allo schema di decreto legislativo di attuazione della richiamata legge 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 trasparenti⁴⁵.

⁴³ Per un approfondimento su genesi ed evoluzione dell’impianto codicistico cfr., ancora, E. De Giovanni, *Il Codice dell’amministrazione digitale: genesi, evoluzione. Principi costituzionali e linee generali*, cit., 21; nonché, L. Stanca, *L’Italia vista da fuori e da dentro*, 2019, *passim*.

⁴⁴ 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’art. 2, comma 1, d.lgs. n. 175/2016. Il CAD, infatti, esclude le società quotate dall’applicazione del testo, ma solo ove le stesse non gestiscano servizi pubblici e non esercitino servizi di pubblico interesse.

⁴⁵ 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*

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.

Sempre con riguardo all'ambito soggettivo di applicazione, poi, ai fini della presente analisi, può essere utile aggiungere che, ai sensi del successivo comma 3 dell'art. 2 CAD, le disposizioni del Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari, la riproduzione e conservazione dei documenti informatici, il domicilio digitale e le comunicazioni elettroniche, nonché l'identità digitale, si applicano anche ai privati, ove non diversamente previsto⁴⁶. Inoltre, in base a quanto stabilito dal seguente comma 4, le disposizioni del CAD concernenti l'accesso ai documenti informatici e la fruibilità delle informazioni digitali si applicano anche agli organismi di diritto pubblico.

Per quando riguarda, invece, l'ambito oggettivo di applicazione del Codice, le materie escluse sono disciplinate sempre dall'art. 2 ai commi 6⁴⁷ e 6-bis⁴⁸.

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 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".

⁴⁶ La ragione per il quale si è affidata a un testo destinato in gran parte alla pubblica Amministrazione la disciplina di aspetti squisitamente privatistici è individuabile nel fatto che l'intento del legislatore, sin dal principio, era quello di "affidare a normative essenzialmente destinate a regolare l'organizzazione e l'azione della pubblica amministrazione anche la disciplina civilistica dell'utilizzo delle nuove tecnologie dell'informazione e della comunicazione" al fine di non prevedere un regime giuridico differenziato a seconda del fatto che l'uso dell'informatica sia realizzato da un soggetto pubblico o privato. Sul punto cfr. E. De Giovanni, *Il Codice dell'amministrazione digitale: genesi, evoluzione. Principi costituzionali e linee generali*, cit., 26.

⁴⁷ In particolare, l'art. 2, comma 6 prevede che "Le disposizioni del presente Codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile. Le disposizioni del presente Codice si applicano al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico".

⁴⁸ Il comma 6-bis, poi, prevede che "Ferma restando l'applicabilità delle disposizioni del presente decreto agli atti di liquidazione, rettifica, accertamento e di irrogazione delle sanzioni di natura tributaria, con decreto del Presidente del Consiglio dei ministri o del Ministro delegato, adottato su proposta del Ministro dell'economia e delle finanze, sono stabiliti le modalità e i termini di applicazione delle disposizioni del presente Codice alle attività e funzioni ispettive e di controllo fiscale".

Tanto premesso sull'impostazione del testo normativo, la sezione II (artt. 3-9) del Capo I del Codice dell'amministrazione digitale dal titolo "Carta della cittadinanza digitale" elenca una serie di diritti digitali riconosciuti ai cittadini e alle imprese⁴⁹.

Oltre, a sancire all'art. 3 il generale diritto all'uso delle tecnologie dell'utenza nei rapporti con la pubblica amministrazione, specificando, che chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti previsti dal Codice nei rapporti con i soggetti di cui all'art. 2, comma 2 dello stesso, il Codice prevede una serie di nuovi diritti digitali. Tra i diritti riconosciuti rientrano, ad esempio, proprio quello all'identità digitale, il diritto al domicilio digitale, all'utilizzo di strumenti di pagamento elettronico, all'accesso a servizi digitali semplici e integrati, alla connessione a internet presso luoghi e uffici pubblici, nonché a forme di partecipazione attraverso modalità elettroniche. Già a una prima lettura delle rubriche delle disposizioni emerge chiaramente l'impostazione del Legislatore (che, in effetti, sembra rimandare anche a quella accolta dalla Corte costituzionale e sopra ricostruita): tradurre in forma positiva una serie di diritti già presenti nell'ambito analogico e radicati nella Costituzione, reinterprestandoli alla luce della trasformazione digitale della società.

Vale la pena evidenziare che, con riferimento a tre ambiti in particolare, al diritto dell'utenza corrisponde evidentemente un obbligo dell'amministrazione di implementare i relativi servizi *online*.

Si tratta, in particolare, di: identificazione degli utenti; accessibilità ai servizi mediante l'app IO; pagamenti elettronici; connettività alla rete internet negli uffici e luoghi pubblici.

Oltre a quanto previsto nella Carta della cittadinanza digitale contenuta nel Codice, va ricordato che l'art. 14-*bis* dello stesso, alla lettera b), attribuisce all'Agenzia per l'Italia Digitale il compito di redigere e verificare l'attuazione del Piano Triennale per l'informatica nella pubblica amministrazione, il documento di indirizzo strategico approvato dal Governo, che fissa gli obiettivi che le amministrazioni pubbliche sono tenute a raggiungere nel triennio e le linee d'azione da seguire in relazione alle diverse componenti di cui consta il Piano. Il Piano ha un ruolo centrale nell'ambito della presente analisi, essendo presente sin dalla sua prima versione (Piano per il triennio 2017-2019) una chiara strategia in materia di identità digitale. Come si approfondirà nel prosieguo, a valle della pandemia da Covid-19 e dell'adozione del Piano nazionale di ripresa e resilienza (di seguito anche "PNRR"), tale la strategia nazionale si è fortemente orientata verso gli obiettivi delineati dal PNRR, anche in considerazione del fatto che l'erogazione dei finanziamenti risultava subordinata al loro conseguimento. La stessa emergenza sanitaria

⁴⁹ In proposito si veda anche la guida di riepilogo dei diritti di cittadinanza digitali previsti dal Codice pubblicata dall'Agenzia ai sensi dell'art. 17, comma 1-*quinquies*.

ha, peraltro, impresso un impulso decisivo ai processi di digitalizzazione e alla diffusione dei servizi digitali. Ciò come si vedrà ha comportato conseguenze sorprendenti con riferimento al tema dell'identità digitale.

Nondimeno, permane in maniera significativa il problema del *digital divide*, che continua a interessare in particolare alcune fasce della popolazione e che, a parere di alcuni, rappresenterebbe attualmente il vero ostacolo alla piena affermazione dei diritti digitali⁵⁰. Sul tema, però, può essere utile rilevare altresì che l'alfabetizzazione digitale, almeno come intento, è anch'essa valorizzata all'interno della Carta della cittadinanza digitale. L'art. 8 CAD, infatti, ponendo un preciso obbligo in capo allo Stato e ai soggetti di cui all'art. 2, comma 2 CAD, prevede che tali soggetti debbano promuovere iniziative volte a favorire la diffusione della cultura digitale tra i cittadini, con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo.

3.2. Il diritto all'identità digitale per l'accesso ai servizi.

Da un punto di vista squisitamente giuridico, il concetto di "identità digitale" o "identità elettronica" è stato codificato, a livello nazionale, all'interno del Codice dell'amministrazione digitale. In particolare, l'art. 1, comma 1, lett. u-quarter) definisce "identità digitale": "la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'art. 64"⁵¹.

⁵⁰ Cfr. A. Iannuzzi – F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, cit., 24. Il progresso dei diritti fondamentali, infatti, passa anche attraverso la digitalizzazione della pubblica Amministrazione e la rimozione di ostacoli, quali la mancanza delle necessarie competenze digitali da parte dei cittadini. Sul tema cfr. anche J. Van Dijk, *The digital divide*, Cambridge, 2020; D. Donati, *Digital divide e promozione della diffusione delle TIC*, in F. Merloni (a cura di), *Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione*, Torino, 2005, 209 ss.; L. Sartori, *Il digital divide*, Bologna, 2006; P. Zuddas, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Oss. AIC*, 2020, 286 ss.; S. D'Ancona – P. Provenzano, *Gli strumenti della Carta della cittadinanza digitale*, in R. Cavallo Perin - D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, cit., 223 ss.; L. Nannipieri, *La dimensione costituzionale del digital divide. In particolare, gli ostacoli cognitivi alla proiezione dell'individuo nello spazio virtuale*, in M. Nisticò – P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014, 189 ss.

⁵¹ Diversa è l'identificazione informatica definita dal CAD alla lett. u-ter, come "la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso. In genere, l'identificazione è indispensabile per l'attribuzione dell'identità del soggetto".

Come anticipato, tra gli altri diritti digitali, agli utenti è riconosciuto anche il diritto di utilizzare la propria identità digitale nei rapporti con la pubblica amministrazione nei casi in cui l'accesso al servizio pubblico richiede l'identificazione elettronica degli stessi.

La Carta della cittadinanza digitale prevede, dunque, il diritto di chiunque *“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”*⁵².

Del resto, l'identità digitale è la base imprescindibile su cui si fondano i processi di digitalizzazione della pubblica amministrazione, se si considera che ogni interazione sociale o operazione giuridicamente valida richiede che il soggetto coinvolto — persona fisica o rappresentante di un'entità giuridica — sia identificato attraverso un profilo digitale che ne attesti in modo univoco il ruolo di autore, destinatario o partecipante all'atto.

Gli strumenti di accesso ai servizi pubblici in rete previsti dalla normativa e attualmente disponibili per gli utenti in Italia sono il Sistema Pubblico di Identità Digitale (*“di seguito anche SPID”*), di cui all'art. 64 CAD⁵³ e la Carta di Identità Elettronica (*“di seguito anche CIE”*) di cui all'art. 66 CAD, nonché il punto di accesso telematico di cui all'art. 64-bis CAD (*“di seguito anche PAT”*).

La norma, dunque, mette sullo stesso piano l'identità digitale (CIE e SPID) e il punto di accesso telematico (PAT), quali strumenti tramite cui è obbligatorio garantire l'accesso ai servizi pubblici online.

L'art. 7, co. 01, CAD, rubricato *“Diritto a servizi on-line semplici e integrati”*, dal canto suo, sancisce il diritto di chiunque *“di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato, tramite gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso di cui all'articolo 64-bis, anche attraverso dispositivi mobili”*.

L'identità digitale consente inoltre di accedere, tramite l'opzione *Login with eIDAS*, anche ai servizi pubblici degli Stati membri dell'Unione europea⁵⁴.

I richiamati diritti digitali di cittadini e imprese hanno una posizione centrale nell'ecosistema dei servizi pubblici digitali disciplinato dal CAD e, pertanto, devono costituire un punto di riferimento costante nell'interpretazione del quadro normativo in materia.

⁵² Cfr. art. 3-bis, comma 1, CAD.

⁵³ *“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, 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).

⁵⁴ Consultabile al seguente indirizzo: www.eid.gov.it/it/nodo-eidas.

3.3. Il Sistema pubblico di identità digitale (SPID), la Carta di identità elettronica (CIE) e la Carta nazionale dei servizi (CNS).

Con particolare riferimento al Sistema pubblico di identità digitale, più comunemente noto come “SPID”, occorre ricordare, innanzitutto, che esso è stato istituito al fine di “*favorire la diffusione di servizi in rete e agevolare l’accesso agli stessi da parte di cittadini e imprese*”⁵⁵.

L’identità SPID è costituita da credenziali, che vengono rilasciate all’utente e che permettono l’accesso a tutti i servizi *online* delle pubbliche amministrazioni e dei soggetti privati che intendono aderire, al fine di evitare il moltiplicarsi di differenti sistemi di autenticazione.

Com’è noto, il sistema SPID è costituito come “*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*”⁵⁶. Per l’adesione a SPID, sia i gestori delle identità digitali (*identity provider*) che i fornitori di servizi (*service provider*) sottoscrivono apposite convenzioni con l’AGID.

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*” 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*”⁵⁷.

Come esposto, la normativa vigente impone ai soggetti che erogano servizi pubblici di consentire agli utenti l’identificazione informatica tramite SPID, laddove prevedano identificazione.

Fermo restando l’obbligo vigente per i soggetti pubblici, anche i soggetti privati (es. fornitori di utilities, enti creditizi ecc.) possono avvalersi di SPID per l’identificazione dei propri utenti⁵⁸.

La normativa regolamentare contenuta nel DPCM del 24 ottobre 2014, però, prevede una disciplina differenziata a seconda che il fornitore di servizi aderente sia o meno un ente tenuto a garantire i diritti digitali di cittadini e utenti sanciti dal CAD.

I soggetti di cui all’art. 2, comma 2, del CAD (pubbliche amministrazioni, gestori di pubblico servizio e società in controllo pubblico), infatti, “*usufruiscono*

⁵⁵ Cfr. art. 64, comma 2-*bis*, CAD.

⁵⁶ Cfr. art. 64, comma 2-*ter*, CAD.

⁵⁷ Il DPCM 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’art. 64, CAD.

⁵⁸ Cfr. art. 64, comma 2-*quinqies*, CAD.

*gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati*⁵⁹, mentre, secondo l'impostazione originaria, solo sui fornitori di servizi privati ricadono obblighi di remunerazione in favore dei gestori di identità digitale, in conformità a quanto previsto nei regolamenti attuativi adottati dall'AGID ai sensi dell'art. 4 del DPCM⁶⁰.

In sintesi, con riferimento ai servizi pubblici: è gratuito l'uso di identità digitali SPID da parte degli utenti, indipendentemente dal numero di accessi e/o transazioni effettuate; è gratuita l'attività di identificazione effettuata mediante SPID per conto di *service provider* pubblici, indipendentemente dal numero di accessi e/o transazioni effettuate.

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 citato DPCM 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 aderenti⁶¹.

Di particolare rilievo, dunque, è il *“Regolamento recante le modalità attuative dello SPID”* (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.

⁵⁹ Cfr. art. 14, comma 5, DPCM.

⁶⁰ Cfr. art. 15, comma 3, DPCM.

⁶¹ Cfr. art. 4, commi 2 e 3, DPCM.

Sempre con riferimento a SPID, poi, è fondamentale ricordare anche che esso non è soltanto una modalità di autenticazione informatica che assicura l'identificazione dell'utente, ma che l'utilizzo di questo strumento viene espressamente equiparato ad una forma di sottoscrizione ai fini dell'inoltro di domande a una amministrazione⁶².

Deve essere sottolineato, poi, che il Codice, all'art. 66, comma 3, prevede che anche la carta d'identità elettronica (CIE)⁶³ e la carta nazionale dei servizi (CNS)⁶⁴ possano essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni. Le modalità tecniche⁶⁵ di emissione della CIE, da parte dei Comuni, sono state definite con decreto dal Ministero dell'Interno. Sempre con riferimento alla CIE, si rileva che, dal 6 aprile 2020, con l'obiettivo di agevolare l'accesso da casa a numerosi

⁶² In proposito, infatti, l'art. 65 CAD, nella formulazione attualmente vigente quale risulta a seguito delle modifiche introdotte dal d.l. n. 76/2020, prevede che le istanze e le dichiarazioni presentate per via telematica alle pubbliche Amministrazioni e ai gestori dei servizi pubblici ai sensi dell'art. 38, commi 1 e 3, del d.P.R. 28 dicembre 2000, n. 445, sono valide: *“a) se sottoscritte mediante una delle forme di cui all'articolo 20; b) ovvero, quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), la carta di identità elettronica o la carta nazionale dei servizi; b-bis) ovvero formate tramite il punto di accesso telematico per i dispositivi mobili di cui all'articolo 64-bis (4); c) ovvero sono sottoscritte e presentate unitamente alla copia del documento d'identità. c-bis) ovvero se trasmesse dall'istante o dal dichiarante dal proprio domicilio digitale iscritto in uno degli elenchi di cui all'articolo 6-bis, 6-ter o 6-quater ovvero, in assenza di un domicilio digitale iscritto, da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS. In tale ultimo caso, di assenza di un domicilio digitale iscritto, la trasmissione costituisce elezione di domicilio digitale ai sensi e per gli effetti dell'articolo 3-bis, comma 1-ter. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario”*. La norma specifica che siffatte istanze e dichiarazioni sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento. Rispetto a quanto fin qui evidenziato, si aggiunge che il d.lgs. n. 217/2017, correttivo al CAD, ha introdotto una nuova fattispecie di formazione del documento informatico nell'ambito dell'art. 20, comma 1-bis, d.lgs. n. 82/2005. Infatti, la disposizione citata prevede che *“Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida”*.

⁶³ Il portale istituzionale dedicato alla Carta d'identità elettronica (CIE) è disponibile al seguente indirizzo: www.cartaidentita.interno.gov.it.

⁶⁴ Cfr. art. 1, comma 1, lett. d), CAD, che definisce la carta nazionale dei servizi come *“il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni”*.

⁶⁵ Il testo del decreto del Ministero dell'Interno del 23 dicembre 2015 recante le modalità tecniche di emissione della Carta d'identità elettronica sono disponibili al seguente indirizzo: www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg.

servizi pubblici, è stata rilasciata dal Ministero dell'Interno e dall'Istituto Poligrafico e Zecca dello Stato la nuova modalità di identificazione ai servizi *online* attraverso la CIE (Carta d'Identità Elettronica 3.0): l'utente può identificarsi tramite "Entra con CIE", senza dovere più utilizzare un dispositivo di lettura contactless collegato al computer, ma attraverso il proprio smartphone con l'applicazione "CIE ID".

In seguito alla modifica dell'art. 64, commi 2-quater e 2-quinquies, del CAD per opera del d.l. n. 76/2020 (c.d. segreto "Semplificazioni"), infatti, le modalità di identificazione SPID e CIE sono state pienamente equiparate, essendo stato previsto che gli utenti, per accedere ai servizi *online* delle amministrazioni pubbliche, hanno diritto ad autenticarsi – oltre che con SPID – anche tramite CIE. Pertanto, le amministrazioni, da quel momento, sono tenute a garantire per l'accesso a tutti i servizi *online* anche tale ulteriore modalità di identificazione.

Lo stesso Decreto "Semplificazioni" è intervenuto altresì sull'art. 64 del CAD, individuando il 28 febbraio 2021 come termine ultimo per lo *switch off* delle modalità di autenticazione diverse da SPID e CIE. A partire da tale data, dunque, è fatto divieto alle amministrazioni di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei 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 2021⁶⁶.

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*.

Sempre con riguardo alle modifiche al citato art. 64, occorre segnalare l'introduzione del comma 2-*duodecies*, ai sensi del quale il riconoscimento dell'utente tramite identità digitale (con livello di garanzia almeno significativo ai sensi dell'art. 8, paragrafo 2, del Regolamento (UE) n. 910/2014) ha lo stesso effetto dell'esibizione di un documento di riconoscimento⁶⁷. La stessa norma prevede che

⁶⁶ Per un approfondimento, sia consentito rinviare a E. Belisario – F. Ricciulli – S. Pagnotta, *Amministrazione digitale, guida ragionata agli switch off*, Santarcangelo di Romagna, 2020.

⁶⁷ Sul punto cfr. A. Mazzeo – M. Nastri, *Identificazione in rete: identità digitale e identità personale*, in *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 33 ss. Gli Autori sono tra i pochi a rilevare l'importanza di questa modifica normativa. L'estensione dell'equiparazione tra l'identificazione elettronica di livello di garanzia significativo e l'esibizione del documento di riconoscimento cartaceo, senza limitarla a specifiche applicazioni predeterminate, ha suscitato, in effetti alcune preoccupazioni. Ciò consente, infatti, l'impiego di strumenti di identificazione elettronica il cui rilascio e utilizzo non godono della massima tutela possibile, senza prevedere alcuna graduazione in relazione ai diversi scenari applicativi, in contrasto con la prassi consolidata del legislatore, tanto per le applicazioni online quanto per quelle tradizionali. In particolare, affermano che "*In precedenza, l'identità digitale era infatti utilizzabile (e tendenzialmente obbligatoria) per l'accesso ai servizi in rete della P.A., ma senza che il suo uso comportasse esplicitamente il riconoscimento personale del soggetto che la utilizza*". E ancora che "*Questo sembra essere a tutti gli effetti l'approdo normativo dell'evoluzione che ha portato alla completa assimilazione (mediante inclusione) dell'identità digitale all'identità personale. La necessità di trovare un centro di imputazione degli*

l'invio di istanze, comunicazioni e documenti mediante un indirizzo PEC iscritto nei registri INI-PEC, IPA o INAD è considerato equivalente a identificazione del mittente e che, inoltre, costituisce elezione di domicilio digitale ai sensi dell'art. 3-*bis*, comma 1-*ter* del CAD.

Ai fini della presente trattazione, molto rilevante è anche il comma 3-*ter* dell'art. 64 CAD che introduce un sistema di verifiche e controlli dell'identità digitale tramite ANPR. In particolare, prevede che: *“I gestori dell'identità digitale accreditati, in qualità di gestori di pubblico servizio, prima del rilascio dell'identità digitale a una persona fisica, verificano i dati identificativi del richiedente, ivi inclusi l'indirizzo di residenza e, ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione gratuita dei dati disponibili presso l'ANPR di cui all'articolo 62, anche tramite la piattaforma prevista dall'articolo 50-ter. Tali verifiche sono svolte anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale, anche ai fini della verifica dell'esistenza in vita. Il direttore dell'AgID, previo accertamento dell'operatività delle funzionalità necessarie, fissa la data a decorrere dalla quale i gestori dell'identità digitale accreditati sono tenuti ad effettuare le verifiche di cui ai precedenti periodi”*.

Il Piano nazionale di ripresa e resilienza (di seguito anche “PNRR”) ha dedicato la Missione 1, componente 1, sub-Investimento 1.4.4 alla diffusione dell'identità digitale⁶⁸. Nel 2023, poi, con l'art. 18-*bis* del d.l. 24 febbraio 2023, n. 13 (introdotto in sede di conversione dalla L. 21 aprile 2023, n. 41), lo Stato ha

effetti giuridici dell'attività in rete da una parte, e la stretta connessione dei dati dell'identità digitale alla persona fisica dall'altra, conducono a tale conclusione obbligata” (41). Storicamente, nell'ambito dell'ordinamento italiano, i controlli in fase di identificazione sono generalmente graduati in relazione al fine della stessa. In generale, il quadro normativo di riferimento in materia di identificazione personale è delineato dagli artt. 1, lettere c) e d), e 35 del d.P.R. n. 445/2000, i quali individuano i documenti idonei a comprovare l'identità del soggetto. Tali documenti, generalmente rilasciati dall'autorità statale e muniti di fotografia del titolare, sono considerati sufficienti ai fini dell'accertamento dell'identità nell'ambito dell'azione amministrativa ordinaria. L'ulteriore attività di verifica prevista dall'ordinamento notarile costituisce, al contrario, una deroga alla disciplina generale. La preoccupazione dei commentatori nasce dal riferimento contenuto nella norma al livello di garanzia “almeno significativo ai sensi dell'articolo 8, paragrafo 2, del Regolamento (UE) n. 910/2014”) e non “elevato” contenuto nel comma 2-*duodecies* e delle implicazioni che questa previsione potrebbe comportare rispetto all'accesso in Italia di strumenti di identificazione provenienti da altri Stati membri non dotati di idonei livelli di garanzia.

⁶⁸ Il piano italiano prevede investimenti pari a 191,5 miliardi di euro, finanziati attraverso il Dispositivo per la Ripresa e la Resilienza, lo strumento chiave del *Next Generation European Union* (NGEU). Prevede ulteriori 30,6 miliardi di risorse nazionali, che confluiscono in un apposito Fondo complementare finanziato attraverso lo scostamento di bilancio approvato nel Consiglio dei ministri del 15 aprile 2021 e autorizzato dal Parlamento, a maggioranza assoluta, nella seduta del 22 aprile. Il totale degli investimenti previsti per gli interventi contenuti nel piano arriva a 222,1 miliardi di euro, a cui si aggiungono 13 miliardi del *React EU*. L'importo destinato all'Italia dal piano *React EU* è stato successivamente elevato a circa 14,4 miliardi (aprile 2022). Si segnala inoltre che anche la quota spettante all'Italia in termini di sovvenzioni è stata incrementata di circa 146 milioni di euro (giugno 2022) a seguito della effettiva variazione del PIL reale registrata nel periodo 2020-2021. Il Piano si articola in sei Missioni. Ciascuna missione è articolata in componenti, all'interno delle quali sono individuati degli investimenti e delle riforme. La prima missione, “Digitalizzazione, Innovazione, Competitività, Cultura”, stanziata 40,29 miliardi, a cui si aggiungono 0,8 miliardi da *React EU* e 8,73 miliardi dal Fondo complementare.

riconosciuto agli *identity provider* un contributo economico *una tantum*, specificamente in relazione al raggiungimento degli obiettivi sulla diffusione dell'identità digitale previsti dalla Missione 1. In particolare, la norma ha stanziato un fondo di 40 milioni di euro, da ripartire tra tutti gli *identity provider* “*in proporzione al numero di identità digitali gestite da ciascun gestore, degli accessi ai servizi erogati dalle pubbliche amministrazioni, delle verifiche dei dati nell'ANPR, tenuto conto dell'incremento delle identità digitali gestite e delle transazioni registrate, nonché del grado di raggiungimento degli obiettivi*” PNRR, secondo le modalità stabilite in apposito decreto.

Nel contesto descritto, nonostante gli investimenti effettuati anche per il tramite del PNRR e la forte diffusione dello strumento⁶⁹, la prospettiva di medio periodo dello SPID è apparsa per diverso tempo incerta. Le dichiarazioni programmatiche del Governo Meloni hanno infatti lasciato intendere la volontà di convergere verso l'utilizzo della Carta di Identità Elettronica (CIE) quale strumento principale di identità digitale, con conseguente rischio di progressiva marginalizzazione dello SPID. A ciò si aggiungono le criticità segnalate dai gestori accreditati, i quali lamentano da anni l'assenza di un adeguato corrispettivo economico per la gestione del servizio, circostanza che potrebbe pregiudicarne la sostenibilità finanziaria. Non irrilevanti sono, inoltre, le difficoltà tecniche e operative emerse in sede applicativa (in particolare nei cc.dd. “click day” o nei momenti di maggiore affluenza), che hanno contribuito a minare la percezione di efficienza del sistema. Il quadro si completa con l'assenza, allo stato, di un indirizzo normativo univoco e di lungo periodo circa la permanenza dello SPID quale canale di identificazione, essendo la sua vigenza più volte prorogata mediante atti puntuali. Fermo restando quanto appena rilevato, va segnalato che il Governo ha recentemente provveduto a stipulare convenzioni con gli *identity provider* accreditati, al fine di rifinanziare e garantire la continuità del servizio, scongiurandone, almeno nell'immediato, la cessazione⁷⁰.

⁶⁹ Secondo i dati dell'AGID, nel 2024, oltre 41 milioni di cittadini hanno adottato SPID, realizzando più di 1,2 miliardi di autenticazioni, e nel primo semestre 2025 si sono registrate oltre 630 milioni di autenticazioni. Media settimanale delle identità rilasciate: circa 76 mila nei primi 5 mesi del 2020, 262 mila nei successivi 7 mesi del 2020, 230 mila nel 2021, 118 mila nel 2022, 62 mila nel 2023, 50 mila nel 2024. Nel 2025 la media settimanale dei mesi da gennaio a luglio si attesta intorno alle 52 mila identità, superando anche i numeri del 2024. Secondo l'Osservatorio *Digital Identity* del Politecnico di Milano, l'89% della popolazione internet italiana utilizza SPID, con l'86% degli utenti che ne fa uso più volte all'anno.

⁷⁰ Si segnala che il comunicato di Alessio Butti, Sottosegretario alla Presidenza del Consiglio dei ministri con delega all'innovazione tecnologica e alla transizione digitale, sulla firma delle proroghe delle convenzioni tra l'Agenzia per l'Italia Digitale e gli *identity provider* per la gestione dello SPID del 7 ottobre 2025 parla di “un accordo per accompagnare la transizione verso l'identità digitale unica”. In particolare, gli accordi, della durata biennale, prevedono la possibilità di un'ulteriore estensione fino a 36 mesi, al fine di garantire la continuità operativa di uno strumento che ha rappresentato il primo passo verso la diffusione e l'adozione dell'identità digitale in Italia. La proroga delle convenzioni vigenti, a parere del Sottosegretario, assicura la stabilità del sistema in un momento di profonda trasformazione del quadro nazionale dell'identità digitale, in cui si inseriscono le iniziative di razionalizzazione promosse dal Governo attraverso la Carta d'Identità Elettronica (CIE), che ha superato i 9 milioni di credenziali attivate, e l'IT Wallet. Come evidenziato dallo

Le ragioni, secondo i più, sarebbero riconducibili anche all'utilizzo della CIE da parte dei cittadini che, sebbene riscuota notevole successo come documento fisico, risulta sostanzialmente inefficace quale strumento di autenticazione digitale. Le motivazioni sono molteplici: dalla complessità della procedura di attivazione, con PIN e PUK frequentemente smarriti o non reperibili, fino alla limitata familiarità degli utenti con le modalità operative. SPID, al contrario, ha evidenziato caratteristiche di immediatezza, accessibilità da qualsiasi dispositivo e sufficiente intuitività da consentire un'adozione su larga scala⁷¹.

In questa sede, dato il carattere ancora recente delle nuove convenzioni, è possibile formulare soltanto alcune prime riflessioni, mentre il loro reale impatto potrà essere valutato solo con il passare del tempo.

I contenuti principali delle convenzioni concernono, in primo luogo, l'obbligo per i provider di garantire la verifica dell'identità degli utenti mediante accesso ai registri anagrafici, in conformità agli standard di sicurezza definiti da AgID, nonché di assicurare livelli di interoperabilità, affidabilità e continuità del servizio secondo i parametri prestazionali definiti contrattualmente. Sono altresì disciplinati i meccanismi di controllo, la reportistica periodica e le responsabilità dei provider in caso di inosservanza degli obblighi convenzionali o di eventi di compromissione della sicurezza.

Le principali novità introdotte dalle convenzioni rinnovate riguardano la valorizzazione economica della base utenti, nel rispetto dei principi di trasparenza, proporzionalità e non discriminazione, quale strumento per assicurare la sostenibilità operativa del sistema; la proroga della durata delle convenzioni fino al 2030, con previsione di ulteriori estensioni, al fine di garantire continuità operativa; e l'esplicita integrazione con ulteriori strumenti di identità digitale nazionale, quali la Carta d'Identità Elettronica (CIE) e l'IT Wallet, in coerenza con l'obiettivo di costruire un ecosistema digitale integrato, sicuro e tecnologicamente avanzato.

stesso Sottosegretario "Il rinnovo degli accordi costituisce un passaggio cruciale nel processo di consolidamento e razionalizzazione dell'identità digitale nazionale. L'Italia ha anticipato di due anni l'obiettivo PNRR in materia di identità digitale e guarda ora a un sistema IT Wallet sempre più completo e interoperabile. La crescita della CIE e il mantenimento di queste convenzioni ci permettono di accompagnare la transizione verso un modello unico, semplice e pienamente allineato agli standard europei". Ad oggi, nel Paese sono state rilasciate complessivamente 96 milioni di identità digitali (55 milioni di CIE e 41 milioni di SPID), che permettono l'accesso a un numero crescente di servizi e documenti. L'IT Wallet, integrato nell'AppIO, conta già oltre 6,4 milioni di utenti attivi, che hanno utilizzato la piattaforma per attivare più di 10,6 milioni di documenti, tra cui patenti, tessere sanitarie e carte europee per le disabilità. Rispetto a tale comunicato, va precisato che l'IT Wallet non costituisce un sistema di identità digitale autonomo, bensì un contenitore di documenti che si appoggia a SPID o CIE per le funzioni di autenticazione. Presentarlo come un'alternativa a SPID risulterebbe pertanto fuorviante: esso rappresenta piuttosto un complemento e un'evoluzione dell'ecosistema digitale, capace di arricchire le funzionalità senza tuttavia sostituire la necessità di disporre di un sistema di autenticazione robusto, diffuso e pienamente operativo.

⁷¹ Cfr. G. Manca, *Spid vivrà altri cinque anni, perché la Cie è un flop: e ora?*, in Agenda Digitale del 9 ottobre 2025.

3.4. Il punto di accesso telematico e l'applicazione "IO".

Tanto esposto in relazione a SPID e CIE, occorre ora soffermarsi sull'erogazione di servizi pubblici online tramite l'app IO, soluzione informatica con la quale è stato realizzato il citato Punto di Accesso Telematico di cui all'art. 64-bis del d.lgs. 7 marzo 2005, n. 82⁷². Giova ribadire in questa sede che l'app IO è stata concepita come piattaforma unica che consente a cittadini e imprese di accedere ai servizi online della pubblica amministrazione in modo integrato e semplificato. Questo strumento, che utilizza l'interoperabilità tra i diversi sistemi digitali pubblici, dovrebbe migliorare l'efficienza e l'usabilità dei servizi pubblici digitali.

A tale fine, sempre l'art. 64-bis, al comma 1-bis (nella formulazione risultante a seguito delle modifiche di cui al d.l. n. 76/2020, prevede che i soggetti coinvolti nella *governance* digitale (pubbliche amministrazioni, concessionari di pubblici servizi, società a controllo pubblico e prestatori di servizi fiduciari qualificati) *“progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con il servizio di cui ai commi 1 e 1-ter, espongono per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida”*.

Gli obblighi previsti dalle norme citate sono posti al fine di consentire la concreta attuazione del diritto degli utenti, sancito dall'art. 7, comma 1 del CAD, di fruire dei servizi digitali *“anche attraverso dispositivi mobili”*.

In attuazione delle norme citate, dunque, è stata sviluppata e resa disponibile agli utenti "IO", l'applicazione dei servizi pubblici che dovrebbe consentire a tutti gli enti di comunicare con i propri utenti attraverso un unico canale, integrato con i sistemi di identificazione SPID e CIE, permettendo così l'erogazione dei servizi *online* tramite dispositivi mobili.

IO è un canale che qualsiasi ente pubblico può utilizzare per inviare comunicazioni ai propri utenti: fornire aggiornamenti, ricordare scadenze o richiedere pagamenti relativi a un determinato servizio. Dopo un primo periodo di sperimentazione presso alcuni enti, l'applicazione è attualmente disponibile sugli *store* e liberamente scaricabile da tutti i cittadini⁷³.

Dal punto di vista tecnico e funzionale, il PAT è disciplinato, oltre che dalle richiamate norme del CAD, dalle *“Linee guida sul punto di accesso telematico ai*

⁷² L'art. 64-bis, comma 1, CAD, ha previsto l'attivazione di un *“punto di accesso telematico”* presso la Presidenza del Consiglio dei ministri, attraverso cui le pubbliche Amministrazioni sono tenute a rendere fruibili i propri servizi in rete.

⁷³ L'app IO ha superato i 40 milioni di download, ma i dati più recenti indicano circa 5 milioni di utenti che la usano stabilmente, mentre un report del maggio 2025 riporta 11,8 milioni di utenti attivi negli ultimi 12 mesi. L'app ha una media di 3,4 milioni di utenti settimanali che la consultano.

servizi della Pubblica Amministrazione”, adottate con Determinazione AGID n. 598 dell’8 novembre 2021 (d’ora in avanti anche solo “Linee guida PAT”).

Secondo quanto previsto dalle stesse, nel PAT - e dunque nell’app IO - i soggetti di cui all’art. 2, comma 2, del CAD, in quanto “Soggetti Erogatori” di servizi pubblici, aderiscono alla piattaforma e ivi rendono disponibili agli utenti i propri servizi pubblici in rete.

Nell’ambito dell’app IO, dunque, tali soggetti sostanzialmente coincidono con le amministrazioni, che, in qualità di fornitori di servizi in rete, ai sensi della sopra richiamata normativa sullo SPID, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali (di cui si è detto *supra*).

Occorre rilevare, inoltre, che l’identificazione dell’utente finale dell’app IO, per espressa previsione delle Linee guida PAT, deve avvenire tramite gli strumenti previsti all’art. 64 del CAD, ivi incluso dunque lo SPID.

Inoltre, sempre per espressa previsione delle richiamate Linee guida, il PAT è integrato con il sistema SPID, “*al fine di assicurare quanto disposto dal comma 2-quater dello stesso articolo 64 [del CAD] in relazione all’identificazione dei soggetti che accedono ai Servizi in rete erogati dalle pubbliche amministrazioni*”. D’altronde, secondo quanto previsto, l’app IO, oltre che con SPID e CIE, è integrata con tutte le piattaforme dei servizi pubblici digitali previste dalla normativa vigente, tra cui anche la piattaforma delle notifiche digitali “SEND”.

È in tale contesto che - sulla base dell’art. 64-quater, comma 7, CAD - nell’ambito del PAT, viene richiesta l’identificazione con CIE o SPID⁷⁴ per accedere alla funzionalità “Documenti su IO”⁷⁵ con la quale gli utenti possono scaricare le copie digitali dei propri documenti analogici, nelle more dell’implementazione dell’IT Wallet sul quale ci si soffermerà nel prosieguo⁷⁶.

⁷⁴ In ambito informatico, la fruizione di un servizio ad accesso controllato (come può essere il PAT), è regolata da almeno due distinte fasi: l’identificazione e l’autenticazione. Tale distinzione rileva da almeno due punti di vista: *i*) quello tecnico, dovendosi distinguere le diverse fasi di colloquio tra due sistemi, che sono consequenziali ma presidiate da misure e logiche diverse; *ii*) quello giuridico, come si evince dall’analisi della normativa applicabile. Per quanto attiene l’aspetto giuridico, infatti, SPID e CIE rappresentano i mezzi di identificazione elettronica delle persone fisiche, notificati dallo Stato italiano all’UE ai sensi del Regolamento UE n. 910/2014 e, come previsto dall’art. 64, comma 2-quater, CAD devono essere utilizzati per “l’accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica”, ma ciò non implica affatto che, a valle dell’identificazione, la fase di autenticazione non possa essere garantita con modalità informatiche diverse.

⁷⁵ Cfr. art. 64-quater, comma 7 CAD ove si stabilisce che “*Nelle more della piena funzionalità del Sistema IT-Wallet, sono rese disponibili, a richiesta, attraverso il punto di accesso telematico di cui all’articolo 64-bis, le versioni digitali della Tessera sanitaria - Tessera europea di assicurazione di malattia (TS/TEAM), della patente di guida mobile e della Carta europea della disabilità. La verifica di validità di tali versioni digitali è consentita, anche a soggetti terzi, mediante funzionalità rese disponibili dal punto di accesso telematico [...]*”.

⁷⁶ Allo stato attuale, si registrano 6,4 milioni di utenti dell’IT Wallet e oltre 10,6 milioni di documenti digitali attivati (patenti, tessere sanitarie, carte europee della disabilità). Si tratta di dati dichiarati dal Sottosegretario Butti con comunicato sulla firma delle proroghe delle convenzioni tra l’Agenzia per l’Italia Digitale e gli *identity provider* per la gestione dello SPID del 7 ottobre 2025 e che testimoniano un’adozione rapida di questo nuovo strumento introdotto nell’app IO.

3.5. Il diritto a servizi digitali semplici, sicuri e integrati.

Il Codice dell'amministrazione digitale, come già anticipato, dedica altresì una disposizione al diritto ai servizi digitali. In particolare, l'art. 7 CAD ha una particolare rubrica, che parla di "diritto a servizi on-line semplici e integrati".

In particolare, prevede il diritto soggettivo pieno di chiunque di fruire dei servizi erogati dai soggetti di cui all'art. 2, comma 2, in forma digitale e in modo integrato, tramite gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso telematico, anche attraverso dispositivi mobili degli utenti secondo i livelli di qualità individuati e periodicamente aggiornati dall'AGID con proprie Linee guida, tenuto anche conto dell'evoluzione tecnologica.

L'obiettivo primario dell'art. 7 è rendere effettivi i diritti di cittadinanza digitale, favorendo interoperabilità e integrazione dei servizi pubblici, che devono essere resi agli utenti in modo semplice e *mobile oriented*.

Come si approfondirà nel prosieguo, al fine di rendere effettivo il diritto in oggetto, l'art. 64-bis, al comma 1-bis, prevede che "*i soggetti di cui all'articolo 2, comma 2, i fornitori di identità digitali e i prestatori dei servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con i servizi di cui ai commi 1 e 1-ter, espongono per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida*". Al fine di incentivare ulteriormente il tema, il Decreto "Semplificazioni" ha ribadito, con la modifica del comma 1-quater della stessa disposizione, che le pubbliche amministrazioni in senso stretto devono rendere fruibili tutti i loro servizi anche in modalità digitale e a tal fine - con un'espressione che è stata poco compresa dai commentatori - che dovevano "*avviare i relativi progetti di trasformazione digitale*" entro il 28 febbraio 2021.

Aggiunge che, per i servizi in rete, i soggetti di cui all'art. 2, comma 2, devono consentire agli utenti di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso all'utente stesso e pubblicano sui propri siti i dati risultanti, ivi incluse le statistiche di utilizzo.

Peraltro, si noti che la rubrica originaria dell'art. 7 era "*Qualità dei servizi resi e soddisfazione dell'utenza*", circostanza che ha portato i commentatori a considerare questa disposizione come "*prima e piena esplicita affermazione della rilevanza della c.d. "customer satisfaction" del diritto amministrativo e della dichiarata comparazione tra pa e imprese erogatrici di servizi al pubblico*"⁷⁷. Nonostante

⁷⁷ C. Boccia – C. Contessa – E. De Giovanni, *Codice dell'Amministrazione digitale. D.L. gs 7 marzo 2005, n. 82 commentato e annotato per articolo*, cit., 77.

le intenzioni del Legislatore, a distanza di anni dall'introduzione di questa disposizione e alla luce delle moltissime modifiche che nel tempo sono state apportate alla sua formulazione, va rilevato che la norma non ha raggiunto i risultati sperati. L'analisi dei dati rileva, infatti, che la maggior parte degli enti pubblici, laddove offre servizi online, non rileva il grado di soddisfazione degli utenti⁷⁸.

A tale proposito, di particolare interesse è quanto previsto dal comma 3 dell'art. 7 CAD. La disposizione stabilisce infatti che, in caso di violazione degli obblighi ivi contemplati, gli utenti – fermo restando il diritto di adire il difensore civico digitale di cui all'art. 17 – possono promuovere un'azione giudiziaria, anche secondo i termini e le modalità previste dal d.lgs. 20 dicembre 2009, n. 198. Si tratta della *class action* amministrativa, uno strumento sul quale si tornerà in seguito, nell'ambito dell'analisi dei mezzi progressivamente introdotti a garanzia dell'effettività dei diritti digitali.

3.6. L'Anagrafe nazionale della popolazione residente (ANPR) come piattaforma che attesta attributi.

Come anticipato⁷⁹, nell'ambito della presente trattazione assume particolare rilevanza l'Anagrafe nazionale della popolazione residente (ANPR), non solo quale esito della digitalizzazione del registro anagrafico, ma soprattutto nella sua funzione più evoluta di rendere disponibili i dati a cittadini e pubbliche amministrazioni. Tale sistema consente di razionalizzare i servizi offerti alle amministrazioni e di semplificare, grazie all'impiego delle tecnologie digitali, l'interazione tra cittadini e PA. Proprio in questa sua veste viene inserita nell'ultimo aggiornamento del piano triennale per l'informatica nella pubblica amministrazione nell'ambito della sezione relativa alle "piattaforme che attestano attributi"⁸⁰. Nel Piano si legge peraltro che "*ANPR si sta integrando con le anagrafi settoriali del lavoro, della pensione e del welfare e ogni nuova anagrafe che abbia come riferimento la popolazione residente sarà logicamente integrata con ANPR*" e il documento reca un approfondimento, tra le altre piattaforme che attestano attributi, sull'integrazione di ANPR con l'Anagrafe nazionale dell'istruzione (ANIST) e con l'Anagrafe nazionale dell'istruzione superiore (ANIS).

Tale sistema è stato istituito, a norma dell'art. 62 del CAD, presso il Ministero dell'Interno con il Decreto del Presidente del Consiglio dei Ministri n. 108 del 2013⁸¹.

⁷⁸ Cfr. i dati forniti dall'Osservatorio Agenda digitale del Politecnico di Milano del 16 ottobre 2025 sulla Maturità dei Comuni italiani.

⁷⁹ Cfr. *supra* cap. I.

⁸⁰ Cfr. piano triennale per l'informatica nella pubblica Amministrazione 2024-2026, agg. 2026, spec. 118 ss. Nel Piano si fa esplicito riferimento a piattaforme che "hanno la caratteristica di attestare attributi anagrafici e di settore".

⁸¹ Cfr. art. 62, comma 1, CAD ove si legge che "*È istituita presso il Ministero dell'interno l'ANPR, quale base di dati di interesse nazionale, ai sensi dell'articolo 60, che subentra all'Indice*

Allo stato, tutti i comuni italiani, anche grazie a politiche governative particolarmente riuscite, risultano subentrati in ANPR⁸².

L'ANPR si configura come un sistema integrato che consente ai Comuni di gestire i servizi anagrafici, di consultare e di estrarre dati, nonché di monitorare le attività e di produrre statistiche⁸³. La sua rilevanza principale, però, risiede nella capacità di aggregare in modo continuativo, mediante gli aggiornamenti inseriti costantemente da parte dei Comuni, l'insieme dei dati anagrafici relativi ai cittadini residenti in Italia e ai cittadini italiani residenti all'estero. Tale archivio costituisce un patrimonio informativo certo, accessibile, affidabile e sicuro, sul quale è possibile fondare lo sviluppo di servizi integrati e avanzati volti a ottimizzare e rendere più efficienti le interazioni tra pubbliche amministrazioni e cittadini.

Le modalità di attuazione, il funzionamento e il progressivo piano di subentro dei Comuni sono stati definiti dal Decreto del Presidente del Consiglio dei ministri n. 194 del 10 novembre 2014.

Con le modifiche apportate all'art. 62 del CAD, è stato previsto che ANPR contenga, oltre ai dati anagrafici, anche l'archivio nazionale informatizzato dei registri di Stato civile e i dati delle liste di leva⁸⁴.

nazionale delle anagrafi (INA), istituito ai sensi del quinto comma dell'articolo 1 della legge 24 dicembre 1954, n. 1228, recante "Ordinamento delle anagrafi della popolazione residente" e all'Anagrafe della popolazione italiana residente all'estero (AIRE), istituita ai sensi della legge 27 ottobre 1988, n. 470, recante "Anagrafe e censimento degli italiani all'estero" Tale base di dati è sottoposta ad un audit di sicurezza con cadenza annuale in conformità alle regole tecniche di cui all'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del Garante per la protezione dei dati personali".

⁸² L'art. 62, comma 2 CAD stabilisce che "Ferme restando le attribuzioni del sindaco di cui all'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali, approvato con il decreto legislativo 18 agosto 2000, n. 267, l'ANPR subentra altresì alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Con il decreto di cui al comma 6 è definito un piano per il graduale subentro dell'ANPR alle citate anagrafi, da completare entro il 31 dicembre 2014. Fino alla completa attuazione di detto piano, l'ANPR acquisisce automaticamente in via telematica i dati contenuti nelle anagrafi tenute dai comuni per i quali non è ancora avvenuto il subentro. L'ANPR è organizzata secondo modalità funzionali e operative che garantiscono la univocità dei dati stessi".

⁸³ Cfr. art. 62, comma 3, CAD: "L'ANPR assicura ai comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, e mette a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale".

⁸⁴ Cfr. art. 62, comma 2-bis CAD dove si prevede che "L'ANPR contiene altresì l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni garantendo agli stessi, anche progressivamente, i servizi necessari all'utilizzo del medesimo e fornisce i dati ai fini della tenuta delle liste di cui all'articolo 1931 del codice dell'ordinamento militare di cui al decreto legislativo 15 marzo 2010, n. 66, secondo le modalità definite con uno o più decreti di cui al comma 6-bis. Le modalità e i tempi di adesione da parte dei comuni all'archivio nazionale informatizzato, con conseguente dismissione della versione analogica dei registri di stato civile, sono definiti con uno o più decreti di cui al comma 6-bis". A partire da ottobre 2023, alcuni Comuni pilota hanno iniziato a utilizzare i servizi messi a disposizione dall'ANPR per lo stato civile e, ad oggi, oltre cinquecento Comuni impiegano tali servizi. L'integrazione di ANPR con i servizi dello Stato civile digitale rappresenterà un rilevante strumento di semplificazione per Comuni e cittadini. Il progetto prevede la

Per effetto delle modifiche all'art. 62 del CAD apportate dal Decreto “Semplificazioni”, è stata prevista l'attribuzione ad ogni cittadino di un codice identificativo unico in ANPR al fine di facilitare l'interoperabilità e l'integrazione con le altre banche dati della PA e dei gestori di servizi pubblici.

I servizi attualmente disponibili per i cittadini sono quelli che consentono di: visualizzare i propri dati anagrafici; effettuare una richiesta di rettifica per errori materiali; richiedere autocertificazioni precompilate con i dati anagrafici presenti in ANPR; richiedere un certificato anagrafico in bollo o in esenzione (sono disponibili 15 tipologie differenti di certificati)⁸⁵; comunicare un cambio di residenza; visualizzare il proprio domicilio digitale, costantemente allineato con l'Indice Nazionale dei Domicili Digitali (INAD); comunicare un punto di contatto (mail o telefono). A ciò si aggiunge, che, a partire da dicembre 2022, sono stati resi disponibili i servizi che consentono ai Comuni di trasmettere e aggiornare costantemente anche i dati elettorali dei cittadini in ANPR con conseguenti ulteriori servizi per i cittadini e per i Comuni⁸⁶.

Nel contesto descritto, le disposizioni dell'art. 62 del CAD sono state successivamente modificate ad opera dell'art. 27, comma 1, lettera e), numero 1), del d.l. 6 novembre 2021, n. 152.

Vale la pena richiamare integralmente il testo dell'art. 62, comma 3, CAD che, nella versione attualmente vigente, dispone: “[...] *Al fine dello svolgimento delle proprie funzioni, anche ampliando l'offerta dei servizi erogati on-line a cittadini e imprese, direttamente o tramite soggetti affidatari dei servizi, il Comune può utilizzare i dati anagrafici eventualmente detenuti localmente e costantemente allineati con ANPR al fine esclusivo di erogare o usufruire di servizi o funzionalità non fornite da ANPR. I Comuni accedono alle informazioni anagrafiche contenute in ANPR, nel rispetto delle disposizioni in materia di protezione dei dati personali e delle misure di sicurezza definite con decreto del Presidente del Consiglio dei ministri ai sensi del comma 6, lettera a), per l'espletamento, anche con modalità*

completa digitalizzazione dei registri dello Stato civile gestiti dai Comuni — relativi a nascita, matrimonio, unione civile, cittadinanza e morte — con l'eliminazione dei tradizionali registri cartacei. Gli atti digitali saranno conservati in un archivio nazionale centralizzato presso il Ministero dell'Interno, garantendo la consultazione a livello nazionale e permettendo il rilascio di estratti o certificati direttamente dal sistema centrale, senza necessità di rivolgersi al Comune di origine.

⁸⁵ Cfr. comunicazione del Ministero dell'Interno consultabile a [questo link](#). Con riferimento, in particolare, al rilascio dei certificati anagrafici, è opportuno rilevare che, come annunciato dal Ministero dell'Interno, dal 15 novembre 2021, attraverso il portale ANPR, è possibile per i cittadini ottenere, mediante accesso diretto al servizio, i seguenti certificati: anagrafico di nascita; anagrafico di matrimonio; di cittadinanza; di esistenza in vita; di residenza; di residenza AIRE; di stato civile; di stato di famiglia; di stato di famiglia e di stato civile; di residenza in convivenza; di stato di famiglia AIRE; di stato di famiglia con rapporti di parentela; di stato Libero; anagrafico di unione civile; di contratto di convivenza.

⁸⁶ Cfr. art. 62, comma 2-ter CAD: “*Con uno o più decreti di cui al comma 6-bis sono definite le modalità di integrazione nell'ANPR delle liste elettorali e dei dati relativi all'iscrizione nelle liste di sezione di cui al decreto del Presidente della Repubblica 20 marzo 1967, n. 223*”.

automatiche, delle verifiche necessarie all'erogazione dei propri servizi e allo svolgimento delle proprie funzioni. L'ANPR consente ai comuni la certificazione dei dati anagrafici nel rispetto di quanto previsto dall'articolo 33 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, anche in modalità telematica."⁸⁷.

Pertanto, alla luce delle disposizioni sopra richiamate, nonché dell'annuncio concernente l'attivazione del servizio, si deve ritenere che a partire dal 15 novembre 2021: i Comuni, per rilasciare le tipologie di certificati sopra indicate, devono necessariamente consultare i dati in ANPR e non i propri dati anagrafici locali; i Comuni possono utilizzare i dati anagrafici detenuti localmente con ANPR al fine esclusivo di erogare o usufruire di servizi o funzionalità non fornite da ANPR. Tali dati, peraltro, dovranno essere costantemente allineati con ANPR; non muta il regime del diritto al rilascio dei certificati anagrafici, sia che la richiesta rivolta al Comune abbia ad oggetto certificati ottenibili tramite ANPR, sia che invece riguardi certificati diversi ed emessi consultando dati anagrafici locali. Pertanto, la normativa di riferimento rimane quella contenuta del richiamato regolamento di cui al DPR 223/1989 e, in particolare, il disposto dell'art. 33, comma 1, che attribuisce a chiunque il diritto di fare richiesta dei certificati, "Fatti salvi i divieti di comunicazione di dati, stabiliti da speciali disposizioni di legge, e quanto previsto dall'articolo 35", norma che disciplina il contenuto dei certificati anagrafici.

Di estremo rilievo per la presente trattazione è anche quanto previsto nell'ultima parte del comma 3 dell'art. 62 CAD, quando afferma che "*I comuni inoltre possono consentire, mediante la piattaforma di cui all'articolo 50-ter ovvero anche mediante apposite convenzioni, la fruizione dei dati anagrafici da parte dei soggetti aventi diritto. L'ANPR assicura ai soggetti di cui all'articolo 2, comma 2, lettere a) e b), l'accesso ai dati contenuti nell'ANPR. L'ANPR attribuisce a ciascun cittadino un codice identificativo univoco per garantire la circolarità dei dati anagrafici e l'interoperabilità con le altre banche dati delle pubbliche amministrazioni e dei gestori di servizi pubblici di cui all'articolo 2, comma 2, lettere a) e b)*".

⁸⁷ Come previsto dall'art. 1, d.P.R. 30 maggio 1989, n. 223 (Nuovo regolamento anagrafico della popolazione residente), introdotto dal d.P.R. 17 luglio 2015, n. 126, gli adempimenti anagrafici previsti dal regolamento sono effettuati in ANPR (Anagrafe Nazionale della Popolazione Residente), di cui all'art. 62 d.lgs. n. 82/2005 (CAD). Tra gli adempimenti anagrafici previsti vi sono quelli concernenti il rilascio di certificati anagrafici, disciplinati dall'art. 33, d.P.R. n. 223/1989, che al comma 1 prevede che "*l'ufficiale di anagrafe rilascia a chiunque ne faccia richiesta, previa identificazione, i certificati concernenti la residenza, lo stato di famiglia degli iscritti nell'anagrafe nazionale della popolazione residente, nonché ogni altra informazione ivi contenuta*". Il successivo comma 2, come recentemente modificato ad opera dell'art. 30, comma 2, lettera b), del d.l. 16 luglio 2020, n. 76 (c.d. "Decreto semplificazioni 2020", conv., con mod. dalla l. n. 120/2020), precisa che "*Al rilascio di cui al comma 1 provvedono anche gli ufficiali d'anagrafe di comuni diversi da quello in cui risiede la persona cui i certificati si riferiscono. Il rilascio di certificati anagrafici in modalità telematica è effettuato mediante i servizi dell'ANPR con le modalità indicate nell'articolo 62, comma 3, del decreto legislativo 7 marzo 2005 n. 82, e si applica a decorrere dall'attivazione del relativo servizio da parte del Ministero dell'interno e di Sogei S.p.a.*".

Come già evidenziato, il progetto ANPR non si limita alla mera digitalizzazione del registro anagrafico, bensì realizza una piattaforma certificativa degli attributi dei cittadini che, grazie ai meccanismi di interoperabilità, mira a semplificare l'interazione tra cittadino e pubblica amministrazione. Tale sistema dovrebbe, a tendere e anche grazie al progressivo sviluppo della Piattaforma Digitale Nazionale Dati (PDND)⁸⁸, dovrebbe consentire alle amministrazioni di erogare servizi digitali con dati anagrafici precompilati⁸⁹, evitando di richiedere ripetutamente le stesse informazioni al cittadino, in piena osservanza del principio del “*once only*”⁹⁰.

3.7. Gli strumenti di garanzia e tutela dei diritti digitali.

Come già rilevato nell'ambito del primo capitolo sul tema dell'identità personale, la principale criticità dei cc.dd. “nuovi diritti” o, in questo caso, dei diritti semplicemente “nuovi” o “ulteriori” è quella dell'effettività della loro tutela. Tanto vale anche, in generale, per tutti i diritti digitali, rispetto ai quali si registra una diffusa scarsa consapevolezza da parte degli utenti, sia della loro esistenza sia della possibilità di esercitarli.

In questo senso, negli anni sono stati profondamente rafforzati gli strumenti a tutela dei diritti digitali, compresa l'identità digitale, a fronte della loro eventuale violazione.

Gli strumenti per ottenere un rimedio a fronte della violazione dei diritti di cittadinanza digitale sono diversi.

⁸⁸ Al fine di consentire il pieno utilizzo delle basi dati di interesse nazionale da parte delle amministrazioni, l'art. 50-ter, CAD prevede l'istituzione della Piattaforma Digitale Nazionale Dati (PDND). L'adozione di tale infrastruttura digitale è volta a migliorare e semplificare l'interoperabilità e lo scambio dei dati pubblici tra pubbliche amministrazioni, standardizzare e promuovere la diffusione degli *open data*, ottimizzare i processi di analisi dati e generazione di sapere, nonché semplificare gli adempimenti amministrativi dei cittadini e delle imprese, in conformità alla disciplina vigente e agli accordi quadro previsti dall'art. 50.

⁸⁹ Per un approfondimento tecnico sulla relazione tra PDND e ANPR nella logica della precompilazione, cfr. catalogo API, consultabile al seguente indirizzo api.gov.it/it/esempi-pratici/dati-anagrafici-precompilati-per-servizi-piu-efficienti. Tra i casi pratici più recenti viene citato quello del Comune di Bordighera nel quale le famiglie che intendono usufruire del servizio di trasporto scolastico per i propri figli possono effettuare l'iscrizione direttamente online sul sito istituzionale. In passato, la procedura richiedeva l'inserimento manuale di tutti i dati anagrafici e familiari, l'allegazione dei documenti necessari e l'attesa dei controlli da parte degli uffici comunali. Attualmente, grazie all'integrazione tra le API dell'Anagrafe Nazionale della Popolazione Residente (ANPR) e i servizi digitali del Comune, la compilazione dei dati avviene automaticamente: al momento dell'iscrizione, il sistema recupera in tempo reale le informazioni relative alla residenza e allo stato di famiglia. Di conseguenza, l'utente deve soltanto confermare i dati e la pratica è immediatamente definita per essere gestita dagli uffici, eliminando passaggi aggiuntivi e potenziali errori di trascrizione. In proposito si veda anche il piano triennale per l'informatica nella pubblica amministrazione 2024-2026, spec. cap. III Servizi, E-Service in interoperabilità tramite PDND, 69 ss.

⁹⁰ Si tratta di un principio cardine della strategia nazionale secondo il quale la pubblica Amministrazione non deve chiedere a cittadini e imprese dati che già possiede. In particolare, è inserito al punto 8 dei principi guida del piano triennale per l'informatica nella pubblica Amministrazione 2024-2026 e viene definito come principio secondo il quale “le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite”.

Come anticipato, anzitutto, il d.l. 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, ha introdotto nel CAD il nuovo art. 18-bis, con cui sono stati rafforzati i poteri dell'AGID in materia di vigilanza, verifica, controllo e monitoraggio dell'attuazione degli obblighi di transizione digitale, nonché sono stati attribuiti alla medesima Agenzia significativi poteri sanzionatori nei confronti delle amministrazioni inadempienti⁹¹.

La norma mira a rafforzare la disciplina sanzionatoria in caso di violazione degli obblighi legati alla trasformazione digitale, al fine di assicurare l'attuazione dell'Agenda digitale italiana ed europea, nonché la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese, anche in base agli obiettivi fissati dal Piano Nazionale di Ripresa e Resilienza (PNRR).

In particolare, l'Agenzia può procedere d'ufficio o su segnalazione del difensore civico digitale⁹². Qualora ravvisi la violazione degli obblighi di cui alle norme espressamente indicate al comma 5 del nuovo art. 18-bis, può procedere alla contestazione e, qualora le violazioni vengano effettivamente accertate al termine della procedura, può comminare una sanzione amministrativa pecuniaria in misura proporzionale alla gravità della violazione accertata. In particolare, scaduti tutti i termini fissati per porvi rimedio, le amministrazioni possono ricevere una sanzione da 10.000 a 100.000 euro.

Le violazioni sanzionabili sono relative, in particolare a: gli obblighi in tema di pagamenti elettronici; gli obblighi in tema di servizi online (consentire agli utenti di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso e pubblicare sui propri siti i dati risultanti, ivi incluse le statistiche di utilizzo); gli obblighi legati alla formazione dei fascicoli informatici e alla consultazione degli stessi; gli obblighi legati alla conservazione ed esibizione dei documenti; l'obbligo di rendere disponibili i dati ai sensi

⁹¹ In attuazione di tale previsione normativa, AGID, con D.D.G. del 4 agosto 2025, n. 190, recante *“Regolamento recante le procedure di contestazione, accertamento, segnalazione e irrogazione delle sanzioni per le violazioni degli obblighi di transizione digitale di cui all'art. 18-bis del Codice dell'amministrazione digitale”*, ha adottato e pubblicato un nuovo Regolamento che sostituisce quello approvato con determinazione n. 270 del 18 ottobre 2022 (pubblicato in G.U. n. 264 dell'11 novembre 2022). Il Regolamento delinea un procedimento sanzionatorio completo, che si articola in un'attività preistruttoria di verifica (cfr. parte II) seguita eventualmente da un procedimento sanzionatorio (cfr. parte III).

⁹² Cfr. art. 17, comma 1-*quater*, CAD. La norma prevede l'istituzione presso l'AgID dell'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Prevede, poi, che *“Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Il difensore civico, accertata la non manifesta infondatezza della segnalazione, la trasmette al Direttore generale dell'AgID per l'esercizio dei poteri di cui all'articolo 18-bis”*. Nella formulazione vigente fino al 2021 era previsto un diverso ruolo del difensore civico, il quale, ricevuta una segnalazione e verificata la sua fondatezza, poteva direttamente trasmettere un invito all'Amministrazione inadempiente.

dell'art. 50 del CAD; l'obbligo di rendere disponibili e accessibili le basi dati ovvero i dati aggregati per il funzionamento della Piattaforma Digitale Nazionale Dati; l'obbligo di rendere accessibili i servizi tramite SPID, CIE e app IO; gli obblighi in materia di migrazione e razionalizzazione della spesa per i data center previsti dall'art. 33-*septies* del d.l. n. 179/2012; gli obblighi di comunicazione telematica di cui all'art. 3-*bis* del CAD.

La sanzione pecuniaria può essere comminata anche per la mancata ottemperanza alla richiesta di dati, documenti o informazioni effettuata dall'Agenzia nell'esercizio delle funzioni di vigilanza, verifica, controllo e monitoraggio, ovvero di trasmissione di informazioni o dati parziali o non veritieri. In questo caso, però, l'AGID potrà applicare la sanzione ridotta della metà.

Le violazioni accertate, inoltre, oltre ad essere pubblicate su un'apposita sezione del sito dell'AGID, incidono sulla valutazione della *performance* individuale dei dirigenti responsabili, comportando dunque responsabilità dirigenziale e disciplinare.

Quanto al difensore civico per il digitale attivo presso l'Agenzia per l'Italia Digitale, è sempre possibile presentare una segnalazione telematica allo stesso.

Il Difensore interviene su segnalazione presentata da un utente attraverso un form presente sul sito AGID. Se ritiene la segnalazione fondata, la trasmette al Direttore generale dell'AGID per l'esercizio dei poteri di vigilanza e sanzionatori sopra descritti.

Si tratta di un modo semplice, veloce e senza particolari oneri che chiunque può utilizzare per qualsiasi violazione delle norme in materia di digitalizzazione e innovazione della pubblica amministrazione (non solo quelle previste nel Codice dell'Amministrazione Digitale).

Con riferimento agli strumenti più squisitamente giudiziali, che, però, come noto, impongono maggiori oneri sia economici che organizzativi ai cittadini, nel caso in cui le amministrazioni non consentano l'uso delle tecnologie nelle comunicazioni e nei rapporti con gli utenti, questi ultimi possono anche ricorrere al Tribunale Amministrativo Regionale competente per territorio (come previsto dall'art. 3, comma 1-*ter*, d.lgs. n. 82/2005).

Infine, come anticipato, nel caso di violazione degli obblighi in materia di servizi online, più utenti possono agire in giudizio, promuovendo la *class action amministrativa*, condividendo i costi e i rischi del giudizio anche con il contributo di associazioni di consumatori e utenti⁹³.

⁹³ Giova ricordare che il d.lgs. 20 dicembre 2009, n. 198 ha introdotto nell'ordinamento italiano un'azione collettiva specificamente diretta nei confronti della pubblica amministrazione e dei concessionari di servizi pubblici, finalizzata a consentire a ciascun soggetto interessato di agire in giudizio per la tutela di interessi collettivi derivanti da inefficienze o disfunzioni nell'erogazione dei servizi. La disciplina processuale delineata dal decreto configura tale azione non come mera tutela di diritti individuali omogenei tipica dell'azione di classe consumeristica, ma come strumento volto alla salvaguardia di posizioni collettive indivisibili, caratterizzate dalla legittimazione autonoma delle associazioni rappresentative e dall'assenza del meccanismo dell'*opt-in*. Il procedimento, che

In tema di accessibilità, diritto digitale sancito dal CAD ma più approfonditamente dalla legge n. 4/2004 (c.d. “legge Stanca”), poi, esiste il “Meccanismo di *feedback*”, cioè uno strumento, come un *form* online, che rappresenta la prima istanza attraverso la quale il cittadino può notificare direttamente all’amministrazione eventuali difetti riscontrati nei siti web o nelle app. Al meccanismo di *feedback* si accede tramite link presente nella Dichiarazione di accessibilità pubblicata nel *footer* dei siti web o nella descrizione delle applicazioni presenti nello store.

In caso di violazione della disciplina in materia di protezione dei dati personali, infine, l’interessato può proporre reclamo al Garante per la protezione dei dati personali⁹⁴.

4. La dimensione sovranazionale del diritto all’identità digitale nella sua funzione identificativa.

L’aggiornamento del Regolamento eIDAS, tema cardine della presente trattazione, si colloca nel più ampio processo di progressiva europeizzazione delle discipline relative alla trasformazione digitale delle amministrazioni pubbliche⁹⁵.

L’espansione del mercato interno e il progressivo ampliamento delle funzioni dell’Unione europea hanno accresciuto l’incidenza della normativa sovranazionale sulle politiche interne di digitalizzazione, considerate leve essenziali per la piena integrazione socioeconomica dell’Unione.

Proprio la competenza sul mercato interno di cui all’art. 114 TFUE costituisce già da alcuni anni il fondamento giuridico dei più rilevanti interventi europei nel settore, inclusa la disciplina dell’identità digitale e dei servizi fiduciari.

deve essere preceduto da diffida, consente di intervenire nella fase stessa di produzione del servizio pubblico, ordinando al soggetto pubblico o al concessionario di porre rimedio al disservizio (art. 4), senza prevedere tuttavia un accertamento o un ristoro del danno patrimoniale eventualmente subito dagli utenti (art. 1, comma 6).

⁹⁴ Cfr. art. 77, Regolamento 2016/679/UE e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l’adeguamento dell’ordinamento nazionale al Regolamento. Il reclamo è lo strumento che consente all’interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali e di richiedere una verifica dell’Autorità. Sul punto cfr., in dottrina, A. Iannuzzi, *Le fonti del diritto dell’Unione europea per la disciplina della società digitale*, in F. Pizzetti (a cura di), *La Regolazione europea della società digitale*, Torino, 2024, 13 ss. L’Autore, dopo aver ricostruito l’ampia produzione dell’Unione europea in materia di tecnologie afferma che l’“UE sta realizzando una poderosa operazione di intervento normativo che sta producendo uno spostamento del baricentro della produzione legislativa, in questi ambiti, dall’autoregolazione privata al regolamento europeo” e saluta con favore l’intervento delle istituzioni che ha il merito di riportare al centro le fonti del diritto rispetto alle fonti elaborate dai poteri privati.

⁹⁵ Per un approfondimento sull’evoluzione della normativa europea in materia di trasformazione digitale cfr. E. Belisario, *Il regolamento eIDAS 2.0 e l’impatto sulla gestione documentale delle PA: quali prospettive?*, in G. Manca (a cura di), *Il regolamento eIDAS n. 2024/1183*, in *Riv. elettronica dir. econ. management*, n. spec. 4/2024, 33 ss.

Sebbene l'Unione non possieda una competenza diretta sull'organizzazione delle amministrazioni nazionali, il consolidato principio del primato del diritto europeo implica che le pubbliche amministrazioni siano tenute a rispettare direttamente le norme dell'UE relative alle tecnologie digitali.

Sul piano della tecnica normativa, si è consolidato il passaggio da strumenti di mera armonizzazione – principalmente direttive – a regolamenti direttamente applicabili, al fine di ridurre la frammentazione dei regimi giuridici nazionali, assicurare certezza del diritto e promuovere standard tecnologici uniformi⁹⁶.

L'ambizione relativa alla realizzazione di un vero e proprio mercato unico digitale comporta sfide significative; per questo l'Unione europea ha di recente avviato anche l'iniziativa politica e programmatica nota come “Decennio Digitale 2030”⁹⁷. Tale iniziativa mira a promuovere una visione sostenibile di società digitale, centrata sulla persona e da attuare entro il 2030, con l'obiettivo di potenziare i diritti e le competenze di cittadini e imprese nell'ambiente digitale.

Per quanto di rilievo in particolare con riferimento all'identificazione prodromica all'accesso ai servizi, il programma politico del Decennio Digitale prevede

⁹⁶ Tale passaggio è evidente anche facendo un parallelismo con la normativa in materia di protezione dei dati personali laddove il Regolamento 2016/679/UE ha abrogato la Direttiva 95/46/CE per le motivazioni espresse all'interno dei Considerando. Cfr. considerando 6 GDPR ove si legge che “*La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*”; nonché; il considerando 7 GDPR dove si afferma che “*Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche*”. Cfr., altresì, il considerando 9 GDPR che recita testualmente “*Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE*” e il considerando 10 ove si evidenzia che “*È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione*”.

⁹⁷ Per un approfondimento storico sulla disciplina europea della società digitale e sull'evoluzione del quadro politico-normativo di riferimento cfr. A. Iannuzzi, *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, cit., 10-11.

come obiettivo l'accessibilità online al 100% dei principali servizi pubblici⁹⁸. Ciò al fine di ampliare i diritti dei cittadini europei e assicurare agli stessi l'accesso ai servizi digitali, anche quando si trovano in altri Paesi membri⁹⁹. La questione dell'identificazione è evidentemente centrale per la realizzazione di tale obiettivo¹⁰⁰.

4.1. Il Regolamento (UE) 910/2014 (eIDAS).

Per una ricostruzione quanto più completa del tema non ci si può esimere dall'analizzare almeno l'ultimo decennio di regolazione europea sul tema e le vicende che hanno coinvolto a più riprese il Regolamento c.d. "eIDAS".

Come noto, il Regolamento (UE) n. 910/2014 per l'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno (meglio conosciuto come "eIDAS" (*electronic IDentification Authentication and Signature*)¹⁰¹ è stato emanato il 23 luglio 2014 e ha assunto piena efficacia dal 1 luglio 2016. Tale Regolamento ha abrogato la precedente Direttiva 1999/93/CEE, riprendendone e rafforzandone, tuttavia, il contenuto.

Nella comunicazione della Commissione europea inerente all'Agenda Digitale europea riportata nelle premesse del Regolamento si riscontra che all'epoca la frammentazione del mercato digitale era percepita come il grande ostacolo all'economia digitale e che "garantire un quadro normativo uniforme eliminerebbe la sfiducia verso gli ambienti telematici, derivante dall'incertezza giuridica attuale". Alla luce di questi obiettivi e in linea con il perseguimento di un adeguato livello di sicurezza, il Regolamento disciplina: "le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro; le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web".

Proprio per superare la disarmonia dei vari Stati su questi temi, il nuovo quadro giuridico viene riportato in un Regolamento, provvisto della forma immediatamente vincolante e applicabile da subito in tutti i suoi elementi in tutti gli Stati membri, senza necessità di recepimento.

⁹⁸ Cfr. anche Relazione sullo stato del decennio digitale 2025 consultabile al seguente indirizzo: digital-strategy.ec.europa.eu/it/library/state-digital-decade-2025-report.

⁹⁹ Per un approfondimento sul Decennio Digitale 2030, cfr., in dottrina, S. Nativi, *Le prospettive europee nel futuro prossimo*, in *Identità digitale, processo e rapporti tra privati*, cit., 464.

¹⁰⁰ Si noti che la strategia prevede altresì l'integrazione del Portafoglio europeo d'identità con il c.d. euro-digitale.

¹⁰¹ Cfr. Regolamento n. 910/2014/UE del Parlamento europeo e del Consiglio del 23 luglio 2014.

Il Regolamento affronta, dunque, principalmente, due materie, contigue ma separate: quella dell'identificazione elettronica (eID)¹⁰² e quella dei servizi fiduciari per le transazioni elettroniche¹⁰³ al fine dichiarato di eliminare le barriere relative al loro utilizzo.

In riferimento alla prima materia, il Regolamento punta alla “*eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri, almeno per l'autenticazione nei servizi pubblici*”. Si stabilisce il principio del riconoscimento reciproco dei mezzi di identificazione elettronica, che, però, è valido solo per quei regimi nazionali di identificazione elettronica che gli Stati membri liberamente decidano di notificare alla Commissione europea e solo in presenza di determinati presupposti.

Invece, per quanto concerne i servizi fiduciari per le transazioni elettroniche, il Regolamento istituisce un “*quadro giuridico generale*”: un insieme di regole comuni a livello europeo per il loro utilizzo. In quest'ambito, la finalità è quella di

¹⁰² Il Regolamento definisce “identificazione elettronica” il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentino un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenti una persona giuridica. Con l'espressione “mezzi di identificazione elettronica”, si riferisce a qualsiasi unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online, mentre costituisce un “regime di identificazione elettronica” qualsiasi sistema che fornisca i già menzionati mezzi. Strettamente collegato all'identificazione elettronica è l'“autenticazione”, definita dal Regolamento come un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità dei dati in forma elettronica. Il Regolamento stabilisce che ciascuno Stato membro, su base volontaria, possa notificare i sistemi di identificazione elettronica forniti ai cittadini e alle aziende per consentire un reciproco riconoscimento dei rispettivi mezzi di identificazione elettronica.

¹⁰³ Per quanto di interesse per la presente analisi, si ritiene opportuno riportare letteralmente le definizioni di “servizio fiduciario”, “prestatori di servizi fiduciari”, “servizio fiduciario qualificato” e “prestatori di servizi fiduciari qualificati”. In particolare, per “servizio fiduciario” si intende un servizio elettronico fornito solitamente dietro pagamento di un corrispettivo e consistente nei seguenti elementi: “*creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi*”; oppure “*creazione, verifica e convalida di certificati di autenticazione di siti web*”; ed infine “*conservazione di firme, sigilli o certificati elettronici relativi a tali servizi*”. Si ha qualificazione dei già menzionati servizi nel caso in cui siano soddisfatti i requisiti che il Regolamento detta e che attestano un livello di sicurezza predeterminato. Invece, per quanto concerne la definizione di “prestatore di servizi fiduciari”, il Regolamento stabilisce che si tratta di quella “*persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato*”. La posizione di prestatore di servizi fiduciari qualificati è da intendersi sulla base della valutazione compiuta da parte dell'Organismo di vigilanza nazionale. La procedura per ottenere la qualificazione è disciplinata dagli artt. 20 e ss. del Regolamento e si articola in più fasi: in un primo momento, è compiuta una notifica da parte del prestatore di servizi all'Organismo di vigilanza, alla quale è allegata una relazione di valutazione di conformità; l'Organismo di vigilanza verifica il contenuto della relazione e solo nel caso di conformità con le disposizioni del Regolamento eIDAS rilascia la qualifica. Una volta ottenuta, il prestatore di servizi qualificato risulta iscritto ad uno degli elenchi di fiducia pubblicamente consultabili e può utilizzare il marchio di fiducia UE per presentare in modo semplice, chiaro e riconoscibile i servizi qualificati. Ogni 24 mesi, il prestatore di servizi fiduciari qualificato è sottoposto ad una verifica da parte dell'organismo di valutazione di conformità, al fine di verificare la perdurante sussistenza dei requisiti di qualificazione.

“migliorare in particolare la fiducia delle piccole e medie imprese (PMI) e dei consumatori nel mercato interno, sono introdotte, tra l’altro, le nozioni di servizi fiduciari qualificati e di prestatori di servizi fiduciari qualificati, alle quali dovrebbe corrispondere un elevato livello di sicurezza”.

Hanno completato la disciplina recata da tale sistema normativo i diversi provvedimenti di attuazione adottati dalla Commissione europea¹⁰⁴.

Può essere utile considerare sin da ora che l’Italia, ai sensi del Regolamento eIDAS, ha notificato SPID per ciascuno dei tre livelli di garanzia (basso, significativo ed elevato) e CIE per il livello elevato. Gli altri paesi dell’Unione che lo hanno fatto, hanno notificato le proprie carte di identità elettroniche.

Nel contesto descritto, nell’ottobre 2020, il Consiglio europeo ha sottolineato l’esigenza di aggiornare il quadro normativo eIDAS, sollecitando la definizione di un sistema europeo che garantisse un’identificazione elettronica pubblica più sicura e uniforme. Ha quindi chiesto alla Commissione di presentare, entro la metà del 2021, una proposta che introducesse una soluzione interoperabile per dimostrare la propria identità online e gestire i relativi dati, permettendo così l’accesso ai servizi digitali pubblici, privati e disponibili oltreconfine.

Può essere utile precisare che, in realtà, i primi riferimenti ad un’identità unica europea si intravedono, già a partire dal 2020, nel discorso sullo stato dell’Unione della Presidente della Commissione europea¹⁰⁵.

La crescente interconnessione digitale tra gli Stati membri dell’Unione Europea, del resto, ha reso impellente la definizione di un quadro normativo comune anche per il riconoscimento delle persone nell’ambito digitale, al fine di superare le frammentazioni derivanti dai sistemi nazionali e garantire la piena operatività e validità giuridica dell’identità online in tutto lo spazio comunitario.

In assenza di tale armonizzazione che non era stata raggiunta nella vigenza del Regolamento eIDAS, le identità digitali rilasciate in uno Stato membro hanno il limite di non essere riconosciute altrove, ostacolando l’accesso a servizi pubblici e privati, la partecipazione economica transfrontaliera e la tutela dei diritti fondamentali dei cittadini¹⁰⁶.

Il 3 giugno 2021 la Commissione ha risposto a tale richiesta adottando la proposta di Regolamento sull’identità digitale europea. Il testo intende aggiornare

¹⁰⁴ Consultabili al presente indirizzo: www.agid.gov.it/it/piattaforme/eidas/atti-esecutivi-eidas

¹⁰⁵ Nel discorso del 16 settembre 2020 si legge che *“Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used”*. Per il testo integrale si rinvia a ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

¹⁰⁶ Dalla relazione che accompagna la proposta di Regolamento del Parlamento europeo e del Consiglio, volta a modificare il regolamento n. 910/2014/UE per definire un quadro comune per l’identità digitale europea, si rileva che, a seguito dell’entrata in vigore del regolamento eIDAS, solo 14 Stati membri hanno notificato l’adozione ufficiale di 19 sistemi di identificazione elettronica.

il Regolamento eIDAS del 2014 – che, come esposto, aveva gettato le basi per un accesso sicuro ai servizi digitali e alle transazioni online in tutta l’Unione – e introduce come elemento cardine il portafoglio europeo di identità digitale. Nello stesso giorno la Commissione ha pubblicato anche una Raccomandazione volta a sviluppare un “Toolbox” comune dell’UE, così da favorire un percorso coordinato verso un nuovo quadro europeo per l’identità digitale¹⁰⁷.

4.2. Il Regolamento (UE) 2024/1183 (eIDAS2) e la costruzione dell’identità digitale europea.

Il 20 maggio 2024 è entrato in vigore il Regolamento Europeo 2024/1183 dell’11 aprile 2024 (GU 30 aprile 2024), c.d. “eIDAS2” (Electronic Identification And trust Services, in seguito anche “Regolamento eIDAS2”)¹⁰⁸, che modifica il Regolamento Europeo n. 910/2014 per quanto riguarda l’istituzione del quadro relativo a un’identità digitale europea¹⁰⁹.

Il Regolamento eIDAS2 si conforma in modo significativo alle evoluzioni tecnologiche, mira a garantire un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari utilizzati in tutta l’Unione, al fine di consentire e facilitare l’esercizio, da parte delle persone fisiche e giuridiche, del diritto di partecipare in modo sicuro alla società digitale e di accedere ai servizi pubblici e privati online in tutta l’Unione.

Il testo di eIDAS viene modificato o integrato ma non abrogato sulla base di quanto emerso dalla consultazione del 2020, nell’ambito della quale erano state approfondite le criticità che hanno portato, nella vigenza del Regolamento, a non raggiungere gli obiettivi prefissati¹¹⁰.

Più in particolare, il nuovo regolamento ha impatti significativi sui comportamenti digitali di cittadini, imprese e professionisti, tra cui si evidenzia il portafoglio europeo di identità digitale, che introduce un’identità digitale unica, sicura e

¹⁰⁷ La Commissione europea ha rivolto agli Stati membri la *Commission Recommendation 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework* con la quale si raccomandava agli Stati membri di adoperarsi per lo sviluppo di una serie di strumenti a sostegno dell’attuazione del quadro europeo in materia di identità digitale, in stretta collaborazione con la Commissione e, se del caso, con altre parti interessate del settore pubblico e privato.

¹⁰⁸ Cfr. Regulation 2024/1183/UE of the European Parliament and of the Council of 11 April 2024 amending Regulation 910/2014/UE as regards establishing the European Digital Identity Framework..

¹⁰⁹ Per un approfondimento sulle tappe fondamentali del processo legislativo di revisione del Regolamento eIDAS, cfr. *Report eIDAS2 ed EUDI Wallet: quadro normativo e traiettorie di innovazione digitale europea*, Osservatori digital innovation del Politecnico di Milano del 25 ottobre 2025. Il report opta per una efficace suddivisione in tre filoni: normativo, relativo agli sviluppi degli atti di esecuzione; tecnico, attinente all’Architecture and Reference Framework (ARF); implementativo, relativo ai Large Scale Pilots (LSPs).

¹¹⁰ Dalla consultazione sono emerse diverse criticità: la struttura dell’atto, la sua scarsa applicazione pratica, l’evoluzione del contesto tecnologico e il cambiamento delle aspettative degli utenti.

interoperabile a livello comunitario, e l’inserimento della conservazione a norma tra i servizi fiduciari qualificati, con il riconoscimento degli effetti giuridici e dell’ammissibilità come prova in giudizio di dati, documenti elettronici e documenti analogici trasformati in digitale tramite scansione elettronica, se conservati mediante un servizio di archiviazione elettronica.

Il Regolamento, inoltre, prevede la revisione e l’ampliamento di diversi servizi fiduciari ovvero: la registrazione di dati elettronici in un registro elettronico (volta a garantire l’integrità delle stesse registrazioni e l’accuratezza del relativo ordine cronologico), il rilascio e la convalida di attestati elettronici di attributi, la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza; alla prestazione di servizi elettronici di recapito certificato si aggiunge, inoltre, la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove (certificati di autenticazione di siti web). I nuovi servizi fiduciari rappresentano, in effetti, una naturale evoluzione derivante dall’introduzione del portafoglio digitale europeo, risultando essenziali per lo sviluppo e la diffusione dell’identità digitale¹¹¹.

Infine, il Regolamento definisce nuove e possibili sanzioni per i prestatori di servizi fiduciari qualificati e anche per i non qualificati. Tali sanzioni sono stabilite da ciascuno Stato membro, nel rispetto dei principi di proporzionalità, effettività e dissuasività.

4.3. L’European Digital Identity Wallet (EUDI Wallet).

Come anticipato, tra le principali novità, il Regolamento eIDAS2 introduce il portafoglio europeo di identità digitale (European Digital Identity Wallet – di seguito anche “EDIW”, “EUDI Wallet” o “EU Wallet”), definito come *“un mezzo di identificazione elettronica, che consente all’utente di archiviare, gestire e convalidare in modo sicuro i dati di identità e attestazioni elettroniche degli attributi, per fornirli alle parti che ne fanno affidamento e ad altri utenti dei Portafogli Europei di Identità Digitale e di firmare tramite firme elettroniche qualificate o di sigillare tramite sigilli elettronici qualificati”*¹¹².

Il Regolamento mira a risolvere la disarmonia esistente tra i diversi Stati membri dell’Unione europea in relazione allo sviluppo e all’interoperabilità dei sistemi nazionali di identificazione elettronica¹¹³. A tal fine, configura in capo agli

¹¹¹ Cfr. G. Manca, *Sanità digitale. Manuale pratico per la gestione di identità, dati e documenti alla luce del regolamento eIDAS*, Roma, 2025, 30.

¹¹² Cfr. art. 3, § 42, eIDAS2.

¹¹³ L’obiettivo si evince dal considerando 5, che parla dell’istituzione di *“un quadro europeo relativo a un’identità digitale che consenta ai cittadini e ai residenti dell’Unione di accedere a servizi pubblici e privati online e offline in tutta l’Unione”*. L’obiettivo dichiarato nel Considerando 6 è di ridurre *“gli ostacoli digitali tra gli Stati membri e consentendo ai cittadini e ai residenti dell’Unione di godere dei vantaggi della digitalizzazione, aumentando nel contempo la trasparenza e la protezione dei loro diritti”*.

Stati membri l'obbligo di fornire ai propri cittadini e alle imprese un portafoglio europeo di identità digitale, sviluppato sulla base delle stesse specifiche normative, entro la fine del 2026, ovvero entro 24 mesi dalla data di entrata in vigore degli atti di esecuzione che la Commissione europea era tenuta ad adottare entro il 21 novembre 2024. Gli atti di esecuzione¹¹⁴, a cui si aggiungono *architecture and reference framework* (ARF) Large Scale Pilots (LSPs), che definiscono standard e procedure, rappresentano lo strumento essenziale per rendere operative le previsioni del Regolamento.

Quanto al funzionamento, tale strumento consente ai cittadini dell'Unione, senza alcun onere economico, di trasferire – sia in modalità connessa sia in assenza di rete – in modo selettivo e protetto, i propri dati identificativi, nonché eventuali ulteriori attestazioni elettroniche relative a specifici attributi personali (ad esempio, titoli di studio, abilitazioni professionali, certificati di stato civile), alle cc.dd. “relying parties”¹¹⁵ o al portafoglio europeo digitale di un terzo soggetto. Il portafoglio rende inoltre possibile l'apposizione di firme elettroniche qualificate o di sigilli elettronici. La funzionalità offline assume particolare rilievo nei rapporti che prevedono un'interazione fisica tra le parti.

Il modello è chiaramente ispirato all'esperienza maturata con gli *electronic payment wallet* – come Apple Pay o Google Wallet – introdotti dai principali fornitori di dispositivi mobili. Questi strumenti hanno dimostrato l'efficacia di un approccio digitale alla gestione di credenziali e strumenti di pagamento: un unico contenitore sicuro, integrato nativamente nel dispositivo, in grado di sostituire o affiancare oggetti fisici come carte di credito o tessere. L'EDIW riprende questa logica, estendendola all'identità digitale e a un insieme molto più ampio di attributi personali. Non si tratta più soltanto di abilitare transazioni economiche, ma di permettere al cittadino di gestire e condividere in modo controllato dati certificati – dalla patente digitale ai titoli di studio, dalle prescrizioni mediche alle credenziali di accesso ai servizi pubblici e privati.

Il Wallet europeo nasce, dunque, dall'evoluzione di un paradigma già sperimentato nel mercato consumer, ma lo reinterpreta in chiave pubblica e regolamentata, con un livello più elevato di garanzie in termini di sovranità dell'utente sui propri dati (la persona decide quali informazioni condividere e con chi, evitando

¹¹⁴ Gli atti di esecuzione sono previsti dall'art. 290 TFUE e hanno la funzione di dettagliare le modalità tecniche e operative di applicazione. Il Regolamento individua circa quaranta atti, che devono essere adottati entro maggio 2026. Nell'ottobre 2025 risultano adottati sedici atti di esecuzione. Per un approfondimento, cfr. *Report eIDAS2 ed EUDI Wallet*, cit., 17 ss. In dottrina cfr. A. Caccia, *Il ruolo degli standard in eIDAS2*, in G. Manca (a cura di), *Il regolamento eIDAS n. 2024/1183*, cit., 9 ss.

¹¹⁵ Con l'espressione “*relying parties*” si identificano i soggetti, persone fisiche o giuridiche, che – previa iscrizione presso lo Stato membro di stabilimento – sono legittimati a basarsi sui dati e sugli attributi trasmessi attraverso i portafogli europei di identità digitale. Resta fermo che essi possono trattare unicamente le informazioni per le quali sia stato conferito uno specifico consenso o un'autorizzazione puntuale.

concentrazioni di dati in mano a grandi piattaforme), interoperabilità transfrontaliera (il portafoglio è riconosciuto e utilizzabile in tutti gli Stati membri dell'UE) e sicurezza e conformità normativa.

Considerata la complessità del testo normativo, ci si sofferma nel prosieguo sulla analisi delle sole disposizioni rilevanti ai fini della presente trattazione.

L'art. 5-*bis* del Regolamento, anzitutto, definisce chiaramente l'obiettivo del nuovo strumento: garantire a tutte le persone fisiche e giuridiche dell'Unione un accesso transfrontaliero sicuro, affidabile e continuo ai servizi pubblici e privati, assicurando, al contempo, che ciascun utente mantenga il pieno controllo sui propri dati personali. La disposizione prevede, infatti, che *“Al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso transfrontaliero sicuro, affidabile e senza interruzioni ai servizi pubblici e privati, pur avendo il pieno controllo sui propri dati, ciascuno Stato membro fornisce almeno un Portafoglio Europeo di identità digitale entro 24 mesi dall'entrata in vigore degli atti di esecuzione di cui al paragrafo 11 e all'articolo 6 quater, paragrafo 4. I portafogli europei di identità digitale sono forniti: a) direttamente da uno Stato membro; b) su mandato di uno Stato membro; c) indipendentemente da uno Stato membro ma riconosciuto da tale Stato membro”*.

Dalle disposizioni iniziali del testo normativo si ricavano, pertanto, rilevanti elementi relativi alle modalità operative di rilascio. In particolare: il EDIW è emesso obbligatoriamente entro 24 mesi dall'entrata in vigore delle regole tecniche e non del regolamento eIDAS2; l'utente, persona fisica o giuridica, deve avere il pieno controllo dei propri dati; se un EDIW è emesso da un soggetto privato, questo portafoglio deve essere riconosciuto dallo Stato membro di utilizzo.

Come si approfondirà, per favorire l'interoperabilità, il Regolamento introduce il principio del riconoscimento reciproco tra i portafogli digitali istituiti nei diversi Stati membri, stabilendo i requisiti necessari per la loro certificazione. Inoltre, viene sancito che il codice sorgente dei componenti software dell'applicazione dei portafogli europei di identità digitale debba essere rilasciato con licenza *open source*¹¹⁶.

Di particolare interesse per la presente analisi è che, trattandosi sempre di un diritto collegato alla cittadinanza digitale, l'uso del portafoglio non è obbligatorio ma facoltativo¹¹⁷. Ne consegue che l'accesso ai servizi pubblici e privati, nonché al mercato del lavoro e la libertà di impresa, non sono in alcun modo limitati o reso

¹¹⁶ Sempre il citato art. 5-*bis* del Regolamento, a tale proposito, prevede che *“Il codice sorgente dei componenti software dell'applicazione dei portafogli europei di identità digitale è caratterizzato da una licenza open source. Gli Stati membri possono prevedere che, per motivi debitamente giustificati, il codice sorgente di componenti specifici diversi da quelli installati sui dispositivi degli utenti non sia divulgato”*.

¹¹⁷ Cfr. art. 5-*bis*, § 15, eIDAS2.

svantaggiosi per le persone fisiche o giuridiche che non utilizzano i portafogli europei di identità digitale. Di conseguenza, resta possibile accedere ai servizi pubblici e privati tramite altri mezzi di identificazione e autenticazione esistenti.

Inoltre, l'utente ha il diritto di revocare gratuitamente la validità del proprio portafoglio europeo¹¹⁸, mantenendo così sempre il pieno controllo sull'uso dello stesso. Per chi decida di adottarlo, è prevista la possibilità di collegarlo alla propria identità digitale nazionale e di utilizzarlo per apporre firme elettroniche con valore legale, senza costi aggiuntivi.

Proseguendo con la disamina dell'art. 5-*bis*, bisogna rilevare che tale norma, al fine di garantire l'intuitività nell'utilizzo dell'EDIW, impone, al paragrafo 4, una serie di attività il cui agevole svolgimento deve essere consentito all'utente, tra cui: *a) richiedere, ottenere, selezionare, combinare, conservare, cancellare, condividere e presentare in modo sicuro, con il controllo esclusivo dell'utente, dati di identificazione personale e, se del caso, in combinazione con attestati elettronici di attributi, necessari per l'autenticazione delle parti facenti affidamento sulla certificazione online e, se del caso, in modalità offline, al fine di accedere ai servizi pubblici e privati, garantendo nel contempo che sia possibile la divulgazione selettiva dei dati; b) generare pseudonimi e conservarli in modo cifrato e locale all'interno del portafoglio europeo di identità digitale; c) autenticare in modo sicuro il portafoglio europeo di identità digitale di un'altra persona e ricevere e condividere dati di identificazione personale e attestati elettronici di attributi in modo sicuro tra i due portafogli europei di identità digitale; d) accedere a un registro di tutte le transazioni effettuate mediante il portafoglio europeo di identità digitale attraverso un pannello di gestione comune che consente all'utente di: i) visualizzare un elenco aggiornato delle parti facenti affidamento sulla certificazione con le quali l'utente ha stabilito una connessione e, se del caso, tutti i dati scambiati; ii) chiedere facilmente che una parte facente affidamento sulla certificazione cancelli i dati personali a norma dell'articolo 17 del regolamento (UE) 2016/679; iii) segnalare facilmente la parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente qualora sia ricevuta una richiesta di dati personali presumibilmente illecita o sospetta; e) firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati; f) scaricare, nella misura in cui ciò sia tecnicamente possibile, i dati dell'utente, gli attestati elettronici di attributi e le configurazioni; g) esercitare il diritto dell'utente alla portabilità dei dati".*

In ottica di tutela dei dati personali e di controllo sui flussi informativi, l'utente deve avere accesso a un registro completo di tutte le transazioni effettuate tramite l'EDIW. Tali dati vengono visualizzati attraverso un cruscotto, che mostra l'elenco aggiornato delle parti affidatarie con cui l'utente ha stabilito connessioni

¹¹⁸ Cfr. art. 5-*bis*, § 9, lett. a, eIDAS2.

e, ove pertinente, i dati scambiati. Attraverso lo stesso cruscotto, l'utente può richiedere la cancellazione dei propri dati personali alla parte detentrici (ai sensi dell'art. 17 GDPR) e segnalare al Garante per la protezione dei dati personali eventuali richieste ritenute sospette o illecite.

Il paragrafo 5, lett. g) dell'art. 5-*bis* prevede ulteriori requisiti che l'EDIW deve rispettare, tra i quali si rileva la necessità che questo portafoglio consenta a ciascun utente-persona fisica di apporre la propria firma elettronica qualificata a titolo gratuito e per impostazione predefinita. Il testo precisa subito dopo che gli Stati membri “*possono prevedere misure proporzionate per garantire che l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche sia limitato a scopi non professionali*”.

Il pieno controllo dell'utente sul proprio EDIW è sancito dal paragrafo 14 dell'art. 5-*bis*, il quale si occupa anche di definire limiti al potere di intervento da parte del fornitore del portafoglio in merito all'attività di raccolta di informazioni attinenti all'utilizzo dell'EDIW stesso. In questo senso, viene fissato un principio di logica separazione, in base al quale i dati personali relativi alla fornitura del portafoglio devono essere mantenuti “logicamente separati” da altri dati detenuti dal fornitore del servizio dell'EDIW¹¹⁹.

Il paragrafo 24 dell'art. 5-*bis* stabilisce invece i livelli di garanzia ai quali devono conformarsi i mezzi di identificazione utilizzati dagli utenti per accedere all'EDIW, richiedendo, come già anticipato, l'integrazione di un livello di garanzia elevato¹²⁰.

Qualora intenda avvalersi dell'EDIW per la fornitura di servizi pubblici o privati mediante interazione digitale¹²¹, la parte facente affidamento sulla certificazione si registra nello Stato membro in cui è stabilita e fornisce i seguenti dati: a) le informazioni necessarie per autenticarsi nei portafogli europei di identità digitale, che comprendono almeno: lo Stato membro in cui la parte facente affidamento sulla certificazione è stabilita; il nome della parte facente affidamento sulla certificazione e, se del caso, il suo numero di registrazione quale appare in un documento ufficiale,

¹¹⁹ Cfr. anche il considerando 14 del Regolamento, che richiede l'adozione di “*tecnologie che preservino la riservatezza, come ad esempio la dimostrazione a conoscenza zero. Tali metodi crittografici dovrebbero consentire a una parte facente affidamento sulla certificazione di convalidare la veridicità di una determinata dichiarazione sulla base dei dati di identificazione e dell'attestato di attributi della persona in questione, senza rivelare alcun dato su cui si basa tale dichiarazione, così da preservare la vita privata dell'utente*”. L'obiettivo enunciato anche nel Considerando 18 è di “*proteggere i cittadini e i residenti dell'Unione dall'uso non autorizzato o fraudolento dei portafogli europei di identità digitale al fine di garantire la fiducia negli stessi e la loro ampia diffusione*”.

¹²⁰ Cfr., in proposito, A. Mazzeo – M. Nastri, *Identificazione in rete: identità digitale e identità personale*, in *Identità digitale, processo e rapporti tra privati*, cit., 44 ss., i quali si soffermano sull'opportunità di optare per un livello “elevato” piuttosto che “significativo”, anche in ragione del fatto che “*in un sistema in cui l'identità digitale e l'identità personale finiscono per riunirsi e sovrapporsi a livello normativo e operativo, la certezza dell'identificazione assume un rilievo fondamentale*”. Gli Autori propongono anche lo scenario di graduazione dei livelli di sicurezza minimi rispetto alla tipologia ed al contesto di uso.

¹²¹ Cfr. art. 5-*quater*, eIDAS2.

unitamente ai dati di identificazione di tale documento ufficiale; b) i dati di contatto della parte facente affidamento sulla certificazione; c) l'uso previsto dei portafogli europei di identità digitale, compresa una indicazione dei dati che la parte facente affidamento sulla certificazione deve richiedere agli utenti.

L'art. 5-*quater* stabilisce un quadro organico per la certificazione dei portafogli europei di identità digitale. La certificazione dell'European Digital Identity Wallet - e dei regimi di identificazione elettronica corrispondenti - di conformità ai requisiti di cui ai richiamati paragrafi 4, 5, 8, 14 e 24 dell'art. 5-*bis* deve essere certificata da organismi appositamente designati dallo Stato membro di riferimento (a meno che i requisiti non attengano alla cybersecurity, nel qual caso si troverà applicazione l'apposita normativa di cui al regolamento (UE) 2019/881). La validità della certificazione così rilasciata si protrae per 5 anni, purché sia espletata con cadenza biennale una valutazione di vulnerabilità. Qualora si dovesse accertare l'esistenza di una vulnerabilità cui non sia stato apportato rimedio tempestivamente, la certificazione diviene automaticamente annullata. La certificazione di conformità ai requisiti richiesti dall'art. 5-*bis* in materia di dati personali, può intervenire a norma del GDPR, secondo il paragrafo 5, art. 5-*quater*.

Inoltre, l'art. 5-*sexies* interviene per definire le modalità di intervento nei casi di violazione o parziale compromissione dei wallet in questione. In tali casi, secondo il comma 1 della menzionata disposizione, lo Stato membro che ha fornito i portafogli interessati dalla violazione deve *“sospendere senza indebito ritardo la fornitura e l'uso di portafogli europei di identità digitale”*. Ove giustificato da particolare gravità della situazione, lo Stato membro potrà addirittura ritirare tempestivamente i portafogli in questione. Successivamente lo Stato membro dovrà provvedere ad informare: gli utenti interessati; i punti di contatto unici previamente nominati a norma dell'art. 46-*quater* del regolamento stesso; le parti che fanno affidamento sulla certificazione; la Commissione.

Nel caso in cui fosse difettato, nei tre mesi successivi alla sospensione, un intervento per sanare la compromessa integrità dei wallet, il successivo comma 2 prevede che lo Stato membro debba comunque provvedere nel senso di ritirare i portafogli, revocandone contestualmente la validità e dando relativo avviso ai soggetti sopra richiamati. Ove invece l'intervento sanatorio fosse intervenuto con successo, lo Stato membro ripristinerà la fornitura e l'utilizzo dei wallet, informandone tempestivamente gli stessi soggetti sopra elencati. Per una più precisa definizione delle procedure da seguire nei casi rientranti nell'art. 5-*sexies*, il comma 5 rimanda a futuri atti di esecuzione che doveva adottare la Commissione entro il 21 dicembre 2024.

Ebbene, come emerge dalla ricostruzione effettuata, il Regolamento eIDAS2 recepisce i principi della identità digitale decentralizzata (*decentralized identity*). Le caratteristiche di questa impostazione, che si differenzia da quella centralizzata o federata (come quella, ad esempio, di SPID), sono il controllo diretto

dell'utente, la possibilità di condividere solo le informazioni necessarie e la separazione dei vari attori in gioco¹²².

5. Il portafoglio italiano (IT Wallet) e i portafogli digitali sviluppati negli altri Stati membri: una prospettiva comparatistica.

Quanto all'Italia, l'esigenza di armonizzazione delle legislazioni nazionali nella materia in oggetto non poteva essere soddisfatta per effetto della sola entrata in vigore del Regolamento eIDAS2. Quest'ultimo si è infatti innestato nel quadro di diritto positivo già maturo e sopra ricostruito, che gravita attorno al Codice dell'Amministrazione digitale.

Come anticipato, la normativa sovranazionale al fine di superare la frammentazione delle identità digitali esistenti nei diversi Stati Membri, impone a ciascuno di essi di notificare alla Commissione entro il 2026 almeno un portafoglio digitale nazionale, da qualificare come "EUDI Wallet".

Tale Wallet dovrà rispettare gli specifici requisiti minimi di funzionalità, sicurezza e certificazione previsti dal Regolamento e sopra riepilogati.

Il portafoglio digitale pubblico italiano è stato istituito dal d.l. 2 marzo 2024, n. 19, convertito con legge n. 56 del 29 aprile 2024, nell'ambito delle misure di attuazione del PNRR.

All'interno del Codice dell'Amministrazione digitale, infatti, nell'ambito della sezione III, rubricata "Identità digitali, istanze e servizi on-line", è stato aggiunto l'art. 64-*quater* rubricato "Sistema di portafoglio digitale italiano - Sistema IT-Wallet".

Tale disposizione prevede che il Sistema di Portafoglio Digitale Italiano (IT-Wallet) viene istituito per rafforzare l'interoperabilità tra le banche dati pubbliche tramite la Piattaforma Digitale Nazionale Dati (PDND) e per favorire la diffusione dei servizi digitali offerti da soggetti pubblici e privati¹²³. Il sistema si compone di due elementi principali: un portafoglio digitale pubblico, accessibile tramite il punto di accesso telematico previsto dall'art. 64-*bis*, e portafogli digitali privati, sviluppati da operatori accreditati dall'AGID¹²⁴.

Per guidare l'implementazione e l'evoluzione del sistema, un decreto del Presidente del Consiglio dei ministri (o dell'Autorità delegata), su proposta dell'AGID e di concerto con i ministeri competenti, definirà le linee guida. Tali linee guida stabiliranno: le caratteristiche tecniche dei portafogli digitali e i servizi

¹²² Per un approfondimento, cfr. *Report eIDAS2 ed EUDI Wallet*, cit., 12-14. Nel report si evidenzia come questa impostazione avvicini eIDAS2 ai paradigmi di *self-sovereign identity* ma con la differenza che il Regolamento affianca al modello decentralizzato un forte presidio normativo (come, ad esempio, la certificazione dei wallet). Tale impostazione combina vantaggi della decentralizzazione e garanzie della fiducia istituzionale. Cfr., altresì, G. Manca, *Sanità digitale. Manuale pratico per la gestione di identità, dati e documenti alla luce del regolamento eIDAS*, cit., 37.

¹²³ Cfr. art. 64-*quater*, comma 1, CAD.

¹²⁴ Cfr. art. 64-*quater*, comma 2, CAD.

disponibili; le modalità di accreditamento dei fornitori privati; i servizi messi a disposizione di pubbliche amministrazioni e operatori privati per la gestione di attestazioni elettroniche (identità, prerogative, deleghe, licenze); gli standard di interoperabilità con banche dati pubbliche e sistemi informativi privati; le misure di sicurezza e affidabilità del sistema; e le modalità di pubblicazione del codice sorgente delle soluzioni software¹²⁵.

La realizzazione e gestione dell'infrastruttura tecnologica del sistema è affidata a due società pubbliche: una incaricata della gestione complessiva e l'altra responsabile della progettazione, rilascio, certificazione e verifica delle attestazioni elettroniche relative a identità, prerogative, deleghe, qualifiche e licenze, assicurandone la validità e il ciclo di vita. Gli oneri per i servizi di verifica forniti dagli Identity Provider pubblici sono coperti con risorse già disponibili¹²⁶.

Successivamente, un ulteriore decreto definirà: i compiti e le funzioni delle società incaricate, la data di avvio dell'IT-Wallet pubblico, i termini entro cui le pubbliche amministrazioni dovranno rendere disponibili i dati in formato digitale, la data di avvio dei portafogli privati accreditati e le eventuali forme di remunerazione dei servizi, mantenendo la gratuità del Wallet pubblico per cittadini e imprese¹²⁷.

La copertura finanziaria dell'intera infrastruttura prevede 102 milioni di euro per il triennio 2024-2026, di cui 69 milioni dal PNRR (Investimento 1.3 "Dati e interoperabilità") e 33 milioni dal Fondo per l'innovazione tecnologica e la digitalizzazione¹²⁸.

Infine, in attesa della piena operatività del sistema, come già anticipato, saranno rese disponibili in formato digitale la Tessera Sanitaria/Tessera Europea di Assicurazione Malattia (TS/TEAM), la patente di guida mobile e la Carta Europea della Disabilità, verificabili anche da soggetti terzi tramite la PDND. Tali documenti digitali hanno lo stesso valore legale dei corrispondenti documenti fisici. La patente digitale sarà inoltre valida come documento di identità e soddisferà gli obblighi previsti dal Codice della Strada per la circolazione sul territorio nazionale¹²⁹.

In linea con gli orientamenti europei, una volta raggiunta la maturità tecnica e la stabilità normativa necessarie, sarà possibile sviluppare ulteriori soluzioni provenienti anche dal settore privato, che potranno entrare a far parte dell'ecosistema dell'IT-Wallet solo se pienamente conformi alle regole tecniche europee e ai relativi standard di sicurezza informatica e protezione dei dati.

¹²⁵ Cfr. art. 64-*quater*, comma 3, CAD.

¹²⁶ Cfr. art. 64-*quater*, comma 4, CAD.

¹²⁷ Cfr. art. 64-*quater*, comma 5, CAD.

¹²⁸ Cfr. art. 64-*quater*, comma 6, CAD.

¹²⁹ Cfr. art. 64-*quater*, comma 7, CAD.

Infine, l'IT-Wallet consentirà agli utenti di autenticarsi in modo sicuro presso i servizi pubblici e privati, nazionali ed europei, e di condividere selettivamente attributi verificati e credenziali digitali, in piena coerenza con il quadro europeo dell'EUDI Wallet sopra descritto.

Quanto agli altri paesi, lo stato delle soluzioni di identità digitale in Europa si configura, alla luce della disciplina eIDAS2 e dell'imminente obbligo di implementazione del portafoglio digitale europeo entro il 2026, come un panorama articolato e differenziato, contraddistinto da livelli eterogenei di maturità tecnologica, penetrazione degli utenti e grado di integrazione normativa¹³⁰.

Nei Paesi del nord Europa, la Svezia con BankID¹³¹, la Danimarca con MitID¹³² e la Finlandia con Suomi.fi ID¹³³ rappresentano modelli paradigmatici di consolidata affidabilità digitale: tali sistemi, con tassi di adozione superiori al 70 % della popolazione adulta, consentono l'accesso a una pluralità di servizi pubblici e privati – dall'erogazione di prestazioni sanitarie alle transazioni finanziarie – con piena interoperabilità e garanzia di autenticazione forte, fungendo altresì da riferimento per l'armonizzazione europea dei requisiti di sicurezza e protezione dei dati personali. In generale, dunque, i Paesi nordici pur non avendo ancora definito una strategia per l'implementazione di eIDAS2, rappresentano casi in cui l'identità digitale è già largamente diffusa. Inoltre, la Commissione europea ha avviato quattro progetti pilota su larga scala per testare i casi d'uso dell'EUDIW, tutti i paesi nordici sono coinvolti in uno o più progetti pilota e due di essi sono guidati da un paese nordico, la Svezia (il progetto pilota EWC) e la Norvegia (il progetto pilota NO-BID)¹³⁴.

Analogamente, i Paesi baltici, e in particolare l'Estonia con la propria infrastruttura X-Road, forniscono quasi la totalità dei servizi pubblici in modalità digitale, configurandosi come benchmark internazionale per l'integrazione dei sistemi di identità digitale e la governance dei dati pubblici.

Tra i paesi dell'Europa centrale, il quadro è più eterogeneo. In Germania, il sistema di e-ID nazionale¹³⁵, sebbene istituito dal 2010, presenta una diffusione limitata tra la popolazione e un'adozione frammentaria. Per sviluppare il proprio

¹³⁰ I dati sono tratti da *Wallet and Agent Overview, a special interests group of the OpenWallet Foundation* (walletoverview.info/wallets).

¹³¹ Sebbene non sia un'iniziativa governativa diretta, è un sistema di identificazione elettronica basato sulle banche, usato dalla maggior parte della popolazione per accedere a servizi sia pubblici che privati. Il governo sta lavorando a un'alternativa pubblica per conformarsi all'EUDI.

¹³² Si tratta di un'infrastruttura di identità digitale nazionale che ha sostituito i sistemi precedenti ed è utilizzata universalmente per l'accesso sicuro ai servizi digitali (www.mitid.dk/en-gb/).

¹³³ Suomi.fi e-Identification è un servizio di identificazione condiviso per i servizi elettronici della pubblica amministrazione (www.suomi.fi/frontpage).

¹³⁴ Per un approfondimento sullo stato dell'arte dell'identità digitale in questi Paesi, oltre che in Islanda e Norvegia, cfr. *The state of digital identity in the Nordics 2024*.

¹³⁵ L'e-ID tedesca, o "eID card", è una carta d'identità elettronica (conosciuta anche come "Personalausweis" se si è cittadini tedeschi) e include una funzione di identificazione online.

wallet la Germania ha adottato un approccio innovativo, lanciando un concorso¹³⁶, che finanzia diversi prototipi per ispirare la creazione del Gov EUDI Wallet.

Austria e Svizzera, invece, hanno sviluppato soluzioni mobile-first – rispettivamente eID Austria¹³⁷, eAusweise¹³⁸ e Swiyu¹³⁹ – che, pur in contesti normativi differenti, perseguono obiettivi di interoperabilità e integrazione con servizi privati, in vista della piena compatibilità con il wallet europeo. Rispetto all’implementazione del wallet, l’Austria sta evolvendo le sue due app già esistenti verso l’architettura del portafoglio digitale europeo. Per facilitare la migrazione, il centro A-SIT ha sviluppato Valera, un wallet open-source usato nei progetti pilota su larga scala. Una volta completati i test, Valera sarà integrato in produzione e unificato con eID Austria ed eAusweise, consentendo agli utenti di passare all’EUDI wallet semplicemente aggiornando l’app¹⁴⁰.

Nei Paesi dell’Europa occidentale, Francia, Paesi Bassi e Belgio mostrano approcci diversificati: in Francia, la piattaforma France Identité¹⁴¹ e la carta d’identità elettronica consentono l’accesso centralizzato ai servizi pubblici; nei Paesi Bassi, il sistema DigiD¹⁴² convive con servizi bancari iDIN e sperimentazioni basate su Self-Sovereign Identity (SSI); in Belgio, l’app itsme¹⁴³, originariamente sviluppata da operatori privati, è stata integrata sotto la supervisione pubblica e notificata ai sensi di eIDAS, assicurando interoperabilità e sicurezza nell’accesso ai servizi fiscali e sanitari.

L’Europa meridionale evidenzia una traiettoria di accelerazione: in Italia, al di là di quanto diffusamente esposto sull’implementazione dell’IT Wallet, si registrano numeri altissimi relativamente alla diffusione e all’utilizzo delle identità digitali previste dalla normativa; in Spagna, con il sistema Cl@ve¹⁴⁴, integrato con versioni pilota del portafoglio digitale, e in Grecia, dove sono in corso applicazioni nazionali per l’identità digitale, si osservano progressi graduali ma strutturali.

Nell’Europa orientale e sud-orientale, Paesi quali Polonia con mObywatel¹⁴⁵, Repubblica Ceca (con tre sistemi notificati) e Slovacchia dispongono di so-

¹³⁶ Si tratta del Funke, eudi wallet prototypes.

¹³⁷ Si tratta di una app di identità digitale per l’uso online che conta circa tre milioni di utenti e già dotata di funzioni tipiche dell’EUDI wallet: identificazione, attestazioni elettroniche (VC), emissione e verifica, firme elettroniche qualificate e identità aziendale.

¹³⁸ Si tratta di una app per le patenti digitali usata soprattutto di persona, cui risultano iscritti circa 1 milione di utenti.

¹³⁹ Si veda www.eid.admin.ch/it

¹⁴⁰ Cfr. www.plus.a-sit.at/open-source.html.

¹⁴¹ Si tratta di una app mobile che permette di creare un’identità digitale basata sulla carta d’identità biometrica, utilizzata per vari servizi online e verifiche fisiche.

¹⁴² Cfr. www.digid.nl/en.

¹⁴³ Cfr. www.itsme-id.com/en-IT.

¹⁴⁴ Cfr. www.clave.gob.es/clave.

¹⁴⁵ Cfr. www.gov.pl/web/mobywatel.

luzioni in via di consolidamento, mentre Romania, Croazia e Slovenia stanno avviando l'implementazione dei portafogli digitali conformi a eIDAS 2.; analogamente, alcuni Stati extra-UE, come l'Ucraina con l'app Diia¹⁴⁶, dimostrano una rapida adozione malgrado contesti complessi.

In prospettiva, come si evince dal breve quadro illustrato, benché il percorso verso un ecosistema digitale europeo armonizzato sia chiaramente tracciato, permangono rilevanti disomogeneità in termini di governance, modelli tecnologici e accettazione sociale. Come già rilevato a livello internazionale, la sfida principale non si esaurisce nella mera implementazione tecnica del portafoglio digitale entro la scadenza fissata dalla normativa sovranazionale, ma concerne la costruzione di un sistema di governance integrato, capace di armonizzare attori pubblici e privati, di assicurare interoperabilità transfrontaliera, di garantire sicurezza e riservatezza dei dati e di tutelare il controllo dell'utente sulle proprie informazioni personali.

6. Prime conclusioni su stato dell'arte e prospettive dell'identità digitale nella sua funzione identificativa.

Ebbene, l'analisi svolta conferma, anzitutto, la persistenza, anche nella dimensione digitale, della dicotomia tipica dell'identità personale, potendo distinguersi tra una nozione sostanziale dell'identità digitale, legata al diritto ad essere sé stessi nella dimensione digitale e ad essere correttamente rappresentati online, che è intimamente connessa alla persona e ai suoi diritti fondamentali, e una nozione anagrafica, fondata sulla identificazione del soggetto.

La prima nozione, quella che si è definita "sostanziale", sembra, come emerge dalla ricostruzione effettuata, trovare ormai una tutela prevalente nella normativa in materia di protezione dei dati personali e in particolare nel Regolamento (UE) 2016/679 – GDPR, che disciplina il trattamento e la protezione dei dati personali, nonché la circolazione degli stessi. Ad oggi, del resto, in un mondo in cui ogni soggetto dissemina quotidianamente e ovunque proprie informazioni, i diritti dell'interessato, tutelabili anche grazie al ricorso alle autorità competenti, si sostanziano più che altro nel controllo dei propri dati e della loro circolazione anche nella dimensione digitale, nonché della propria identità come somma degli stessi¹⁴⁷.

¹⁴⁶ Cfr. www.expo.diia.gov.ua/. Si segnala, in proposito, che in Ucraina, applicazioni come questa, nate con la finalità di digitalizzare i servizi pubblici, di recente sono state estese al servizio delle necessità dei cittadini sopravvenute in tempo di guerra.

¹⁴⁷ Come ricorda S. Rodotà nella relazione tenuta alla XXVI Conferenza internazionale dei Garanti per la privacy del 16 settembre 2024, sussiste uno stretto legame tra privacy, libertà e dignità, sicché, la tutela della privacy si proietta al di là della semplice protezione della sfera privata e diviene elemento essenziale della cittadinanza del nuovo millennio. Lo stesso Rodotà afferma che *“Senza una forte tutela del “corpo elettronico”, dell'insieme delle informazioni raccolte su ciascuno di noi, la stessa libertà personale viene messa in pericolo: la privacy si precisa così come una condizione ineliminabile della società della libertà, come uno strumento indispensabile per contrastare le spinte verso una società della classificazione, della sorveglianza, della selezione sociale”*.

A tendere, è probabile e si evince anche dalle scelte di politica normativa effettuata da alcuni paesi come la Danimarca e la California che - alla luce dell'avanzamento tecnologico e del parziale fallimento che si è registrato nella tutela legata esclusivamente alla privacy - tale tutela si rafforzi con il supporto anche della normativa in materia di proprietà intellettuale e diritto d'autore, laddove la gestione dei contenuti digitali individuali si intreccia con la sfera identitaria del soggetto. Come anticipato, esistono proposte normative volte a riconoscere alla persona diritti esclusivi sui propri tratti facciali, sulla voce e sulle caratteristiche corporee, includendo una tutela, come tipico delle opere dell'ingegno, anche successiva alla morte.

In tale prospettiva, l'identità digitale sostanziale si pone come vettore di diritti fondamentali, la cui tutela è mediata da strumenti normativi e tecnologici volti a garantire riservatezza, integrità e autonomia dell'individuo nella dimensione digitale.

Sul punto, dunque, deve ribadirsi quanto già approfondito nella prima parte della presente trattazione circa il fatto che, nonostante l'apparente "allargamento" dell'identità nella dimensione digitale, si profila, in realtà, come messo in luce da vari Autori¹⁴⁸, una regressione sul tema dei diritti. Quest'ultima può essere fronteggiata solo con strumenti giuridici creativi, che siano in grado di elaborare rimedi giudiziali e stragiudiziali innovativi per gestire i rischi sempre più sofisticati posti dalla rete.

Anche la nozione anagrafica dell'identità digitale, oggetto di approfondimento della presente analisi, può essere considerata, a parere della scrivente, un vero e proprio laboratorio di quello che è stato definito come "costituzionalismo digitale"¹⁴⁹, in quanto consente di svolgere alcune riflessioni sul tema dei diritti digitali e della regolazione degli stessi.

In particolare, con riferimento ai diritti digitali e alla loro qualificazione, alla luce delle teorie elaborate sul tema dalla dottrina e della giurisprudenza citata che si è sviluppata sul tema, il diritto all'identità digitale come strumento di identificazione per l'accesso ai servizi può essere letto come la proiezione digitale del corrispondente diritto analogico.

¹⁴⁸ Cfr. G. Alpa, *Il diritto ad essere sé stessi*, cit., 258. L'A. analizza l'evoluzione dell'individuo verso la dimensione informatica, rilevando che "appare più un regresso di sapore mercantile piuttosto che un progresso nelle garanzie individuali". Nello stesso senso cfr. M. Luciani, *Quale identità?*, cit., il quale sostiene condivisibilmente che "nel contesto del ripiegamento individualistico che esperiamo oggi (negato dagli ingenui i quali s'illudono che l'agorà telematica sia davvero una piazza civica in cui si matura coscienza collettiva e non una selva in cui ogni singolo si perde, senza riuscire ad allacciare alcuna relazione realmente "politica" con gli altri), l'autogoverno, almeno parziale, dei propri dati sarà forse ben poco, ma almeno è qualcosa".

¹⁴⁹ Cfr. A. Simoncini, *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale tra forma di stato e forma di governo*, in *Oss. fonti*, 2021, 727 ss.; E. Cheli, *Conclusioni*, ivi, 2021, 955 ss.

Sebbene tale diritto non goda di riconoscimento costituzionale esplicito, esso risulta tutelato dal fitto sistema di presidi normativi elaborato a livello sovranazionale e di diritto primario, che si è tentato di ricostruire nella presente analisi.

Tali strumenti, nel loro insieme, sembrano assicurare, in concreto, la tutela dell'identità strumentale all'identificazione, garantendole, anzitutto, riconoscimento e configurando l'identità digitale come strumento abilitante all'identificazione e all'accesso ai servizi pubblici, piuttosto che mero supporto tecnologico. Sia nell'ordinamento nazionale sia nel quadro sovranazionale dell'Unione, infatti, l'identità digitale, l'identità europea unificata e il relativo wallet si atteggiano a diritti strumentali e presupposti necessari per l'effettivo esercizio dell'accesso ai servizi pubblici e, più in generale, delle prerogative connesse alla cittadinanza, tanto statale quanto europea.

Segnatamente, l'identità digitale si configura quale imprescindibile corollario dei processi di innovazione tecnologica e organizzativa della pubblica amministrazione e, al contempo, quale manifestazione avanzata della cittadinanza amministrativa dell'individuo.

Dalla strategia europea si desume come la categoria della cittadinanza digitale si ponga in rapporto di stretta complementarità con la cittadinanza dell'Unione, la quale ricomprende, tra i propri attributi qualificanti, la libertà di circolazione e il diritto di soggiorno sull'intero territorio degli Stati membri. L'Unione europea, in questo senso, annovera, tra le proprie finalità strategiche, l'esigenza di assicurare ai cittadini dell'Unione l'accesso ai servizi pubblici digitali anche in Stati membri diversi da quello di residenza, evitando loro l'onere di costituire nuove identità informatiche ovvero di comunicare ulteriori dati personali. Ciò in un quadro complessivo orientato alla piena interoperabilità transfrontaliera, alla semplificazione degli adempimenti e alla progressiva affermazione di un ecosistema europeo unitario dell'identità digitale.

Nel quadro così delineato, l'identità digitale si presta a essere intesa quale attributo personale sottoposto a un procedimento di validazione e di riconoscimento da parte dell'apparato pubblico, il quale ne garantisce la piena operatività tanto nei rapporti con l'Amministrazione quanto nelle interazioni economiche e sociali. Essa assume, infatti, una funzione abilitante in un mercato progressivamente orientato — secondo le direttrici di sviluppo tracciate dall'Unione europea — all'adozione di sistemi di identificazione digitale omogenei, interoperabili e idonei a dispiegare i propri effetti senza soluzione di continuità nello spazio transfrontaliero dell'Unione.

Quanto all'effettività della tutela, che, come si è visto, rimane una delle questioni più critiche dei nuovi diritti o dei diritti nuovi, il sistema, come visto, è stato progressivamente rafforzato da strumenti di tutela - non solo giudiziali - attivabili anche in caso di violazione o mancato riconoscimento del diritto all'identità digitale. Alla luce di tutto quanto esposto, si deve propendere, al momento, per la non necessità di una revisione costituzionale.

Quanto al tema delle tecniche di regolazione, anch'esso è stato approfondito nella presente trattazione in una prospettiva costituzionalistica ed è possibile svolgere alcune prime riflessioni.

Il regime regolatorio dell'identità digitale, come esposto, si caratterizza per un'architettura multilivello, combinando norme sovranazionale, nazionali di rango primario, nazionali di rango secondario, linee guida tecniche e altri tipi di soft law. Il profilo positivo di questo sistema, come già esposto, è l'attenzione per il tema dell'identità, seppur in assenza di una base giuridica espressa in Costituzione.

In questo contesto, come del resto per tutta la regolazione delle tecnologie, tuttavia, come anticipato, un ruolo determinante è stato assunto dal Governo a livello nazionale e dalla Commissione europea a livello sovranazionale. Nella presente trattazione esempio paradigmatico risulta certamente la normativa nazionale sul digitale e sull'identità digitale per lo più affidata a decretazione delegata e d'urgenza. Altro esempio lampante sono gli atti di esecuzione relativi all'EUDI Wallet, che, come visto, disciplinano le modalità di rilascio, le caratteristiche tecniche, i requisiti di sicurezza, i criteri di interoperabilità e le funzioni di certificazione dei portafogli. Tali atti di esecuzione, adottati dalla Commissione europea ai sensi dell'art. 290 TFUE, definendo standard e procedure, rappresentano elemento essenziale per rendere operative le previsioni del Regolamento eIDAS2. Risultano, dunque, indispensabili per rendere effettiva l'identità digitale europea, ma al prezzo di una redistribuzione del potere normativo: dalla rappresentanza politica del Parlamento a una governance più tecnica, guidata dalla Commissione e dai Governi. Ciò apre, anche con riferimento all'EUDI Wallet, un dibattito che si è già sviluppato più in generale sul tema della regolazione delle tecnologie sul bilanciamento tra efficienza normativa rispetto a una materia in continua evoluzione e pieno controllo democratico del processo regolatorio¹⁵⁰.

Infine, non possono essere trascurati anche i rischi e le criticità connessi all'espansione dell'identità digitale in termini sia territoriali che dimensionali. L'interoperabilità transfrontaliera per l'accesso ai servizi pubblici e privati nel mercato unico digitale, pur rappresentando un elemento di efficienza e integrazione dei ser-

¹⁵⁰ In senso favorevole ad una legislazione "per principi" rispetto a un approccio di dettaglio, cfr. A. Iannuzzi, *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, cit., 20; in senso contrario cfr. O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *Riv. AIC*, 2025, 119 ss., spec. 127, il quale paventa il rischio dell'eccessivo potere attribuito alla Commissione europea. In particolare, parlando del sistema previsto dall'AI Act, analogo a quello del Regolamento eIDAS2, si chiede se "*l'aggiornamento di un insieme di usi e applicazioni di intelligenza artificiale, con la conseguente integrazione, in caso di emersione di nuove tipologie che presentano un rischio significativo, è una mera ricognizione tecnica che può essere delegata all'organo esecutivo dell'Unione o implica (visto che nessuna tecnologia, e tanto meno un ecosistema a sé come è l'intelligenza artificiale, può definirsi neutrale) delle scelte di natura assiologico-sostanziale che dovrebbero essere affidate all'organo legislativo all'interno del circuito democratico rappresentativo, per quanto azzoppato dell'Unione*".

vizi digitali, comporta fisiologicamente vulnerabilità sotto il profilo della protezione dei dati personali, della sicurezza informatica, con conseguenti inevitabili pericoli per i cittadini europei.

A livello di sistema, inoltre, si intravede un problema legato alle responsabilità rispetto a tali rischi, laddove, come già avvenuto in altri ambiti del diritto, la regolazione e la governance multilivello hanno creato spesso problemi di conflitti normativi derivanti da una sovrabbondanza della regolazione¹⁵¹ e di conflitti di competenze tra autorità, piuttosto che rappresentare un efficace presidio per soggetti, che, alla luce della complessità normativa, sono diventati, di fronte al potere pubblico, al contempo cittadini, utenti, consumatori, interessati, utilizzatori.

È in questo quadro che si sta ragionando, in Italia, su una riforma del Codice dell'amministrazione digitale che comporti l'adeguamento della normativa interna sull'identificazione digitale rispetto al mutato quadro delineato dal Regolamento eIDAS2. Quanto alla dimensione sovranazionale, l'Europa si sta comprensibilmente orientando, tramite il c.d. "Digital Omnibus"¹⁵², a una riforma complessiva di una serie di normative sul tema del digitale in una logica di semplificazione.

¹⁵¹ Cfr. S. Torreggiani, *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *Riv. it. inf. dir.*, 2021, 49 ss.

¹⁵² Cfr. Proposal for a Regulation of the European Parliament and of the Council amending Regulations 2016/679/UE, 2018/1724/UE, 2018/1725/UE, 2023/2854/UE and Directives 2002/58/EC, 2022/2555/UE and 2022/2557/UE as regards the simplification of the digital legislative framework, and repealing Regulations 2018/1807/UE, 2019/1150/UE, 2022/868/UE, and Directive 2019/1024/UE (Digital Omnibus).

CAPITOLO III

L'identità e l'identificazione del minore nella dimensione digitale

SOMMARIO: 1. Introduzione: l'identità personale e digitale del minore - 2. La tutela giuridica dei minori nei confronti dei *mass media* - 3. Minori, internet e piattaforme: le difficoltà dei Legislatori nel regolare il rapporto tra minori e tecnologie digitali - 4. La protezione dei dati personali dei minori nell'ambiente digitale - 5. La verifica dell'età come strumento di protezione: una prospettiva transnazionale e interdisciplinare - 5.1. La disciplina sovranazionale in tema di verifica dell'età. La tutela dei minori nel Digital Services Act - 5.2. L'attuazione dell'art. 28, par. 4 DSA: le linee guida e il prototipo per la verifica dell'età della Commissione europea - 5.3. Il quadro normativo nazionale in tema di verifica dell'età. SPID per i minori: le Linee Guida dell'Agenzia per l'Italia digitale - 5.4. L'impatto del "Decreto Caivano" - 5.5. I principi affermati dal Regolamento AGCOM in tema di verifica dell'età - 5.6. Le più recenti novità della normativa italiana in tema di verifica dell'età - 6. Il fenomeno dello "sharenting" e dei "baby influencer" - 7. Tecniche di regolazione a confronto: l'esempio francese - 7.1. L'esperienza francese sull'obbligo di verifica dell'età - 7.2. L'approccio francese ai fenomeni dello "sharenting" e dei "baby influencer" - 8. L'impatto dell'intelligenza artificiale sull'identità digitale del minore: profili di rischio e opportunità - 9. Prime considerazioni conclusive su tutela e prospettive dell'identità digitale del minore.

1. Introduzione: l'identità personale e digitale del minore.

Se l'identità personale è, per sua natura, volubile, lo è ancor di più nel caso dei minori, quale individui in continua "evoluzione"¹.

Nel minore possono, come per tutti gli altri soggetti, coesistere molteplici identità, riflesso della sua complessità interiore. Al contempo, il minore 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, utilizzando, talvolta in modo indifferenziato, termini quali "infanzia", "adolescenza", "gioinezza", "fanciullezza", senza riuscire, spesso, ad afferrare la complessità di tale soggetto, che si trasforma con estrema velocità².

¹ I minori di età sono dalla dottrina spesso definiti "soggetti in formazione". Cfr., tra gli altri, E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, 1-2; A.C. Moro, *Manuale di diritto minorile*, Bologna, 2014, 4, ove parla più specificamente di un "soggetto con esigenza di maturazione della sua identità".

² Sia consentito, per un approfondimento, il rinvio a F. Ricciulli, *L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti*, in *Riv. it. inf. dir.*, 2024, 355 ss.

Fatta questa premessa, occorre anzitutto chiedersi come si configuri l'identità personale di un minore e, nell'ottica della sua protezione, quale sia l'effettivo oggetto della tutela, poiché ciò che si intende salvaguardare potrebbe, nel giro di breve tempo, essere già mutato.

Tale questione riguarda più che altro l'identità nella sua accezione "sostanziale", intesa come diritto a essere sé stessi o a essere correttamente rappresentati³. Ciò che si intende essere o apparire nel presente può essere diverso nel futuro (anche un futuro molto prossimo, se si tratta di un bambino).

Il tema, poi, si fa ancor più complesso quando, accanto all'identità personale, il minore sviluppa altresì una identità digitale e/o virtuale⁴. In effetti, come si approfondirà nel prosieguo, seppur astrattamente possibile, è ormai remoto il caso del minore del tutto privo di un'identità digitale⁵.

Ebbene, se un bambino o un adolescente viene coinvolto in uno spot pubblicitario per iniziativa del genitore – o persino per un suo desiderio espresso in tenera età – come possiamo davvero sapere se quella scelta rispecchia la sua volontà autentica? E soprattutto, come possiamo essere certi che, una volta cresciuto e pienamente consapevole della propria identità, si riconoscerà ancora nell'immagine di sé che è stata costruita e diffusa? Quanto c'è il rischio di una identità "plasmata"⁶dall'adulto? In quali casi, invece, può, e quindi deve, parlarsi di "autodeterminazione"⁷?

Queste riflessioni non valgono solo per la pubblicità tradizionale, ma ancor di più per fenomeni che si sono diffusi più di recente come quello dei "baby influencer" e dello "sharenting", ossia la pratica, ormai diffusissima, di esporre online foto, video e contenuti che ritraggono minori, nella maggior parte dei casi ad opera dei genitori. In questi casi, come si proverà ad approfondire nel prosieguo, la

³ Per un approfondimento sull'identità personale e sulle nozioni elaborate in dottrina e giurisprudenza cfr. *supra* cap. I.

⁴ Sulla nozione di "identità digitale" e "identità virtuale" cfr. cap. *supra* II.

⁵ Di recente ha fatto molto discutere il caso eccezionale della nota attrice Millie Bobby Brown, che ha scelto di non divulgare nome e foto della figlia per evitare di crearle un'identità digitale precoce. Sarà infatti la bambina, se e quando lo vorrà, a costruire autonomamente la propria presenza online in futuro.

⁶ Cfr. E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 4

⁷ Tra gli autori che si sono interrogati sul tema cfr. D. Marcello, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo*, Napoli, 2023, 22. L'A. sostiene che per lungo tempo, le visioni dell'educazione familiare, inizialmente di impronta patriarcale e successivamente adultocentrica, hanno portato a considerare quasi esclusivamente i bisogni materiali dei minori. Anche la dottrina civilistica si è concentrata soprattutto sugli aspetti patrimoniali, trascurando in gran parte le necessità di natura esistenziale, nella convinzione – radicata nella tradizione – che i ragazzi fossero incapaci di tutelare autonomamente i propri interessi. Nell'attualità, invece, emerge anche la necessità di proteggere la loro sfera esistenziale, la capacità di autodeterminazione e la riservatezza intesa come diritto fondamentale, che si concretizza anche nella gestione dei propri dati. Tale esigenza risulta strettamente connessa all'uso delle tecnologie, le quali non costituiscono soltanto un mezzo di espressione, ma veri e propri spazi esistenziali nei quali i minori costruiscono e sviluppano la propria personalità.

rappresentazione dell'infanzia diventa spesso un contenuto monetizzabile, un mezzo per costruire visibilità e, talvolta, un vero e proprio lavoro, che, però, riguarda persone ancora prive degli strumenti per comprenderne fino in fondo le conseguenze.

In questo contesto, è lecito domandarsi se queste immagini e questi racconti, una volta scolpiti nella rete, accompagneranno i minori in modo coerente con chi saranno davvero o se finiranno, al contrario, per vincolare la loro libertà di definire sé stessi, la percezione della propria identità-dignità e la propria storia⁸.

Accanto a quello della celere e ineludibile mutevolezza, un ulteriore concetto da assumere come presupposto di fondo per affrontare il tema dell'identità del minore nella dimensione digitale è quello della "vulnerabilità"⁹: la tutela nei confronti dei diritti dei minori in rete, infatti, in quanto soggetti deboli o vulnerabili, dovrebbe essere speciale e rafforzata¹⁰.

⁸ Per un approfondimento su identità e dignità cfr. G. Alpa, *Il diritto di essere sé stessi*, cit., 293-298.

⁹ Sulla letteratura in tema di "vulnerabilità", cfr. V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, Bari, 2022, 32-34, ove l'A. sintetizza così gli elementi essenziali che devono ricorrere per parlare di vulnerabilità: "esposizione ad un rischio (maggiore probabilità di esposizione al rischio per il soggetto vulnerabile); mancanza di resilienza: il soggetto vulnerabile non ha le risorse per evitare il rischio che può provocare il danno (mentre un soggetto non vulnerabile in presenza di un rischio di danno può adottare le precauzioni necessarie per evitarlo); il soggetto vulnerabile non è in grado di rispondere adeguatamente al danno nel caso in cui il rischio si è materializzato". Cfr. anche S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 11; nonché, A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, 5, ove l'A. parla di una generale "vulnerabilità sociale" dei navigatori di internet alla luce della asimmetria rispetto ai poteri privati che si amplifica ulteriormente quando si parla di minori di età.

¹⁰ M. Orofino, F. Pizzetti (a cura di), *Privacy, minori e cyberbullismo*, 337, Torino, 2018; A. Iannuzzi, C. Colapietro, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, in *Riv. it. inf. dir.*, 2024, 333 ss. Per un approfondimento sull'evoluzione del diritto minorile dall'ottica patrimonialista "che si è focalizzato sul minore di età quale persona - soggetto vulnerabile - ritenendola meritevole di una speciale protezione da sé stesso e dagli altri nel suo percorso di crescita verso l'età adulta" cfr. E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 2; M. Dogliotti, *Sul concetto di diritto minorile: autonomia, favor minoris, principi costituzionali*, in *Dir. fam. pers.*, 1977, 954 ss.; V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, cit., 31-34, secondo la quale "la maggiore esposizione al rischio del soggetto vulnerabile determina la necessità di costruire misure di protezione ex ante, dirette a ridurre la probabilità che tali rischi possano concretizzarsi; e misure ex post di riparazione, nel caso in cui la lesione si sia verificata.

Ciò tanto più in un'epoca in cui la dimensione digitale non si incontra in modo occasionale ma tutti, e ancor più i minori in quanto “nativi digitali”¹¹, sono costantemente e inesorabilmente “immersi” nella stessa¹².

La questione della tutela dell'identità-dignità in rete si rivela ancor più articolata se si considera che la dimensione digitale, pur mettendo in luce rischi ben noti e ampiamente dibattuti, non esaurisce in essi la propria portata, potendo anzi configurarsi quale spazio al contempo idoneo allo sviluppo e alla piena espressione della personalità del minore¹³.

A tale proposito, vale la pena ricordare che già da tempo si discute dell'opportunità di riconoscere costituzionalmente un vero e proprio diritto di accesso alla rete, intesa non più soltanto come infrastruttura tecnologica, bensì come un nuovo ambito di esercizio di diritti fondamentali. Non a caso, negli anni si sono susseguite proposte volte a qualificare l'accesso a internet come libertà da affiancare a quella di manifestazione del pensiero¹⁴, così come non sono mancate iniziative che ne hanno auspicato l'inserimento nella Parte I, Titolo II della Costituzione, tra i “Rapporti etico-sociali”, con l'intento di configurarlo, piuttosto,

¹¹ M. Prensky, *Digital Natives, Digital Immigrants*, in *Digital Natives Digital Immigrants*, 2001, 1 ss., ove l'A. elabora questa espressione per indicare le persone nate dalla fine degli anni '90, cresciute con la possibilità di apprendere fin da piccole il linguaggio informatico e l'uso degli strumenti digitali. Lo stesso Autore definisce «immigrati digitali» coloro che, pur utilizzando le tecnologie, non hanno avuto un'infanzia immersa in esse. Cfr. anche A. Dario, A. La Lumia, *Minori, internet e social network*, Milano, 2021, 10. Gli AA. affermano che i nativi digitali necessitano di una speciale tutela, benché dovrebbero apparentemente avere maggiore dimestichezza e confidenza con tutto ciò che è telematico; F. Capeci, *Generazione 2.0. Chi sono, cosa vogliono, come dialogare con loro*, Milano, 2014, 16 ss.; A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 41, la quale ricollega a questa qualifica anche una maggiore capacità di eludere le barriere poste a presidio della loro tutela.

¹² Sul punto, A. Iannuzzi, C. Colapietro, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, cit., 334, ove si legge che “tale posizione, di portata senz'altro generale, si estende alla realtà che coinvolge i soggetti minori d'età, i quali – in quanto “nativi” digitali – sono costantemente immersi in una dimensione cibernetica totalizzante e capace di permeare (e persino invadere) ogni aspetto della loro vita, a partire dalle formazioni sociali ove essi formano la propria personalità in modo prevalente: la scuola e la famiglia”. Cfr., altresì, S. Sica, V. Zeno Zencovich, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Dir. inf.*, 2010, 384 ss.

Dati rilevanti sulla presenza sempre più massiccia dei minori nella dimensione digitale emergono dal “Manifesto dei bambini sui diritti in ambiente digitale”, presentato dall'Autorità garante per l'infanzia e l'adolescenza il 17 maggio 2023. Secondo quanto affermato nell'“Online age verification methods for children”, redatto dall'European Parliamentary Research Service) nel febbraio 2023, un bambino su tre è un utente di internet e un utente di internet su tre ha meno di 18 anni. Inoltre, nell'Ue, la maggior parte dei bambini utilizza quotidianamente lo smartphone, quasi il doppio rispetto a dieci anni fa, e comincia a farlo già in età molto più precoce.

¹³ E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 113 afferma, in questo senso, che “nella rete internet, ancora più che nelle reti televisive circola una grande massa di informazioni disponibili, in positivo, per l'educazione dei minori e, in negativo, idonea a mettere a rischio il loro sano sviluppo”. Si veda anche il “Parere del garante europeo della protezione dei dati sulla promozione della fiducia nella società dell'informazione tramite l'incentivazione della protezione dei dati e della vita privata” (2010/C) (280/01).

¹⁴ S. Rodotà, *Il mondo nella rete, Quali i diritti, quali i vincoli*, Roma, 2014, 13.

come un diritto sociale a tutti gli effetti¹⁵. L'esperienza della pandemia da Covid-19 ha restituito vigore a tale dibattito, mostrando in modo inequivocabile come la rete rappresenti ormai un presupposto irrinunciabile per l'esercizio di diritti fondamentali, quali, con specifico riferimento ai più giovani, l'accesso all'istruzione e alla formazione¹⁶.

Il contesto descritto impone, dunque, di non limitarsi a ragionare sugli strumenti di tutela a salvaguardia del minore nello spazio digitale, ma anche di interrogarsi su come la rete possa essere al contempo valorizzata quale risorsa per favorire la massima espressione e il pieno sviluppo della personalità dello stesso, mettendogli a disposizione opportunità formative, relazionali e creative, che sarebbe riduttivo – e ormai irrealistico – trascurare¹⁷. In altre parole, va considerato, per non cadere in riduttive semplificazioni, che la dimensione digitale si configura, contemporaneamente, come luogo di espressione grazie al quale il minore può sentirsi più incluso all'interno di una comunità e quale luogo di isolamento, dipendenza e rischio di esposizione a contenuti inappropriati¹⁸.

Infine, deve essere preso in considerazione un ulteriore interesse da contemperare con l'esigenza di proteggere i minori nello spazio digitale, oltre a quello di garantire la piena espressione della loro personalità. Si tratta, come diversi autori hanno correttamente evidenziato, dell'interesse, che forse negli anni è diventato addirittura controinteresse¹⁹, alla promozione dello sviluppo e della crescita del mercato digitale²⁰.

Ebbene, nel contesto descritto, come si approfondirà nell'ambito della presente analisi, l'approccio adottato sul tema a livello nazionale e dall'Unione europea, dopo anni in cui si è registrata una generale incapacità di regolare la maggior parte dei fenomeni che coinvolgono i minori *online*, è quello di introdurre divieti per i giovani, più che altro nella loro qualità di "utenti" e speculari obblighi per i gestori delle piattaforme. Entrano a questo punto in gioco le tecniche di

¹⁵ Cfr. proposta c.d. Rodotà e successivamente "D'Ippolito" e "Liuzzi". Per una ricostruzione approfondita del tema cfr. G. D'Ippolito, *Il diritto di accesso ad Internet in Italia: dal 21(-bis) al 34-bis*, in *Riv. dir. media*, 2021, 81 ss.

¹⁶ Camera dei deputati, *Proposta di legge costituzionale Madia e Orlando: Modifica all'articolo 21 della Costituzione, in materia di riconoscimento del diritto di accesso alla rete internet (2769)*.

¹⁷ In questo senso, E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 125; A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 5, ove l'A. parla di "equilibrio tra libertà e controllo".

¹⁸ Sugli effetti psicologici riscontrati in tutte le parti del mondo, cfr. R. Luna, *Qualcosa è andato storto*, Milano, 2025, 90 ss.

¹⁹ *Ibidem*, 104.

²⁰ A. Iannuzzi, C. Colapietro, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, cit., 335. Si rinvia anche alla Comunicazione del 6 maggio 2015 che la Commissione europea ha trasmesso al Parlamento europeo, al Consiglio, al Comitato sociale economico europeo e al Comitato delle Regioni (COM 20115, 192 final) nella quale si definisce un quadro complessivo che traccia la strategia eurounitaria per la realizzazione del mercato digitale unico in Europa.

verifica dell'età²¹, che sono state individuate dalla maggior parte dei Paesi come soluzione più idonea per prevenire i pericoli che affliggono i minori e che nella maggior parte dei casi implicano l'identificazione del soggetto che vuole accedere alla dimensione digitale. Scarsa attenzione, invece, nonostante si registrino varie proposte normative in diversi Paesi europei, risulta ancora riservata al minore come "contenuto del servizio".

Si anticipa sin da ora, però, che la questione non può ridursi all'elaborazione di regole astratte o di meri meccanismi di controllo tecnologico, pur rilevanti²². L'aspetto decisivo sembra collocarsi, piuttosto, in una dimensione pregiuridica, rappresentata dalla costruzione di una cultura digitale condivisa, saldamente fondata sull'informazione corretta, sulla piena consapevolezza e sulla corresponsabilità dei soggetti coinvolti.

Già da tempo si evidenzia la necessità di una formazione digitale organica e strutturata e che trovi un primo presidio all'interno della famiglia e nel sistema scolastico, al fine di dotare i minori di strumenti adeguati a riconoscere e fronteggiare minacce e rischi connessi all'uso delle tecnologie. Un simile intervento non può considerarsi esaustivo se non si traduce in una più ampia consapevolezza collettiva, che coinvolga in modo diretto, appunto, anche gli adulti – genitori, educatori, istituzioni e *providers* – chiamati a svolgere un ruolo attivo di guida, supervisione e orientamento²³.

L'obiettivo dovrebbe essere quello di non limitarsi a vietare o sanzionare, ma formare: accompagnare bambini, adolescenti e anche gli adulti stessi a sviluppare capacità critiche, a riconoscere i rischi e a compiere scelte consapevoli. In assenza di un simile percorso formativo, ogni divieto rischia di rimanere inefficace e di trasformarsi in una protezione solo apparente.

Diventa quindi essenziale predisporre strumenti conoscitivi adeguati, linguaggi chiari e spazi di confronto intergenerazionale, affinché gli adulti siano messi nelle condizioni di svolgere in modo informato e responsabile la propria

²¹ Con le espressioni "tecniche o strumenti di verifica dell'età" o, in inglese, "age assurance", "age verification" e "age gate" si fa comunemente, ancorché attecnicamente, riferimento all'insieme degli strumenti e delle procedure volte a verificare l'età di un soggetto, al fine di stabilire se sia minorenne e, di conseguenza, se possa accedere a determinati servizi o contenuti online. Nel presente studio la locuzione *sistemi di verifica dell'età* (o *sistemi di age verification*) sarà utilizzata in senso generale per indicare l'oggetto dell'indagine. Quando invece si affronteranno i profili giuridici connessi ai singoli sistemi, verranno adottate le specifiche espressioni corrispondenti: "sistemi basati sulla dichiarazione dell'età" o "sistemi di self-declaration", "sistemi basati sulla verifica dell'età" o "sistemi di age verification" "sistemi basati sulla stima dell'età" o "age estimation". Giova evidenziare che nel richiamato report "Online age verification methods for children" dell'EPRS si parla, invece, di "metodi di verifica dell'età", riferendosi a strumenti vari che vanno dalla dichiarazione dell'età all'esibizione del documento di identità o della carta di credito.

²² In questo senso, E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 125, afferma che "sembra inutile porre un limite d'età sotto il quale vietare l'accesso alla Rete". L'A., inoltre, ritiene auspicabile "l'attuazione di una severa politica di controllo di quanto condiviso online" tramite i gestori delle piattaforme.

²³ Cfr., in particolare, A. Dario, A. La Lumia, *Minori, internet e social network*, cit., 11.

funzione di guida. Solo un patto educativo davvero condiviso potrà trasformare i rischi in opportunità di crescita e consentire ai minori di sviluppare un'autonomia digitale autentica e consapevole.

Con riferimento alla struttura e alla metodologia dell'analisi, poste le necessarie basi nei capitoli precedenti, nell'ambito del presente capitolo si è scelto di focalizzarsi sul soggetto minore. Con riferimento a quest'ultimo, si intende approfondire entrambe le accezioni dell'identità personale – quella “sostanziale” e quella “anagrafica” – analizzandone anche l'evoluzione nella dimensione digitale. La prima va intesa come il diritto del minore a essere sé stesso e a essere correttamente – o a non essere affatto – rappresentato online. La seconda sarà invece approfondita attraverso l'esame degli strumenti di identificazione digitale, con particolare attenzione a quelli finalizzati alla verifica dell'età per l'accesso a determinati servizi o contenuti.

In particolare, muovendo dall'analisi dei principali fenomeni che riguardano i minori nello spazio digitale e degli strumenti giuridici attualmente predisposti dal legislatore a livello sovranazionale e nazionale per la tutela degli stessi, la presente trattazione si propone di offrire risposte ai seguenti quesiti di ricerca:

- a) in primo luogo, se tali strumenti possano dirsi effettivamente idonei ed efficaci, tenuto conto, da un lato, della natura intrinsecamente dinamica e in continua trasformazione dell'identità del minore e, dall'altro, della difficoltà di garantire un adeguato livello di consapevolezza circa i rischi connessi all'ambiente digitale, che si manifesta in misura significativa anche tra gli adulti e che, a maggior ragione, può risultare ancora più marcata nei soggetti di minore età;
- b) in secondo luogo, anche alla luce dell'analisi comparatistica delle principali prassi diffuse a livello internazionale e di alcune specifiche normative adottate dalla Francia, quale possa configurarsi come punto di equilibrio sostenibile tra le esigenze di protezione dell'identità e dell'integrità del minore nel contesto digitale, le opportunità di crescita e di sviluppo personale offerte allo stesso dalle tecnologie e, non da ultimo, le istanze di espansione e competitività del mercato digitale;
- c) se sia possibile ragionare nel senso di una nuova nozione di “migliore interesse del minore”²⁴ derivante dal mutato contesto in cui viviamo, alla

²⁴ Sul principio del “migliore interesse del minore” o *best interest of the child* si veda: Convenzione ONU sui Diritti del Fanciullo, 1989 (art. 3); Carta dei Diritti Fondamentali dell'UE, 2000 (art. 24); Codice civile italiano (artt. 337-ter e 337-quater); l. n. 184/1983 (adozioni e affido); l. n. 54/2006 (affidamento condiviso). Nella giurisprudenza della Corte europea dei Diritti dell'Uomo si ricordano tra i principali casi: *Neulinger e Shuruk c. Svizzera*, 2010, n. 41615/07; *K.U. c. Finlandia*, 2008, n. 2872/02; *Maumousseau e Washington c. Francia*, 2007, n. 39388/05; *X c. Lettonia*, 2013, n. 27853/09; *S.c. Francia*, 2005, n. 73316/01.

luce delle trasformazioni indotte dalla società digitale e dall'evoluzione tecnologica²⁵;

- d) infine, quale ruolo possono assumere le tecnologie digitali più innovative, in particolare i sistemi di intelligenza artificiale, nella costruzione, gestione e tutela dell'identità del minore, e quali implicazioni emergono in termini di rischi e opportunità sul piano giuridico.

2. La tutela giuridica dei minori nei confronti dei *mass media*.

Con riferimento ai *mass media* che potremmo definire "tradizionali", si riscontra una disciplina piuttosto dettagliata, sebbene ancora suscettibile di integrazioni tramite regole tecniche emanate dalle Autorità competenti.

Già la Convenzione di New York sui diritti del fanciullo del 20 novembre 1989, ratificata in Italia con la l. 27 maggio 1991, n. 176, tratta del rapporto tra minori e *mass media*²⁶.

L'art. 17 della Convenzione afferma, in particolare, che gli Stati firmatari "*riconoscono l'importanza della funzione esercitata dai mass-media e vigilano affinché il fanciullo possa accedere ad una informazione ed a materiali provenienti da fonti nazionali ed internazionali varie, soprattutto se finalizzati a promuovere il suo benessere sociale, spirituale e morale nonché la sua salute fisica e mentale*".

Di conseguenza, gli Stati devono impegnarsi a incoraggiare: a) i *mass-media* a divulgare informazioni e materiali che hanno una utilità sociale e culturale per il fanciullo e corrispondono allo spirito dell'art. 29²⁷; b) la cooperazione

²⁵ Sul punto cfr. P. Stanzone, G. Sciancalepore, *Minori e diritti fondamentali*, Napoli, 2006, 9 i quali suggeriscono che è importante il tema dell'interesse del minore e soprattutto "*l'individuazione del suo contenuto*". In proposito, gli AA. evidenziano, infatti, che "*il legislatore lo richiama in molteplici norme senza però fornire indicazioni sui criteri per la determinazione di tale nozione*". È infatti, espressamente arduo tentare di precisare in che cosa consista l'interesse del minore. È possibile, tuttavia, affermare che la via da percorrere non conduce ad una definizione astratta, valida per tutti i tempi, per tutti i luoghi, per ogni occasione".

²⁶ Una premessa di carattere generale si rinviene nell'art. 16 della Convenzione di New York nel quale si legge che "*Nessun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione. Il fanciullo ha diritto alla protezione della legge contro tali interferenze o tali affronti*".

²⁷ Cfr. art. 29 ove si legge che "*1. Gli Stati parti convengono che l'educazione del fanciullo deve avere come finalità: a) favorire lo sviluppo della personalità del fanciullo nonché lo sviluppo delle sue facoltà e delle sue attitudini mentali e fisiche, in tutta la loro potenzialità; b) sviluppare nel fanciullo il rispetto dei diritti dell'uomo e delle libertà fondamentali e dei principi consacrati nella Carta delle Nazioni Unite; c) sviluppare nel fanciullo il rispetto dei suoi genitori, della sua identità, della sua lingua e dei suoi valori culturali, nonché il rispetto dei valori nazionali del paese nel quale vive, del paese di cui può essere originario e delle civiltà diverse dalla sua; d) preparare il fanciullo ad assumere le responsabilità della vita in una società libera, in uno spirito di comprensione, di pace, di tolleranza, di uguaglianza tra i sessi e di amicizia tra tutti i popoli e gruppi etnici, nazionali e religiosi e delle persone di origine autoctona; e) sviluppare nel fanciullo il rispetto dell'ambiente naturale. 2. Nessuna disposizione del presente articolo o dell'art. 28 sarà interpretata in maniera da nuocere alla libertà delle persone fisiche o morali di creare e di dirigere istituzioni didattiche, a condizione che i principi enunciati al paragrafo 1 del presente articolo siano*

internazionale in vista di produrre, scambiare e divulgare informazioni e materiali di questo tipo provenienti da varie fonti culturali, nazionali ed internazionali; c) la produzione e la diffusione di libri per l'infanzia; d) i *mass-media* a tenere conto in particolar modo delle esigenze linguistiche dei fanciulli autoctoni o appartenenti ad un gruppo minoritario; e) l'elaborazione di principi direttivi appropriati destinati a proteggere il fanciullo dalle informazioni e dai materiali che possano compromettere il suo benessere in considerazione delle disposizioni degli artt. 13²⁸ e 18²⁹.

In ambito nazionale, con riferimento alla radiotelevisione, esiste da tempo una normativa specifica dedicata ai minori³⁰.

Da ultimo, il d.lgs. 8 novembre 2021, n. 208 (di seguito anche "TUSMA"), con cui è stata recepita la direttiva 2018/1808/UE del Parlamento europeo e del Consiglio³¹, ha introdotto modifiche al d.lgs. 31 luglio 2005, n. 177, recante il Testo unico dei servizi di media audiovisivi e radiofonici.

Il Titolo IV del TUSMA, dedicato alla disciplina dei servizi di media audiovisivi e radiofonici, si apre con disposizioni di carattere generale volte a garantire la tutela dei diritti fondamentali della persona, riservando particolare attenzione alla protezione dei minori³².

rispettati e che l'educazione impartita in tali istituzioni sia conforme alle norme minime prescritte dallo Stato".

²⁸ Cfr. art. 13 "1. Il fanciullo ha diritto alla libertà di espressione. Questo diritto comprende la libertà di ricercare, di ricevere e di divulgare informazioni e idee di ogni specie, indipendentemente dalle frontiere, sotto forma orale, scritta, stampata o artistica, o con ogni altro mezzo a scelta del fanciullo. 2. L'esercizio di questo diritto può essere regolamentato unicamente dalle limitazioni stabilite dalla legge e che sono necessarie: a) al rispetto dei diritti o della reputazione altrui; oppure b) alla salvaguardia della sicurezza nazionale, dell'ordine pubblico, della salute o della moralità pubbliche".

²⁹ Cfr. art. 18: "1. Gli Stati parti faranno del loro meglio per garantire il riconoscimento del principio secondo il quale entrambi i genitori hanno una responsabilità comune per quanto riguarda l'educazione del fanciullo e il provvedere al suo sviluppo. La responsabilità di allevare il fanciullo e di provvedere al suo sviluppo incombe innanzitutto ai genitori oppure, se del caso, ai suoi tutori legali, i quali devono essere guidati principalmente dall'interesse preminente del fanciullo. 2. Al fine di garantire e di promuovere i diritti enunciati nella presente Convenzione, gli Stati parti accordano gli aiuti appropriati ai genitori e ai tutori legali nell'esercizio della responsabilità che incombe loro di allevare il fanciullo e provvedono alla creazione di istituzioni, istituti e servizi incaricati di vigilare sul benessere del fanciullo. 3. Gli Stati parti adottano ogni appropriato provvedimento per garantire ai fanciulli i cui genitori lavorano il diritto di beneficiare dei servizi e degli istituti di assistenza all'infanzia, per i quali essi abbiano i requisiti necessari".

³⁰ Per una ricostruzione dell'evoluzione storica della disciplina cfr. P. Stanzione, G. Sciancalepore, *Minori e diritti fondamentali*, cit., 50-56; E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 111 ss.; Id., *I soggetti vulnerabili: prospettive di tutela della persona*, in *Dir. fam. pers.*, 2020, 383 ss.

³¹ Il d.lgs. 8 novembre 2021, n. 208, reca "Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato. (21G00231)".

³² Il capo I prevede "Disposizioni applicabili a tutti i servizi di media audiovisivi e radiofonici - Norme a tutela dei diritti fondamentali della persona e dei minori". Sul tema cfr., in dottrina, M.

In tale prospettiva assumono rilievo gli artt. 37 e 38, che rappresentano il nucleo essenziale della normativa in materia.

Tali disposizioni configurano un modello di protezione dei minori che si caratterizza per la combinazione di divieti, obblighi positivi, strumenti tecnici di prevenzione, attività educative e sanzioni effettive. Si tratta di una disciplina di carattere sistemico, che intende bilanciare le esigenze di libertà di espressione e di mercato con la primaria esigenza di tutela dei soggetti minori di età, riaffermando la centralità di un approccio integrato tra regolazione, co-regolamentazione e vigilanza istituzionale.

In particolare, l'art. 37, rubricato "*Disposizioni a tutela dei minori nella programmazione audiovisiva e radiofonica*", delinea un sistema organico e multilivello di protezione dei minori finalizzato a salvaguardarne lo sviluppo psico-fisico e morale rispetto ai contenuti trasmessi o resi disponibili dai fornitori di servizi audiovisivi e radiofonici. La norma si articola in più commi, ciascuno dei quali individua specifici divieti, limiti temporali e obblighi di adozione di strumenti tecnici di protezione. In primo luogo, viene stabilito un divieto assoluto di diffusione, nei servizi lineari, di contenuti gravemente nocivi, come rappresentazioni di violenza gratuita, efferata o insistita, ovvero contenuti di natura pornografica o comunque classificati come vietati ai minori di 18 anni³³. A tale divieto si accompagna, tuttavia, una limitata eccezione per i servizi a richiesta, in cui la trasmissione è consentita solo a condizione che siano predisposti rigorosi sistemi di verifica dell'età e misure di *parental control* che rendano impossibile l'accesso ai minori³⁴.

Il legislatore distingue, inoltre, i contenuti non vietati in assoluto, ma potenzialmente dannosi per lo sviluppo psico-fisico e morale dei minori, come le opere vietate ai minori di 14 anni. In questo caso, la diffusione è subordinata

Orofino, *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 *Riv. dir. media*, 2022, 1 ss.

³³ Cfr. art. 37, commi 1 e 12. Per attuare queste disposizioni, i fornitori devono seguire criteri individuati dall'Autorità per le Garanzie nelle Comunicazioni attraverso procedure di co-regolamentazione. Ai sensi del comma 12, l'AGCom, infatti, è chiamata a definire i criteri per classificare i contenuti vietati o dannosi, in modo che i fornitori possano uniformarsi entro 30 giorni dalla pubblicazione dei regolamenti. I contenuti classificati ai sensi del comma 1 devono essere accessibili solo con le protezioni previste al comma 5.

³⁴ Per la deroga cfr. art. 37, comma 3. Tale disposizione introduce un'eccezione al divieto del comma 1, consentendo la distribuzione di contenuti gravemente nocivi solo nei servizi a richiesta (*on demand*), ma esclusivamente se sono adottati sistemi specifici di controllo che impediscano ai minori l'accesso normale a tali contenuti e sono rispettate le regole tecniche di protezione previste dal comma 5 e da altri commi collegati. Ai sensi del comma 5, infatti, "*al fine di garantire un adeguato livello di tutela della dignità umana e dello sviluppo fisico, mentale e morale dei minori*", l'AGCOM, con il coinvolgimento di altri enti (tra cui il Ministero e l'Autorità garante per l'infanzia), è chiamata a stabilire in dettaglio quali accorgimenti tecnici devono essere utilizzati per proteggere i minori. Tra questi, sono previsti: l'uso di codici PIN o sistemi di verifica dell'età; filtri di accesso ai contenuti in base alla classificazione; l'obbligo di *parental control*, che può essere disattivato solo da un adulto tramite codice. Il codice deve essere comunicato in modo riservato all'adulto che sottoscrive il contratto.

all'osservanza di precise cautele: trasmissione esclusivamente in orari protetti (tra le ore 23:00 e le ore 7:00), obbligo di segnalazione mediante avvisi acustici e simboli visivi chiari e permanenti, nonché adozione di strumenti tecnici che ne impediscano l'accesso da parte di soggetti non adulti³⁵. La norma estende tali cautele anche alle anteprime cinematografiche, valorizzando il principio secondo cui la tutela deve operare non soltanto rispetto al contenuto principale, ma anche con riguardo ai materiali promozionali ad esso collegati³⁶.

Un ulteriore profilo di rilievo è rappresentato dalla previsione di obblighi positivi in capo ai fornitori di servizi, tenuti a aderire al Codice di autoregolamentazione "Media e Minori"³⁷ e a garantire particolari cautele nella programmazione destinata ai minori, con specifico riguardo alla comunicazione commerciale. Rilevante è anche la disciplina sull'impiego di minori nei programmi, che richiama l'emanazione di regolamenti attuativi in concerto con diversi dicasteri, a conferma della dimensione intersettoriale del tema. Sul versante della protezione dei dati personali, il legislatore stabilisce il divieto assoluto di utilizzo a fini commerciali dei dati raccolti in relazione ai minori, impedendo così forme di profilazione, pubblicità mirata o marketing diretto³⁸. Infine, la norma introduce obblighi di promozione attiva dell'educazione mediale, prevedendo iniziative scolastiche e programmi informativi rivolti anche ai genitori, da trasmettere nelle fasce di massimo ascolto³⁹, nonché quote di programmazione riservate a contenuti rivolti specificamente al pubblico minorile o comunque adatti a un'audience mista⁴⁰.

L'art. 38 completa e rafforza il quadro tracciato dalla disposizione precedente, disciplinando le attività di vigilanza e il sistema sanzionatorio sul rispetto delle norme a tutela dei minori. La competenza primaria in materia è attribuita all'Autorità per le Garanzie nelle Comunicazioni (di seguito anche solo AGCom), che si avvale del supporto organizzativo del Ministero competente e di un apposito Comitato consultivo⁴¹. L'AGCom è investita del potere di contestare le violazioni, assicurare il contraddittorio con i soggetti responsabili e comminare sanzioni graduate in base alla gravità, alla durata e alla reiterazione delle condotte⁴².

³⁵ Cfr. art. 37, comma 2.

³⁶ Cfr. art. 37, comma 4.

³⁷ Cfr. art. 37, comma 6. Tutti i fornitori di media sono obbligati a rispettare le regole contenute nel Codice di autoregolamentazione "Media e Minori", che doveva essere adottato entro il 31 dicembre 2024.

³⁸ Cfr. art. 37, comma 9.

³⁹ Cfr. art. 37, comma 10.

⁴⁰ Cfr. art. 37, comma 11. L'AGCom è incaricata di stabilire la percentuale minima di trasmissione da riservare a tali contenuti. Nell'ambito del comma 7, in ogni caso, si richiede ai fornitori di garantire ulteriori tutele anche all'interno dei programmi rivolti direttamente ai minori, con particolare attenzione ai messaggi pubblicitari, promozionali e altre forme di comunicazione commerciale.

⁴¹ Cfr. art. 38, comma 1.

⁴² Cfr. art. 38, comma 2.

Le sanzioni spaziano dalle ammende pecuniarie, che possono raggiungere l'importo di 600.000 euro, fino alle misure interdittive più incisive, quali la sospensione del titolo abilitativo o, nei casi di violazione del divieto relativo ai contenuti gravemente nocivi resi disponibili *on demand*, persino la disattivazione degli impianti di trasmissione⁴³.

Dunque, l'art. 38 assicura che le norme a tutela dei minori nei media non restino solo sulla carta, ma siano effettivamente sorvegliate e sanzionate, con un sistema articolato di vigilanza, punizione delle violazioni e rendicontazione pubblica.

A tale proposito, sul piano della pubblicità di tali sanzioni, le stesse, quelle amministrative applicate dall'AGCom e quelle previste dal codice di autoregolamentazione "Media e Minori", quando irrogate dal relativo Comitato, devono essere rese pubbliche. In particolare, chi viene sanzionato può essere obbligato a comunicare la sanzione nei notiziari trasmessi in fascia oraria di massimo ascolto, per garantire trasparenza e deterrenza.

Inoltre, l'AGCOM, insieme ad altri soggetti istituzionali (Autorità garante per l'infanzia, Comitato consultivo interistituzionale, Autorità politica per la famiglia), deve presentare ogni anno al Parlamento, entro il 31 marzo, una relazione dettagliata sulle misure adottate per la tutela dei minori, sui procedimenti avviati e sulle sanzioni applicate; ogni sei mesi, poi, trasmettere alla Commissione parlamentare per l'infanzia e l'adolescenza una relazione informativa sulle attività svolte, con eventuali segnalazioni, osservazioni e suggerimenti⁴⁴.

A proposito dei media cc.dd. "tradizionali", può essere utile richiamare anche l'art. 7 del d.lgs. 2 agosto 2007, n. 145, recante "Attuazione dell'art. 14 della direttiva 2005/29/CE che modifica la direttiva 84/450/CEE sulla pubblicità ingannevole", rubricato "Bambini e adolescenti" ove si afferma che "*è considerata ingannevole la pubblicità che, in quanto suscettibile di raggiungere bambini ed adolescenti, abusa della loro naturale credulità o mancanza di esperienza o che, impiegando bambini ed adolescenti in messaggi pubblicitari, fermo quanto disposto dall'articolo 10 della legge 3 maggio 2004, n. 112, abusa dei naturali sentimenti degli adulti per i più giovani*" e che è altresì ingannevole "*la pubblicità, che, in quanto suscettibile di raggiungere bambini ed adolescenti, può, anche indirettamente, minacciare la loro sicurezza*".

Si aggiunge che il codice del consumo nello stesso senso, al comma 4 dell'art. 21, afferma che "*è considerata, altresì, scorretta la pratica commerciale che, in quanto suscettibile di raggiungere bambini ed adolescenti, può, anche indirettamente, minacciare la loro sicurezza*". Peculiare il fatto che in entrambi questi ultimi testi normativi si parla di "bambini" e non di "minori".

⁴³ Cfr. art. 38, comma 3.

⁴⁴ Cfr. art. 38, comma 5.

Vale la pena menzionare, infine, il decreto 27 aprile 2006, n. 218, che contiene il Regolamento recante disciplina dell'impiego di minori di anni quattordici in programmi televisivi.

3. Minori, internet e piattaforme: le difficoltà dei legislatori nel regolare il rapporto tra minori e tecnologie digitali.

Come rilevato in dottrina⁴⁵, le giovani generazioni mostrano una marcata tendenza ad abbandonare i canali tradizionali soggetti alla regolamentazione legislativa, orientandosi invece verso la rete e i servizi digitali, con particolare predilezione per le piattaforme online. Non si tratta solo dei *social network*⁴⁶ ma anche, ad esempio, delle applicazioni che consentono il tracciamento dell'attività fisica o delle abitudini alimentari, di servizi digitali di sostegno psicologico e, più in generale, di telemedicina.

Tali tecnologie, a maggior ragione se potenziate da algoritmi o sistemi di intelligenza artificiale, non sono meri strumenti di comunicazione, ma un varco attraverso cui anche i più giovani possono accedere senza limiti spaziali a una molteplicità di contenuti, relazioni e opportunità, e, al contempo, un canale attraverso cui il mondo esterno può penetrare, talora in modo invasivo, nella sfera privata⁴⁷. Si tratta, dunque, di tecnologie per loro natura globali, rapide e in continua evoluzione, senza dubbio più invasive di quelle utilizzate nel passato, che, di conseguenza, hanno posto e pongono sfide inedite alla tutela giuridica dell'infanzia.

L'esposizione precoce a contenuti non adeguati all'età e a situazioni di rischio⁴⁸, la circolazione di condotte predatorie o manipolative, le pratiche di profilazione commerciale particolarmente invasive, unitamente ai fenomeni di

⁴⁵ Cfr. A. Dario, A. La Lumia, *Minori, internet e social network*, cit., 7.

⁴⁶ Cfr. la voce *social network*, in *Treccani - Enciclopedia online*, ove si legge che “*con l'espressione social network si identifica un servizio informatico on line che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro. Generalmente i s. n. prevedono una registrazione mediante la creazione di un profilo personale protetto da password e la possibilità di effettuare ricerche nel database della struttura informatica per localizzare altri utenti e organizzarli in gruppi e liste di contatti. Le informazioni condivise variano da servizio a servizio e possono includere dati personali, sensibili (credo religioso, opinioni politiche, inclinazioni sessuali ecc.) e professionali. Sui s. n. gli utenti non sono solo fruitori, ma anche creatori di contenuti. La rete sociale diventa un ipertesto interattivo tramite cui diffondere pensieri, idee, link e contenuti multimediali*”.

⁴⁷ F. Ruggeri, *Minori e privacy*, in E. Battelli (a cura di), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, 141 ss.

⁴⁸ Si pensi a cyberbullismo, condivisione e visualizzazione di contenuti sessuali, istigazione all'anoressia e bulimia e a comportamenti rischiosi, «social challenge», che incoraggiano a partecipare a sfide pericolose e autolesionistiche.

dipendenza tecnologica⁴⁹ e all'insorgenza di disturbi di natura depressiva⁵⁰, alimentare⁵¹ o del sonno⁵², rappresentano solo alcune delle criticità che rendono l'ambiente digitale un contesto potenzialmente lesivo per i minori. Risultano allarmanti anche i dati sull'impatto legato alla fruizione di contenuti pornografici⁵³.

Nonostante tali rischi siano ormai confermati da innumerevoli studi, il mondo di internet, sembra non conoscere più la *summa divisio* tra capacità e incapacità di agire della persona, legata alla minore età che, tradizionalmente, costituisce uno spartiacque per il compimento di atti giuridicamente validi⁵⁴, oltre che consentiti dall'ordinamento.

In disparte i profili diffusamente affrontati dalla dottrina privatistica concernenti il contratto sottoscritto dal minore con il *social network* e la sua

⁴⁹ Con riferimento al fenomeno dell'*Internet Gaming Disorder* – ossia la dipendenza patologica correlata all'utilizzo della rete, che si manifesta principalmente attraverso videogiochi, piattaforme social e contenuti audiovisivi – si osserva che l'Organizzazione mondiale della sanità, a partire dal 2019, ne ha disposto l'inserimento all'interno della classificazione internazionale dei disturbi del comportamento da dipendenza. La rilevanza epidemiologica del fenomeno è confermata dai dati diffusi dal Centro Nazionale Dipendenze e Doping dell'Istituto Superiore di Sanità, secondo i quali, nella fascia scolastica compresa tra gli 11 e i 17 anni, circa il 12% degli studenti – pari a quasi 480.000 soggetti – presenta un rischio concreto di sviluppare tale disturbo. Il dato appare significativamente più elevato nella popolazione maschile (18% nella scuola secondaria di primo grado e 13,8% nella secondaria di secondo grado), rispetto a quella femminile (10,8% e 5,5% rispettivamente), con incidenza massima nella fascia delle scuole medie (14,3% contro il 10,2% delle superiori). A ciò si aggiunge quanto rilevato da *Save the Children*, secondo cui la metà degli adolescenti italiani trascorre mediamente oltre cinque ore al giorno online, con un utilizzo quotidiano di Internet che coinvolge oltre il 91% dei ragazzi tra i 14 e i 17 anni, prevalentemente per attività di messaggistica istantanea (93%), fruizione di contenuti audiovisivi (84%), frequentazione dei social network (79%) e videogiochi (72,4%). Come segnalato, infine, dal *Safer Internet Center Italia*, la c.d. "dipendenza da Internet" può determinare, nei casi più gravi, una vera e propria sindrome, caratterizzata dall'impossibilità di astenersi dalla connessione e dall'insorgenza di un marcato disagio in caso di privazione, con evidenti ripercussioni sulla sfera relazionale, sociale e comportamentale dei minori coinvolti.

⁵⁰ Cfr. E. Bozzola, G. Spina, R. Agostiniani, S. Barni, R. Russo, E. Scarpatò, A. Di Mauro, A.V. Di Stefano, C. Caruso, G. Corsello, A. Staiano, *The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*, in *International Journal of Environmental Research and Public Health*, 19, 2022, 9960 ss.

⁵¹ G. Fioravanti, E. Cassioli, E. Rossi, L. Lucherini Angeletti, S. Casale, V. Ricca, G. Castellini, *The relationship between problematic Instagram use and eating disorders psychopathology: an explanatory structural equation model*, in *Soc. Psychiatry Psychiatr Epidemiol*, 2024, 59, 1617 ss.

⁵² R. Alonzo, J. Hussain, S. Stranges, K.K. Anderson, *Interplay between social media use, sleep quality, and mental health in youth: A systematic review*, in *Sleep Med. Review*, 56, 2021.

⁵³ Cfr. risoluzione del Consiglio d'Europa, *Pornografia minorile – mezzi e disposizioni di contrasto all'esposizione delle persone di minore età a contenuti pornografici*, aprile 2022, ove si segnala l'allarmante incremento dell'esposizione dei minori a materiale pornografico reso possibile dalla facilità di accesso alle piattaforme digitali, evidenziandone i potenziali effetti pregiudizievoli sulla salute e sullo sviluppo (dipendenza, stereotipi di genere, difficoltà relazionali). In termini analoghi v. anche il rapporto del Governo australiano, *The effects of pornography on children and young people*, 2017, che sottolinea il rischio, in particolare per gli adolescenti di sesso maschile, di una maggiore propensione a condotte di aggressione sessuale.

⁵⁴ A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 10.

capacità negoziale⁵⁵, la responsabilità genitoriale per fatto illecito compiuto dal minore online⁵⁶ e la responsabilità dei gestori delle piattaforme, nell'ambito della presente analisi ci si sofferma sui profili più squisitamente pubblicistici del tema, con particolare riguardo alle tecniche di regolazione e ai diritti digitali.

Un'eccezione alla generale assenza di regolazione sul tema è rappresentata dalla normativa in materia di protezione dei dati personali, ambito in cui è emersa – ma solo a partire dal 2018⁵⁷, con il Regolamento 2016/679 – una maggiore consapevolezza circa la necessità di salvaguardare l'identità e la riservatezza dei minori online⁵⁸.

Come si approfondirà nel prosieguo, il legislatore europeo ha introdotto specifiche disposizioni riguardanti il trattamento dei dati personali dei minori, imponendo limiti d'età per la validità del consenso e richiedendo un linguaggio chiaro e comprensibile nelle informative rivolte agli stessi. Parte della dottrina, peraltro, reputa tale tutela già in parte superata dalle tecnologie successivamente sviluppate⁵⁹. I riflessi degli effetti di queste nuove modalità tecnologiche, nei diversi settori saranno, a parere di alcuni, così dirompenti, da richiedere, ancora una volta, una risposta giuridica condivisa a livello europeo, che tenga conto dell'abbattimento delle barriere spaziali, operato dalla rete.

Sempre il legislatore europeo, come si vedrà più avanti, nell'affrontare la questione della regolamentazione dei servizi digitali, in particolare per quanto riguarda le piattaforme e i motori di ricerca di maggiori dimensioni – ormai non più rinviabile – sta dedicando ora particolare attenzione ai minori, concentrando i propri sforzi sugli strumenti di verifica dell'età.

Se, come evidenziato, la normativa nazionale e sovranazionale tradizionalmente riservano ai minori una particolare attenzione⁶⁰, riconoscendoli

⁵⁵ E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 114 ss.; nonché, ancora, A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 28.

⁵⁶ Per un approfondimento sulla responsabilità da atto illecito di cui all'art. 2048 c.c. e su altri profili che ineriscono la responsabilità genitoriale cfr. E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 127-132. Sul tema v. anche D. Pierantoni, *Minori su Internet: profili di responsabilità*, in *Riv. it. inf. dir.*, 2024, 399 ss.; A. Dario, A. La Lumia, *Minori, internet e social network*, Milano, 2021, 12 ss.

⁵⁷ Cfr. sul tema il rapporto "On line age verification methods for children", redatto dall'EPRS nel febbraio 2023.

⁵⁸ A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 26, ove con riferimento alla protezione dei dati personali l'A. parla di una disciplina "disomogenea" a cui avrebbe posto rimedio il GDPR.

⁵⁹ *Ibidem*, 3. L'A., già in premessa, ritiene positivo l'intervento del GDPR nella misura in cui avrebbe previsto una specifica tutela per i minori. Tuttavia, quella del Regolamento n. 2016/679/UE sembra, a parere di Astone, quasi una disciplina di "chiusura" di una fase che sta per essere rivoluzionata da forme sempre più sofisticate di raccolta e analisi dei dati, destinate a superare il sistema del web 3.0.

⁶⁰ In molteplici settori del diritto, infatti, i minori beneficiano di garanzie speciali volte a proteggerne lo sviluppo fisico, psicologico ed educativo: basti pensare al diritto di famiglia, al diritto penale minorile o al diritto all'istruzione.

come soggetti meritevoli di una tutela rafforzata in quanto “vulnerabili” per definizione⁶¹, tale sensibilità non ha trovato un corrispettivo altrettanto efficace e sistematico con riferimento alla regolazione della relazione dei minori con le tecnologie⁶². La protezione in ambito digitale si è rivelata, infatti, certamente tardiva, e, in ogni caso, frammentaria e spesso subordinata a interessi di natura economica o tecnica.

In altre parole, nonostante l’evidente asimmetria tra vulnerabilità del minore e potenza degli strumenti digitali cui ha accesso e i dati preoccupanti che si registrano sui danni che tale squilibrio ha comportato e comporta, il legislatore – tanto a livello nazionale quanto sovranazionale – ha esitato a predisporre un *corpus* normativo organico e specificamente orientato alla protezione dei minori nei contesti digitali⁶³.

Le motivazioni della iniziale inerzia del legislatore sono da ricercare, come rilevato da autorevole dottrina, nel più complesso rapporto tra regolazione e tecnologie⁶⁴.

Si registra, infatti, in generale, una condizione di “solitudine” di un legislatore che, per lunghi periodi, rimane inerte di fronte alle frenetiche accelerazioni imposte dalla tecnologia: un legislatore progressivamente relegato ai margini, insieme al principio di certezza del diritto e, secondo alcuni, alla stessa legittimazione del circuito democratico rappresentativo, a vantaggio di un attivismo dei giudici sempre più spinto, nel quale il confine tra interpretazione creativa e manipolazione tende a farsi pericolosamente labile⁶⁵.

⁶¹ E. Andreola, *Minori e incapaci in Internet*, Napoli, 2019, 12, il quale descrive il minore come “il consumatore più debole tra i consumatori”, poiché, “se il consumatore è solo talvolta la parte debole del contratto, il minore lo è per condizione”.

⁶² Sul punto si riporta letteralmente la felice espressione di A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, cit., 7, il quale afferma che “Proprio il “corpo elettronico” dei minori nativi digitali, posti in una condizione di oggettiva debolezza, è stato, per lungo tempo, sguarnito di quelle garanzie e tutele di cui l’ordinamento giuridico si è fatto carico nel “mondo reale in funzione di garantire quello che, con una formula ormai nota, viene definito il best interest of child”.

⁶³ E. Battelli, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, cit., 113. Cfr. altresì l’all. B alla delibera n. 96/25/CONS di approvazione del Regolamento AGCOM nel quale si legge “Prima dell’adozione del Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore nel 2018, non esistevano restrizioni specifiche al trattamento online dei dati dei minori in Europa”.

⁶⁴ Come ricorda M. Luciani, *Quale identità?*, cit., 353, “Di fronte alle sfide dello sviluppo tecnico-scientifico, il diritto riesce a rispondere solo con notevole ritardo. Il diritto ha bisogno della forma e, sebbene la regolazione giuridica sia sempre più spesso incapace di disegnare forme astratte idonee all’inquadramento dei fenomeni sociali, il processo di formalizzazione giuridica della regolazione richiede tempo”.

⁶⁵ O. Pollicino, *Regolazione e innovazione tecnologica nell’«ordinamento della rete»*, in *Riv. AIC*, 2025, 126 ss., evidenzia che occorre, tuttavia, riconoscere che l’inerzia del potere legislativo non è sempre frutto di costrizione, ma spesso è in parte volontaria: per evitare di rimanere costantemente in ritardo rispetto al ritmo dell’innovazione tecnologica, infatti, il legislatore preferisce non intervenire, delegando così ai giudici decisioni di grande impatto, talvolta drammatiche. Tali scelte implicano delicati bilanciamenti rispetto a una tecnologia tutt’altro che neutrale, intrisa di significati assiologici e sostanziali.

Si aggiungono, poi, due ulteriori fattori che contribuiscono alla crisi del legislatore sul tema.

In primis, l'evidente straripamento dell'attività, anche paranormativa e regolatoria, delle Autorità indipendenti competenti. Tale iperattività ha portato spesso alla sovrapposizione tra le Autorità stesse a danno dell'efficacia della tutela degli utenti, tra i quali i minori⁶⁶.

Inoltre, la pervasività della produzione normativa dell'Unione europea, ancor più forte sul tema delle tecnologie, che ha limitato lo spazio di intervento del legislatore nazionale⁶⁷.

Negli ultimissimi tempi, come anticipato, si è registrata un'intensa attività legislativa, contraddistinta da una molteplicità di interventi normativi e dall'elaborazione di numerosi progetti di legge, sia a livello nazionale⁶⁸ sia nel contesto europeo⁶⁹.

Nonostante ciò, permane, comunque, la carenza di una normativa organica che protegga i diritti dei minori – i quali, nel contesto digitale, si propongono come soggetti attivi o la cui presenza è promossa dai genitori – in grado di affrontare compiutamente i fenomeni oggetto di questa analisi e capace di coniugare tutela rafforzata, effettività e rapidità di adattamento al progresso tecnologico.

In effetti, , come opportunamente evidenziato dalla più autorevole dottrina, la produzione normativa che il legislatore ha ultimamente espresso in maniera convulsa e ridondante in relazione alle tecnologie e ad alcuni peculiari fenomeni della dimensione digitale appare suscettibile di tradursi in una iperregolamentazione che, lungi dal costituire garanzia di effettività, non appare *ex se* idonea a realizzare in modo compiuto le finalità perseguite e può anzi rivelarsi foriera di rilevanti criticità applicative⁷⁰.

4. La protezione dei dati personali dei minori nell'ambiente digitale.

Come evidenziato, nel contesto descritto, fino ai tempi più recenti il principale presidio per i minori nella dimensione digitale, è stato rappresentato dalla normativa in materia di protezione dei dati personali. Ciò anche grazie, anzitutto, alla centralità assunta dalla “privacy” nel suo nuovo significato con il quale, come già anticipato nella presente trattazione, non si intende più solo la protezione della

⁶⁶ Sia consentito ancora il rinvio a F. Ricciulli, *L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti*, cit., 361.

⁶⁷ O. Pollicino, *Regolazione e innovazione tecnologica nell'«ordinamento della rete»*, cit., 131.

⁶⁸ Tra gli altri, v., in materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori, A.A.C. 1217, 1771, 1800 e 1863.

⁶⁹ Come riportato nel report “On line age verification methods for children” dell'EPRS numerosi Paesi stanno introducendo leggi e/o codici di condotta per affrontare questo tema.

⁷⁰ Per un approfondimento sul tema della ipertrofia normativa sul tema delle tecnologie e sulla attuale esigenza di semplificazione, cfr. cap. II.

sfera privata e il “diritto di essere lasciati soli”⁷¹ ma più che altro quello di controllare la circolazione dei propri dati personali e di tutelare la propria identità⁷².

Con particolare riferimento alla protezione dei dati personali dei minori, non si può non prendere le mosse dal già menzionato Regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, (di seguito anche RGPD o, in inglese, GDPR)⁷³.

Ai fini della presente analisi vale la pena ricordare che l’adozione di tale Regolamento, tra le altre esigenze, rispondeva a quella di aggiornare la normativa sul trattamento dei dati alla luce della digitalizzazione nel frattempo avvenuta. La trasformazione digitale, infatti, ha profondamente modificato il modo in cui i dati personali vengono raccolti, trattati e scambiati, aumentando esponenzialmente la quantità di informazioni generate e condivise online⁷⁴. Questa evoluzione ha reso necessaria l’adozione del Regolamento per garantire una protezione efficace dei dati nell’era digitale, armonizzando le norme tra gli Stati membri dell’UE e rafforzando i diritti degli individui. Il Regolamento risponde all’esigenza di tutelare la privacy in un contesto in cui tecnologie come i *social media*, il *cloud computing* e l’intelligenza artificiale espongono gli utenti a nuovi rischi⁷⁵.

Va tuttavia chiarito, come osservato dalla più autorevole dottrina, che la finalità in esame è rivolta indistintamente a tutti gli individui, senza che il Regolamento preveda, con riguardo all’ambito di applicazione soggettivo, riferimenti specifici a categorie particolari di soggetti – quali, ad esempio, i minori

⁷¹ S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 193 ss.

⁷² Sul tema cfr. S. Rodotà, *Intorno alla privacy. Ipotesi e prospettive*, in AA.VV., *Studi in memoria di Franco Piga*, Milano, 1992, 1 ss.; A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, cit., 9.

⁷³ Cfr. sul punto G. Spoto, *Disciplina del consenso e tutela del minore*, in S. Sica, V. D’Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 111 ss.

⁷⁴ Cfr. G. Resta, *Governare l’innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, 199 SS.

⁷⁵ Cfr. considerando 6 e 7 del regolamento ove si prevede rispettivamente che: *La rapidità dell’evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l’economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all’interno dell’Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali; Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell’Unione, affiancato da efficaci misure di attuazione, data l’importanza di creare il clima di fiducia che consentirà lo sviluppo dell’economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.*

– salvo naturalmente le disposizioni espressamente dedicate, che saranno analizzate in seguito⁷⁶.

L'utilizzo dei cc.dd. “nuovi media”, ossia quelli che si servono della rete, del resto, implica una consistente circolazione di dati personali, anche di soggetti, quali minori, che, come si è detto, sono in fase di formazione⁷⁷. Si considerino, ad esempio, le tecniche di profilazione e quelle finalizzate alla patrimonializzazione dei dati personali, che si fondano proprio sulle informazioni raccolte dai gestori dei servizi. Questi dati vengono spesso forniti dagli utenti in modo inconsapevole, fenomeno ancor più preoccupante quando si tratta di minori⁷⁸.

Con specifico riferimento al tema in oggetto, occorre partire dall'analisi dei considerando del Regolamento che, come noto, contengono i principi ispiratori dell'intera disciplina contenuta nello stesso.

In particolare, ai fini della presente analisi, rilevano i Considerando 38, 58 e 65 del richiamato Regolamento

Il Considerando 38 sottolinea che i minori necessitano di una protezione speciale dei loro dati personali, poiché possono non essere pienamente consapevoli dei rischi che corrono e dei propri diritti. Questa protezione è particolarmente importante per l'uso dei dati a fini di *marketing*, profilazione e raccolta durante l'uso di servizi rivolti direttamente a loro. Tuttavia, il consenso dei genitori non è richiesto per servizi di prevenzione o consulenza forniti direttamente al minore.

Il Considerando 58, poi, relativo alla trasparenza, con riferimento ai minori, precisa che “*Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente*”⁷⁹.

⁷⁶ C. Camardi, *Minore e privacy nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2019, 122 ss.

⁷⁷ F. Ruggeri, *Minori e privacy*, in E. Battelli (a cura di), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, 141 ss. Con riferimento alla tutela rafforzata dedicata ai minori dalla normativa in materia di protezione dei dati personali, l'A. evidenzia che “*in questo contesto, infatti, il diradamento dei contatti reali con altre persone rischia di non far riconoscere i limiti alla condivisione di informazioni di carattere personale*”. Sul tema cfr., altresì, G. Pedrazzi, *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, in *Inf. e dir.*, 2017, 437 ss.

⁷⁸ E. Battelli (a cura di), *Diritto Privato Digitale*, cit., 132, Secondo l'A “*il fisiologico sviluppo e la graduale maturazione dei minori espongono questi ultimi maggiormente rispetto agli adulti, rendendoli più facilmente oggetto delle più subdole e invasive tecniche di targeting e di marketing*”. Cfr. anche V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, cit., 25.

⁷⁹ Cfr. E. Battelli (a cura di), *Diritto Privato Digitale*, cit., 136, sulla critica al c.d. “consenso digitale”; C. Irti, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 2019, 617 ss., ove l'A. rileva come, nonostante i propositi della normativa in materia di trasparenza, il minore andrebbe oggettivamente e soggettivamente messo nelle condizioni di compiere consapevolmente le proprie valutazioni. Se è poco trasparente il trattamento dei dati e la loro circolazione, allora perde di valore anche il consenso, che pure viene criticato dalla dottrina citata. Sul punto si veda anche L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, 254 ss., 257, afferma che “*il consenso si rivela mero simulacro di*

Il Considerando 65, infine, riconosce una particolare tutela ai minori in relazione al diritto alla cancellazione dei dati personali (c.d. “diritto all’oblio”)⁸⁰. Tale diritto assume rilievo specifico quando il trattamento si basa sul consenso prestato dall’interessato durante la minore età, fase in cui potrebbe non aver pienamente compreso i rischi connessi al trattamento dei propri dati, in particolare se diffusi online. Il Regolamento prevede, dunque, che, una volta raggiunta la maggiore età, l’interessato possa esercitare il diritto alla cancellazione, anche indipendentemente dal fatto di non essere più minore, al fine di eliminare dati personali trattati sulla base di un consenso ritenuto non pienamente consapevole al momento della prestazione.

Il Regolamento, colmando un vuoto sul tema⁸¹, dedica, poi, una specifica disposizione, l’art. 8 GDPR, alle “*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell’informazione*”. In particolare, l’articolo stabilisce le condizioni per la liceità del trattamento dei dati personali dei minori in relazione all’offerta diretta di servizi della società dell’informazione basata sul consenso (art. 6, par. 1, lett. a). Il trattamento è lecito se il minore ha almeno 16 anni; se ha un’età inferiore, è necessario il consenso – o l’autorizzazione – del titolare della responsabilità genitoriale. Come rilevato dalla dottrina, la disposizione, basandosi sul raggiungimento di una determinata età a partire dalla quale è possibile esprimere autonomamente il consenso, sembra individuare diverse fasi della minore età⁸².

Gli Stati membri, per espressa previsione del Regolamento, possono abbassare questo limite previsto dalla normativa sovranazionale⁸³, ma non al di sotto dei 13 anni⁸⁴.

Infine, sempre ai sensi dell’art. 8 GDPR, il titolare del trattamento deve compiere ogni sforzo ragionevole, tenendo conto della tecnologia disponibile, per verificare che tale consenso genitoriale sia effettivamente prestato. La disposizione lascia impregiudicato il diritto nazionale in materia di capacità contrattuale dei minori.

autodeterminazione e quindi inadeguato strumento di protezione, mostrando la propria ontologica debolezza quale espressione di autodeterminazione e strumento di tutela del mercato del dato”.

⁸⁰ Cfr. R. Senigaglia, *Reg. UE 2016/679 e diritto all’oblio nella comunicazione telematica. Identità, informazione e trasparenza nell’ordine della dignità personale*, in *Nuove leggi civ. comm.*, 2017, 1023 ss.

⁸¹ E. Battelli (a cura di), *Diritto Privato Digitale*, cit., 132; nonché, A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, cit., 25.

⁸² Cfr. M. Nitti, *La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in *Fam. dir.*, 2018, 390, ss.

⁸³ Cfr. A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, cit., 27, secondo il quale tale deroga vanificherebbe il tentativo di armonizzazione operato dal Regolamento.

⁸⁴ Tale limite è previsto dal *Children’s Online Privacy Protection Act*.

Occorre precisare che l'art. 8 GDPR, come si evince dalla rubrica, non intende essere una disposizione dedicata in generale al consenso del minore rispetto al trattamento dei propri dati personali, quanto più una specifica norma dedicata al caso in cui è utente dei "servizi della società dell'informazione"⁸⁵. Va precisato altresì che la disposizione si applica ai soli servizi "offerta direttamente" a soggetti minori e non si applica al caso in cui il prestatore di servizi dichiara espressamente che i suoi servizi sono resi a un pubblico composto esclusivamente da persone maggiorenni⁸⁶.

Ebbene, dal complesso delle disposizioni contenute nel Regolamento si evince che il minore, come si rilevava con riferimento ad altri settori dell'ordinamento, viene considerato più vulnerabile e per questo soggetto a cui dedicare una tutela specifica e rafforzata⁸⁷. In particolare, per questa categoria, passando da una tutela formale e astratta ad una reale e concreta⁸⁸, sono stati introdotti meccanismi di protezione specifici declinati sul limite di età per esprimere il consenso e sugli obblighi informativi⁸⁹. Si evince, però, altresì il tentativo del legislatore europeo di bilanciare l'esigenza di una speciale protezione con quella di lasciare uno spazio di autodeterminazione al soggetto minore⁹⁰. Ciò nonostante, parte della dottrina si

⁸⁵ Come noto, la definizione è contenuta all'art. 1, § 1, lett. b) della direttiva n. 2015/1535/Ue, ove si legge che "1. Ai fini della presente direttiva si applicano le seguenti definizioni: a) «prodotto»: i prodotti di fabbricazione industriale e i prodotti agricoli, compresi i prodotti della pesca; b) «servizio»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per: i) «a distanza»: un servizio fornito senza la presenza simultanea delle parti; ii) «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici; iii) «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale". Cfr., altresì, F. Resta, *commento all'art. 8*, in E. Belisario, G. Scorza, G.M. Riccio (a cura di), *Commentario del GDPR e normativa privacy*, Padova, 2022, 106 ss.

⁸⁶ F. Ruggeri, *Minori e privacy*, cit., 148.

⁸⁷ Cfr., oltre alle disposizioni menzionate, anche gli artt. 6, par. 1, lett. f; 12, par. 1; 17, par. 1, lett. F; 40, par. 2, lett. g; 57, par. 1, lett. b del Regolamento. Per un approfondimento sull'approccio *vulnerable data subjects* sia a livello europeo, sia internazionale cfr. anche A. Soro, *Vulnerable Person: Data Protection and Digital Society*, in *Italian American Bar Ass'N Journal*, 2016, 117 ss.; P. Stanzione, *Data protection and Vulnerability*, in *European Journal of Privacy Law and Tech*, 2020, 9 ss.; V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, cit.; F. Resta, *commento all'art. 8*, cit., 106-107.

⁸⁸ A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, cit., 25.

⁸⁹ V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, cit., 70.

⁹⁰ F. Ruggeri, *Minori e privacy*, cit., 149. Sul punto l'autore afferma che "Rispetto al trattamento dei dati, nello specifico, può però rilevarsi ancora una volta una peculiare caratteristica. Ovvero che la rete enfatizza più che mai la contraddizione propria dei minori di oggi: sempre più autonomi, da un lato; sempre più esposti al rischio, dall'altro. Indipendenti ma vulnerabili, alla ricerca della libertà ma bisognosi di tutela, nella vita virtuale ormai forse più che in quella reale".

interroghi sulla attualità di una disciplina differenziata per la protezione dei dati dei minori rispetto ai maggiori di età⁹¹.

Durante l'assemblea plenaria del febbraio 2025, il Comitato europeo per la protezione dei dati (European Data Protection Board o "EDPB") ha adottato una dichiarazione sui sistemi di verifica dell'età, rilevando come tale misura sia essenziale per impedire ai minori di accedere a contenuti non appropriati alla loro età. Allo stesso tempo, l'EDPB ha riconosciuto che il metodo di verifica dell'età deve essere il meno invasivo possibile e che resta primaria l'esigenza di tutelare i dati personali dei minori⁹².

Venendo alla normativa nazionale in materia di protezione dei dati personali, il D.lgs. 196/2003, come modificato dal d.lgs. n. 101/2018 (di seguito anche "Codice Privacy"), aggiornato in attuazione del Regolamento (UE) 2016/679 (GDPR), dedica una specifica attenzione alla protezione dei dati personali dei minori, riconoscendone la particolare vulnerabilità nell'ambiente digitale. In particolare, l'art. 2-*quinqüies* del Codice stabilisce le condizioni per la validità del consenso prestato da un minore in relazione all'offerta diretta di servizi della società dell'informazione, ossia quei servizi (come *social network*, piattaforme online, app, giochi digitali, servizi in cloud) che sono normalmente forniti a pagamento o gratuitamente via Internet.

Secondo quanto previsto dalla normativa italiana, i minori di età inferiore ai 14 anni non possono prestare autonomamente il consenso al trattamento dei propri dati personali per tali servizi. In questi casi, il trattamento è lecito solo se il consenso è prestato o autorizzato da chi esercita la responsabilità genitoriale sul minore (genitori o tutori legali). Una volta compiuti i 14 anni, invece, il minore può validamente esprimere il proprio consenso in autonomia.

La soglia dei 14 anni è stata fissata dall'Italia nell'ambito della menzionata facoltà riconosciuta dal GDPR agli Stati membri, che, come esposto, consente di abbassare il limite dei 16 anni previsto a livello europeo, purché non al di sotto dei 13 anni⁹³.

In effetti, il Legislatore nazionale, con questa previsione, ha introdotto nell'ambito dell'ordinamento italiano una eccezione alla regola generale dettata dall'art. 2 c.c. per cui la capacità di agire si acquista al compimento del diciottesimo anno di età⁹⁴.

Oltre alla questione dell'età, il Codice Privacy impone al titolare del trattamento una serie di obblighi aggiuntivi per garantire che il consenso sia

⁹¹ L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, cit., 258.

⁹² Cfr. statement 1/25 on Age Assurance dell'European Data Protection Board (EDPB).

⁹³ Sulla scelta dei quattordici anni cfr. F. Resta, *commento all'art. 8*, cit., 108, ove si evidenzia nell'ordinamento italiano viene riconosciuta una sia pur parziale capacità di agire al minore quattordicenne. Si veda, ad esempio, la l. 29 maggio 2017, n. 71 in materia di cyberbullismo.

⁹⁴ F. Ruggeri, *Minori e privacy*, cit., 150.

effettivamente valido e consapevole. Tra questi, vi è l'obbligo di adottare misure ragionevoli, in base alle tecnologie disponibili, per verificare che, nei casi richiesti, il consenso sia effettivamente fornito o autorizzato da chi ha la responsabilità genitoriale. Questo può avvenire, ad esempio, attraverso procedure di conferma via e-mail, dichiarazioni esplicite o strumenti di verifica dell'identità.

Un altro aspetto importante riguarda l'informativa sul trattamento dei dati. Quando il destinatario del servizio è un minore, l'informativa deve essere redatta con un linguaggio chiaro, semplice e facilmente comprensibile, adeguato al livello di maturità del minore stesso. Questo per assicurare che il minore possa comprendere realmente quali dati vengono trattati, per quali finalità e quali sono i suoi diritti in materia di protezione dei dati personali.

Infine, il Codice Privacy chiarisce che le disposizioni relative al consenso per il trattamento dei dati non interferiscono con le norme generali del diritto contrattuale italiano. Ciò significa che, anche se un minore può prestare validamente il consenso al trattamento dei dati personali per l'uso di un servizio online, tale circostanza non implica automaticamente che egli abbia la capacità giuridica di concludere un contratto con piena efficacia: tale capacità resta disciplinata dalle norme civilistiche in materia di minori.

Fatte queste premesse sulla normativa, va rilevato che il Garante per la Protezione dei Dati Personali è intervenuto più volte sul tema, non solo attraverso un'importante attività di sensibilizzazione e orientamento⁹⁵, ma anche mediante l'adozione di numerosi provvedimenti. In gran parte si tratta di interventi relativi al tema della verifica dell'età⁹⁶. Del resto, come anticipato, l'art. 8 par. 2 chiede al titolare del trattamento di adoperarsi in ogni modo ragionevole per verificare che il consenso del minore sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, ma non precisa con quali modalità, salvo aggiungere “*in considerazione delle tecnologie disponibili*”. Ma v'è di più. Se è richiesto che tali soggetti ottengano il consenso dei genitori prima di trattare i dati personali del minore, non vi è però alcun “previo” obbligo – all'interno della normativa in

⁹⁵ L'espressione “*Se non ha l'età, i social possono attendere*”, ad esempio, è lo *slogan* di una campagna di sensibilizzazione lanciata dal Garante per la protezione dei dati personali e Telefono Azzurro nel febbraio 2021, in seguito al caso della tragica morte di una bambina per una “sfida” su TikTok. L'obiettivo della campagna è quello di mettere in guardia i genitori sui pericoli della rete e sull'importanza di verificare l'età dei figli prima che si iscrivano ai social network, le cui soglie minime di età sono stabilite dalla normativa nazionale e sovranazionale.

⁹⁶ Alla luce di tale limite previsto dalla normativa nazionale e sovranazionale, l'Autorità garante italiana per la protezione dei dati personali è a più riprese intervenuta con una serie di provvedimenti rivolti ai titolari del trattamento, richiamando la necessità di approntare misure idonee a verificare l'età dei minori. Sul tema cfr. provvedimento del 22 gennaio 2021 - registro dei provvedimenti n. 20 del 22 gennaio 2021; provvedimento del 7 luglio 2022 - registro dei provvedimenti n. 248 del 7 luglio 2022; provvedimento del 2 febbraio 2023 - Registro dei provvedimenti n. 39 del 2 febbraio 2023; provvedimento del 30 marzo 2023 - registro dei provvedimenti n. 112 del 30 marzo 2023; provvedimento dell'11 aprile 2023 - registro dei provvedimenti n. 114 dell'11 aprile 2023.

materia di privacy – di verificare la reale età del minore o l’effettivo coinvolgimento di chi esercita la responsabilità genitoriale⁹⁷.

Tuttavia, come già accennato, la tutela dei dati personali del minore nel contesto digitale non si limita alla verifica dell’età per l’accesso ai servizi a lui destinati o al consenso, espresso dal minore o dai genitori, per l’utilizzo dei servizi informativi rivolti ai più giovani. Essa comprende anche diverse situazioni legate alla diffusione della sua immagine online e dunque alla sua identità nella nozione “sostanziale”. Nel prosieguo verranno esaminate nel dettaglio le posizioni dell’Autorità in merito ai fenomeni dello “*sharenting*”, dei “*baby influencer*”, nonché dell’utilizzo di sistemi e modelli basati su intelligenza artificiale.

5. La verifica dell’età come strumento di protezione: una prospettiva transnazionale e interdisciplinare.

Il tema dei sistemi di verifica dell’età assume un ruolo centrale nel contesto della disciplina giuridica dei rapporti tra minori e servizi della società dell’informazione.

La sua introduzione tocca un tema di fondo di politica normativa in quanto si tratta di un approccio preventivo ai problemi e che, pur volendo tutelare una categoria specifica come i minori, di fatto, comporta la verifica di massa di tutti gli utenti⁹⁸.

Sebbene esso, come esposto, venga in rilievo già nell’ambito nella normativa in materia di protezione dei dati personali – in particolare, ai sensi dell’art. 8 GDPR – la sua rilevanza si estende ben oltre tale comparto normativo, configurandosi come una questione intersettoriale, che coinvolge trasversalmente diversi rami del diritto, accomunati dall’intento di garantire una tutela effettiva e sostanziale dei soggetti minorenni nello spazio digitale⁹⁹.

⁹⁷ Cfr. A. Astone, *I dati personali dei minori in rete. Dall’internet delle persone all’internet delle cose*, cit., 28, ove l’A. propone in queste pagine un sistema di notifica tramite mail a chi esercita la potestà genitoriale al momento in cui avviene la creazione di un account social da parte del figlio minore e altri sistemi più intrusivi mutuati dalla prassi statunitense.

⁹⁸ Cfr. G.M. Riccio, *Chat Control: sorveglianza di massa in nome della protezione dei minori?*, in *Corriere delle comunicazioni*, 16 ottobre 2025. L’Autore tratta il diverso tema della proposta di Regolamento dell’Unione Europea per prevenire e combattere l’abuso sessuale sui minori online (c.d. CSA Regulation), nota al pubblico come “Chat Control”. L’analisi sull’approccio regolatorio vale tuttavia anche per la verifica dell’età. In quel caso, la normativa europea imporrebbe ai fornitori di servizi di comunicazione (come WhatsApp, Signal, Instagram, e provider di e-mail) di dotarsi di strumenti per rilevare, segnalare e rimuovere materiali contenenti abusi sessuali sui minori. Questo avverrebbe tramite una scansione, su larga scala, di tutte le comunicazioni private, nota come *client-side scanning*.

⁹⁹ Per un approfondimento sul tema dell’*age verification* in senso ampio cfr. *Report age verification online, rischi e strumenti di tutela dei diritti dei minori* del Centro di ricerca interdipartimentale Europeo di Studi Avanzati sull’Innovazione Digitale (Research Center IDEAS – Innovation Digital European Advanced Studies) del 24 giugno 2025.

Sul piano della *data protection*, come esposto, la verifica dell'età costituisce una condizione di liceità del trattamento in relazione ai minori che accedano a servizi digitali. L'obbligo per i titolari del trattamento di implementare sistemi idonei ad accertare l'età dell'utente, e – ove necessario – a raccogliere il consenso del titolare della responsabilità genitoriale, impone l'adozione di misure tecniche e organizzative adeguate, nel rispetto del principio di *accountability*¹⁰⁰. Tuttavia, come già rilevato, l'applicazione concreta di tali obblighi si scontra con la persistente assenza di *standard* armonizzati a livello europeo in merito agli strumenti di verifica, nonché con tensioni tra esigenze di tutela e principi di proporzionalità e minimizzazione dei dati.

La questione, però, non può esaurirsi in una prospettiva di tipo esclusivamente *privacy-oriented*. In altre parole, il tema non è solo quale sia l'età adeguata a esprimere il consenso rispetto all'utilizzo dei servizi della società dell'informazione, potendo essere altre le esigenze legate alla verifica dell'età dell'utente. Si considerino, ad esempio, i principi di non discriminazione, di libertà e sicurezza, così come i diritti alla libertà di espressione e di informazione. Il tema si estende, inoltre, a profili connessi al benessere e alla salute. Proprio per tali ragioni, la questione della verifica dell'età è stata oggetto di attenzione da parte di diverse branche del diritto e diverse autorità.

Nell'ambito del diritto contrattuale, si pone il tema della capacità di agire del minore nel concludere rapporti giuridici mediante l'adesione a contratti digitali – frequentemente mediante meccanismi di *click-wrap* o *browse-wrap* – con conseguenti riflessi in termini di validità, efficacia e annullabilità degli atti compiuti. Il ricorso a forme di verifica dell'età rappresenta, in tale contesto, uno strumento funzionale alla tutela dell'affidamento legittimo dei prestatori di servizi, ma al contempo deve essere compatibile con le regole dettate in materia di capacità giuridica e capacità d'agire, nonché con la disciplina consumeristica.

Non meno rilevante è l'interazione tra la verifica dell'età e il diritto penale, soprattutto nei casi in cui l'accesso dei minori a contenuti digitali non filtrati espone questi ultimi a concreti rischi di lesione della propria integrità psicofisica. La verifica dell'età, in tali ipotesi, assume una valenza parapreventiva, idonea a scongiurare fenomeni lesivi quali l'adescamento online, la diffusione di materiale pedopornografico, il cyberbullismo, nonché l'accesso a contenuti violenti, discriminatori o sessualmente espliciti. In tal senso, essa costituisce un presidio a tutela non solo della persona del minore, ma anche dell'ordine pubblico digitale.

Analogamente, nel contesto del diritto dei consumatori, la verifica dell'età rileva quale strumento di prevenzione rispetto a pratiche commerciali scorrette, profilazioni occulte, dark patterns e altre tecniche persuasive non adeguatamente percepibili da soggetti non pienamente consapevoli. In presenza di utenti

¹⁰⁰ Ai sensi dell'art. 5, par. 2, “*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»)*”.

minorenni, l'esigenza di una verifica affidabile dell'età si salda con quella di assicurare la speciale protezione che l'ordinamento riconosce ai consumatori vulnerabili, secondo quanto previsto dalla normativa unionale in materia (cfr. direttiva 2005/29/CE).

Inoltre, come si vedrà, il tema della verifica dell'età è oggetto di crescente attenzione anche nel diritto amministrativo e regolamentare, come evidenziato, tra l'altro, dalle previsioni del *Digital Services Act* (Reg. 2022/2065/UE), il quale, come si approfondirà nel prosieguo, impone ai prestatori di piattaforme online obblighi specifici in relazione all'esposizione dei minori a contenuti illeciti o dannosi. Il quadro normativo emergente richiede l'adozione di sistemi di *age assurance* e *age verification* che siano al contempo efficaci, proporzionati, interoperabili e rispettosi dei diritti fondamentali.

Infine, non può sottacersi la dimensione internazionale e comparatistica del problema. La varietà di soluzioni normative adottate nei diversi ordinamenti in merito all'età minima per l'accesso a contenuti o servizi digitali, nonché alle modalità tecniche ammesse per la verifica dell'età, genera significative difficoltà di armonizzazione normativa, oltre a porre questioni di *conflict of laws* e coordinamento transfrontaliero, in particolare nei casi di prestatori di servizi stabiliti extra UE ma operanti sul territorio dell'Unione.

La verifica dell'età si configura, dunque, come una questione di sistema, che impone un ripensamento organico e multilivello degli strumenti giuridici attualmente disponibili. Essa non può essere affrontata in maniera frammentata, né esclusivamente mediante strumenti tecnici o automatizzati, ma necessita di una *governance* integrata che coinvolga normatori, garanti, operatori economici, tecnologi e società civile, nel quadro di un equilibrato bilanciamento tra tutela dei minori, libertà di iniziativa economica, diritto all'educazione digitale e diritti fondamentali della persona.

5.1. La disciplina sovranazionale in tema di verifica dell'età: la tutela dei minori nel Digital Services Act.

Più di recente, i temi dei servizi digitali e dei diritti degli utenti rispetto agli stessi sono stati profondamente impattati dal Regolamento 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE, c.d. "Digital Services Act" (di seguito, anche "DSA"). Tale Regolamento, entrato in vigore il 17 febbraio 2024, è parte di un "pacchetto" di due atti legislativi dell'Unione europea, che comprende anche il Regolamento (UE) 2022/1925, cd. "Regolamento sui mercati digitali" o, in inglese, Digital Markets Act (di seguito, anche "DMA")¹⁰¹.

¹⁰¹ Cfr. sul tema O. Pollicino, *Regolazione e innovazione tecnologica nell'«ordinamento della rete»*, cit., 154. L'A. si sofferma sull'obiettivo del "pacchetto": riformare nel suo complesso il mercato digitale, combinando insieme, da un lato, novità concernenti gli obblighi dei provider alla

Come anticipato, del resto, ormai, in tema di regolamentazione delle tecnologie, non si può prescindere dall'analisi di quanto stabilito a livello eurounitario.

L'intervento del legislatore europeo trova giustificazione nell'assunzione, da parte dei servizi della società dell'informazione – in particolare dei servizi di intermediazione – di un ruolo strutturale sia nell'economia dell'Unione, sia nella quotidianità dei suoi cittadini. A distanza di vent'anni dall'adozione del quadro normativo vigente, delineato dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio, l'evoluzione tecnologica e l'affermazione di nuovi modelli di *business* e di servizi innovativi – quali le reti sociali (*social network*) e le piattaforme *online* che consentono ai consumatori di concludere contratti a distanza con operatori commerciali – hanno ampliato le possibilità, per utenti professionali e consumatori, di accedere alle informazioni, diffonderle e porre in essere transazioni attraverso modalità radicalmente nuove. La trasformazione digitale e il maggiore utilizzo di tali servizi hanno tuttavia anche dato origine a nuovi rischi e sfide per i singoli destinatari dei vari servizi, per le imprese e per la società nel suo insieme¹⁰². Di conseguenza, rispetto all'ambito di applicazione, il Digital Services Act riguarda un'ampia gamma di servizi digitali che fungono da intermediari tra utenti e contenuti, beni o servizi.

Il Digital Services Act si pone in continuità con quanto stabilito dalla Direttiva 2000/31/CE ma introduce diversi elementi di novità¹⁰³.

Certamente, a differenza del passato, il DSA avvia una nuova fase di regolamentazione di natura pubblicistica, che coinvolge gli Internet Service Provider, in un contesto in cui tale impostazione è stata a lungo considerata complessa, se non addirittura inappropriata. Con il DSA, invece, si è finalmente giunti a stabilire regole per le attività degli operatori digitali online, ponendo al centro non soltanto la tutela dei diritti individuali, ma anche di quelli collettivi¹⁰⁴.

tutela di un ambiente digitale trasparente e sicuro e, dall'altro lato, nuove regole relative alla promozione della concorrenza.

¹⁰² Cfr. considerando n. 1 del *Digital Services Act*. Sull'evoluzione normativa dalla direttiva n. 2000/31/CE al *Digital Services Act* cfr. S. Tommasi, *Digital Services Act e responsabilità dei provider*, in E. Battelli (a cura di), *Diritto privato digitale*, cit., 144. L'Autrice rileva che, a distanza di più di venti anni dall'adozione della direttiva, risulta completamente cambiato il contesto di riferimento. In particolare, all'epoca della direttiva, si trattava di promuovere questa tipologia di servizi e non c'era un uso così diffuso di sistemi di intelligenza artificiale. Inoltre, allo stato attuale, la questione principale sul tema è diventata quella di fronteggiare l'enorme potere in mano agli intermediari di servizi digitali e ridurre i rischi di effetti negativi sui valori democratici e i diritti fondamentali.

¹⁰³ S. Tommasi, *The Liability of Internet Service Providers in the Proposed Digital Services Act*, in *European Review of Private Law*, 2022, 925 ss. Secondo O. Pollicino, *Regolazione e innovazione tecnologica nell'«ordinamento della rete»*, cit., 153, nel contesto europeo, alcune delle garanzie procedurali prima evocate sotto il profilo teorico, sono state "codificate" con l'adozione del *Digital Services Act*.

¹⁰⁴ Sulla svolta pubblicistica della regolazione realizzata dal *Digital Services Act* cfr. M. Orofino, *Il DSA tra continuità (solo apparente) ed innovazione*, in F. Pizzetti, S. Calzolaio, A.

Può essere utile premettere che il Regolamento adotta un'architettura normativa ispirata al principio del *risk-based approach*, articolando il quadro degli obblighi secondo il criterio della proporzionalità in relazione alla natura, alla dimensione e all'impatto dei servizi digitali.

Tale impostazione si traduce in un sistema progressivo, in cui la misura e la complessità delle prescrizioni aumentano al crescere della capacità del prestatore di incidere su diritti fondamentali, ordine pubblico, processi democratici e sicurezza dei mercati digitali.

In questo senso, il Regolamento classifica le piattaforme digitali in quattro categorie principali, ognuna delle quali è soggetta a specifici obblighi di conformità: gli Intermediary Services, gli Hosting Services, le Online Platforms, e le Very Large Online Platforms (VLOP) e i Very Large Online Search Engines (VLOSE).

La disciplina generale, applicabile a tutti i prestatori di servizi di intermediazione (mere conduit, caching, hosting), si limita a stabilire obblighi orizzontali di trasparenza, di cooperazione con le autorità e di gestione delle segnalazioni di contenuti illeciti, preservando il regime di responsabilità limitata di cui agli artt. 4-6 DSA.

Un livello più intenso di regolazione è previsto per le piattaforme online in senso proprio, che assumono un ruolo attivo nella messa in contatto tra utenti e nella diffusione di contenuti, beni o servizi. Per tali operatori, il Regolamento introduce meccanismi di *notice and action*, obblighi di tracciabilità dei destinatari commerciali, sistemi di reclamo interni e limiti alla profilazione pubblicitaria nei confronti dei minori.

La regolazione più stringente, però, è prevista per le piattaforme online di grandissime dimensioni (Very Large Online Platforms, VLOP) e per i motori di ricerca online di grandissime dimensioni (Very Large Online Search Engines, VLOSE), definiti come servizi che raggiungono almeno 45 milioni di destinatari attivi mensili nell'Unione (pari a circa il 10% della popolazione UE)¹⁰⁵. Per tali soggetti, il Legislatore europeo presume l'esistenza di rischi sistemici derivanti dalla scala e dalla pervasività del servizio¹⁰⁶.

In relazione a tali rischi, il Regolamento impone obblighi specifici e di natura rafforzata, tra cui: valutazioni annuali per individuare, analizzare e valutare i rischi connessi alla diffusione di contenuti illegali, alla limitazione o distorsione

Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea della società digitale*, cit., 144 ss.

¹⁰⁵ Cfr. art. 33, DSA.

¹⁰⁶ Del resto, come rilevato dalla dottrina, scopo ultimo era (ed è) quello di «addomesticare» i giganti del mercato digitale. Sul punto cfr. G. Wagner et al., *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, 987 ss.; O. Pollicino, *Regolazione e innovazione tecnologica nell'«ordinamento della rete»*, cit., 154.

dell'esercizio dei diritti fondamentali, alla manipolazione deliberata del servizio e agli effetti negativi sulla salute, sulla sicurezza pubblica e sui processi elettorali¹⁰⁷; adozione di misure di mitigazione proporzionate, calibrate sulla natura e gravità dei rischi individuati¹⁰⁸; sottoposizione ad audit indipendenti annuali per verificare la conformità agli obblighi di gestione del rischio¹⁰⁹; obblighi di trasparenza rafforzata, inclusa la pubblicazione di relazioni dettagliate, la comunicazione dei sistemi di raccomandazione e la possibilità per gli utenti di optare per sistemi non basati sulla profilazione¹¹⁰; messa a disposizione dei dati a ricercatori accreditati per finalità di studio sui rischi sistemici¹¹¹; designazione di un compliance officer interno¹¹².

La vigilanza su VLOP e VLOSE è attribuita in via esclusiva alla Commissione Europea¹¹³, la quale esercita poteri di indagine, ispezione e sanzione, comprese ammende fino al 6% del fatturato annuo mondiale in caso di violazione grave e persistente.

L'impostazione del Digital Services Act, pertanto, configura un modello di responsabilità graduata: la disciplina generale salvaguarda la libertà di impresa e la neutralità degli intermediari di dimensioni ridotte, mentre l'intervento regolatorio si intensifica nei confronti degli operatori in grado di generare effetti sistemici, assicurando così un equilibrio tra tutela dell'ecosistema digitale e oneri regolatori proporzionali¹¹⁴.

Con specifico riferimento alla tutela prevista per i minori, il Regolamento contiene diverse disposizioni di interesse ai fini della presente analisi.

Prendendo le mosse dai considerando, all'interno della definizione generale degli obblighi di diligenza (*due diligence obligations*), il Considerando 40 indica espressamente che il quadro armonizzato del DSA mira a tutelare “*la sicurezza e la fiducia di tutti gli utenti, compresi i consumatori, i minori e gli utenti particolarmente vulnerabili*”. Tale menzione colloca la protezione dei minori tra gli obiettivi trasversali di tutte le misure previste dal Regolamento.

L'attenzione per la particolare categoria di utenti di minore età deve responsabilizzare i prestatori di servizi intermediari fin dalla progettazione del servizio attraverso una impostazione delle condizioni generali di funzionamento immediatamente chiara e facilmente intellegibile. Un obbligo che diventa assolutamente più stringente qualora si tratti specificamente di servizi destinati o

¹⁰⁷ Cfr. art. 34, DSA.

¹⁰⁸ Cfr. art. 35, DSA.

¹⁰⁹ Cfr. art. 37, DSA.

¹¹⁰ Cfr. artt. 27 e 38, DSA.

¹¹¹ Cfr. art. 40, DSA.

¹¹² Cfr. art. 4, DSA.

¹¹³ Cfr. artt. 56 ss., DSA.

¹¹⁴ Cfr. S. Tommasi, *Digital Services Act e responsabilità dei provider*, in E. Battelli (a cura di), *Diritto privato digitale*, cit., 156-158.

utilizzati prevalentemente da minori¹¹⁵ per cui i rischi associati alla diffusione di contenuti illegali da valutare sono significativi e sistemici¹¹⁶: la fruizione del servizio potrebbe esporli a contenuti nocivi per la salute, lo sviluppo fisico, mentale, morale magari attraverso infrastrutture tecnologiche che sfruttino “*intenzionalmente o involontariamente le debolezze e l’inesperienza dei minori*”,¹¹⁷ causando finanche comportamenti di dipendenza.

Il Considerando 71 è il passaggio più ampio e diretto sulla protezione dei minori.

Infatti, lo stesso: definisce quando un servizio è “accessibile ai minori” (quando i termini d’uso lo consentono, è diretto a minori o il prestatore è ragionevolmente consapevole della loro presenza); stabilisce che i prestatori di piattaforme accessibili ai minori “dovrebbero adottare misure appropriate e proporzionate” per garantire privacy, sicurezza e protezione, con particolare riguardo alla progettazione delle interfacce (*safety by design*); indica che le piattaforme possono aderire a codici di condotta specifici o altre forme di autoregolamentazione in materia di tutela dei minori.

Il Considerando 88¹¹⁸, poi, è inserito nella parte dedicata alla valutazione e mitigazione dei rischi sistemici (artt. 34 e 35 DSA) e prevede che la protezione dei minori sia una componente specifica dell’analisi del rischio per le piattaforme di grandissime dimensioni (VLOP) e i motori di ricerca di grandissime dimensioni (VLOSE).

Prevede altresì che le misure di mitigazione possano includere: miglioramenti dei sistemi di raccomandazione per evitare effetti “rabbit hole”; rafforzamento dei sistemi di verifica dell’età; impostazioni predefinite sicure per minori; strumenti di segnalazione e intervento mirati.

Inoltre, il fornitore deve garantire che l’accesso del minore al servizio sia “condizionato” nei contenuti nocivi e organizzato in modo da consentirgli l’effettiva fruizione, ove eventualmente necessaria, di tutti i meccanismi di segnalazione, azione e reclamo previsti dal regolamento¹¹⁹.

L’art. 28, rubricato “Protezione online dei minori”, prescrive che, anche se i fornitori di piattaforme online non sono obbligati a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minore, se sono consapevoli, con ragionevole certezza che il destinatario del servizio è minore, devono adottare 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

¹¹⁵ Cfr. considerando 46 e 89.

¹¹⁶ Cfr. considerando 80 e 104.

¹¹⁷ Cfr. considerando 81.

¹¹⁸ Questo considerando estende la tutela dei minori oltre l’art. 28 DSA, collegandola anche alla governance del rischio sistemico.

¹¹⁹ Cfr. considerando 89.

meccanismi di verifica dell'età. Sono tenuti altresì, in quel caso, a fare in modo che non siano presentate sulla loro interfaccia pubblicità basate sulla profilazione¹²⁰.

Di particolare rilievo è il paragrafo 4 dell'art. 28, che prevede la Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1. Tali orientamenti, che saranno approfonditi nel prosieguo, sono stati pubblicati dalla Commissione il 14 luglio 2025.

Ai sensi dell'art. 34 DSA, la valutazione dei rischi sistemici deve includere, tra gli altri, i rischi per la protezione dei minori, anche quando derivano dall'esposizione a contenuti legali ma nocivi, da interazioni indesiderate o da design persuasivi dannosi per la salute psicofisica.

Inoltre, come anticipato, ai sensi dell'art. 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*”¹²¹.

Dall'interpretazione sistematica delle disposizioni appena menzionate¹²² e considerato quanto già previsto dal GDPR sul tema, si evince, dunque, che la normativa sovranazionale richiama l'esigenza di meccanismi di verifica dell'età, 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.

In altre parole, si può dire che è di origine europea la normativa dalla quale promana una regolazione fortemente pervasiva sul tema¹²³.

¹²⁰ L. Gatt, I.A. Caggiano, *Consumers and digital environments as a structural vulnerability relationship*, in *European Journal of Privacy Law and Technologies*, 2023, 9 ss.; S. Tommasi, *Digital Services Act e responsabilità dei provider*, cit., 156.

¹²¹ Come rilevato da autorevole dottrina questa disposizione “è centrale nel processo di costituzionalizzazione del potere esercitato dai giganti digitali, adeguando il loro impatto alla tutela dei valori democratici e dello Stato di diritto nell'ecosistema algoritmico”. Così O. Pollicino, *Regolazione e innovazione tecnologica nell'«ordinamento della rete»*, cit., 155.

¹²² Da un'analisi sistematica emerge come il DSA tratti i minori non come un tema settoriale isolato, ma come un filo conduttore trasversale che incide su più livelli: principi generali (considerando 40), obblighi specifici per piattaforme accessibili ai minori (art. 28 e considerando 71), e misure di governance del rischio per operatori di scala sistemica (considerando 88, artt. 34-35).

¹²³ Il Parlamento europeo ha più volte chiesto migliori sistemi di verifica dell'età per proteggere i bambini online, ad esempio nella sua relazione d'iniziativa sulla protezione dei consumatori nei videogiochi online adottata nel gennaio 2023 e nella risoluzione di marzo 2021 sui diritti dei bambini alla luce della strategia dell'UE sui diritti dell'infanzia. Allo stesso modo, migliori sistemi di verifica dell'età per proteggere i minori online fanno parte della proposta della Commissione europea di dichiarazione europea sui diritti e i principi digitali per il decennio digitale e della Dichiarazione dell'OCSE per un futuro digitale affidabile, sostenibile e inclusivo. Cfr. anche *Report age verification online, rischi e strumenti di tutela dei diritti dei minori* del Centro di ricerca

5.2. L'attuazione dell'art. 28, par. 4, DSA: le linee guida e il prototipo per la verifica dell'età della Commissione europea.

Il 14 luglio 2025 in bozza e il 10 ottobre in versione definitiva, sono stati pubblicati gli orientamenti della Commissione ai sensi dell'art. 28, paragrafo 4 DSA appena citati¹²⁴. Tali orientamenti dovrebbero assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1 dell'art. 28 DSA; quindi, nell'adottare misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio.

In ordine al valore del documento, la Commissione ha dichiarato che utilizzerà tali orientamenti per valutare la conformità all'art. 28, paragrafo 1 DSA. Essi, dunque, fungeranno da punto di riferimento per verificare se le piattaforme online che consentono ai minori di utilizzarle soddisfano le norme necessarie e possono informare le autorità nazionali di regolamentazione nelle loro azioni di esecuzione. Tuttavia, seguire tali Linee guida è volontario e non garantisce automaticamente la conformità.

In generale, le Linee guida danno diverse indicazioni utili che si applicheranno a tutte le piattaforme online accessibili ai minori, ad eccezione delle microimprese e delle piccole imprese.

Ai fini della presente trattazione, risulta di particolare interesse la sezione 6 dedicata al tema del "Service design" e, in particolare, il paragrafo 6.1. sul tema dell'"Age assurance".

La Commissione parte dal presupposto che le misure che limitano l'accesso in base all'età siano un mezzo efficace per garantire un elevato livello di privacy, sicurezza e protezione dei minori sulle piattaforme online e che, in questo senso, gli strumenti di verifica dell'età possono aiutare i fornitori ad applicare restrizioni di accesso agli utenti al di sotto di una certa età, al fine di proteggere i minori dall'accesso a contenuti online non adatti alla loro età, come il gioco d'azzardo o la pornografia, o dall'esposizione ad altri rischi come l'adescamento. Il presupposto di fondo è anche che tali misure possano disincentivare l'accesso di adulti a piattaforme pensate per i minori e a meglio progettare quei servizi pensati proprio per i minori.

Come noto e come ribadito nell'ambito delle Linee guida, esistono principalmente tre tipologie di strumenti di "Age assurance"¹²⁵: si tratta di sistemi

interdipartimentale Europeo di Studi Avanzati sull'Innovazione Digitale (Research Center IDEAS – Innovation Digital European Advanced Studies) del 24 giugno 2025, 9 ss.

¹²⁴ Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to article 28(4) of regulation 2022/2065/UE.

¹²⁵ I metodi di verifica dell'età utilizzati per determinare l'età di un utente.

di “self-declaration”¹²⁶, “age estimation”¹²⁷ e “age verification”¹²⁸. La principale differenza tra i vari sistemi risiede nel livello di accuratezza, che nei sistemi di age verification è alto, mentre nei sistemi di age estimation più basso, trattandosi, più che altro, di un’approssimazione.

Le Linee guida della Commissione seguono il medesimo approccio basato sul rischio e sul principio di proporzionalità a cui è ispirato il Digital Services Act. Di conseguenza, precisano che prima di decidere se applicare restrizioni di accesso basate sull’età, supportate da metodi di age assurance, i fornitori di piattaforme online accessibili ai minori dovrebbero sempre effettuare una valutazione (*assessment*)¹²⁹ per determinare se tale misura sia appropriata per garantire un elevato livello di privacy, sicurezza e protezione dei minori sul loro servizio e se sia proporzionata, o se tale elevato livello possa essere raggiunto già ricorrendo ad altre misure meno invasive. La valutazione che comporta la decisione di implementare strumenti di age assurance e l’adeguatezza e l’efficacia delle misure stesse deve essere motivata e supportata, nonché adeguatamente pubblicizzata. Tale ragionamento, peraltro, potrebbe essere svolto anche con riferimento a specifiche sezioni, funzioni o contenuti della piattaforma, evitando, se si può, di sottoporre a una misura restrittiva l’intero sistema.

Dopo aver effettuato questo tipo di analisi, i soggetti obbligati devono farne una ulteriore. Nel caso in cui occorra verificare l’età dell’utente, si tratta di capire, infatti, quale tra i metodi citati sia necessario e proporzionato rispetto al contesto e al raggiungimento dello scopo.

Ebbene, in alcune circostanze è la stessa Commissione a determinare a priori che l’uso di restrizioni di accesso supportate da metodi di verifica dell’età è una misura adeguata e proporzionata per garantire un elevato livello di privacy, sicurezza e protezione dei minori. In particolare: “*a. Quando determinati prodotti*

¹²⁶ Consists of methods that rely on the individual to supply their age or confirm their age range, either by voluntarily providing their date of birth or age, or by declaring themselves to be above a certain age, typically by clicking on a button online.

¹²⁷ Consists of methods which allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, or to be over or under a certain age.

¹²⁸ Is a system that relies on physical identifiers or verified sources of identification that provide a high degree of certainty in determining the age of a user.

¹²⁹ A parere della Commissione, tale valutazione dovrebbe garantire che qualsiasi restrizione all’esercizio dei diritti e delle libertà fondamentali dei destinatari, in particolare dei minori, sia proporzionata. Di conseguenza, la Commissione ritiene che i fornitori di piattaforme online dovrebbero rendere pubblico il risultato di tale valutazione sull’interfaccia online del proprio servizio, sia nel caso in cui la valutazione concluda che non è necessaria alcuna restrizione di accesso basata sulla verifica dell’età, sia nel caso in cui tale restrizione sia considerata una misura adeguata e proporzionata.

Con riferimento alle modalità per condurre tale valutazione, prima di valutare l’opportunità di adottare un metodo specifico di verifica o stima dell’età a supporto delle restrizioni di accesso, i fornitori di piattaforme online accessibili ai minori dovrebbero considerare le seguenti caratteristiche di tale metodo: a) accuratezza, b) affidabilità, c) robustezza, d) non intrusività, e) non discriminazione. Se rispettano tali caratteristiche, il metodo scelto può dirsi appropriato e proporzionato.

o servizi comportano un rischio elevato per i minori e tali rischi non possono essere mitigati con misure meno restrittive, tenendo conto delle leggi applicabili dell'Unione e nazionali, ad esempio: i. la vendita di alcolici, tabacco o prodotti correlati alla nicotina, droghe; ii. l'accesso a qualsiasi tipo di contenuto pornografico; iii. l'accesso a contenuti relativi al gioco d'azzardo; b. Laddove, a causa di rischi identificati per i minori, i termini e le condizioni o qualsiasi altro obbligo contrattuale del servizio richiedano che un utente abbia almeno 18 anni per accedere al servizio, anche se non esiste un requisito di età formale stabilito dalla legge; c. Qualsiasi altra circostanza in cui il fornitore di una piattaforma online accessibile ai minori abbia individuato rischi per la privacy, la sicurezza o l'incolumità dei minori, compresi i rischi relativi ai contenuti, alla condotta e ai consumatori, nonché i rischi di contatto (ad esempio, derivanti da funzionalità quali chat dal vivo, condivisione di immagini/video, messaggistica anonima), laddove tali rischi non possano essere mitigati da altre misure meno invasive in modo altrettanto efficace quanto le restrizioni di accesso supportate dalla verifica dell'età¹³⁰; d. Laddove il diritto dell'Unione o il diritto nazionale, in conformità con il diritto dell'Unione, prescriva un'età minima per accedere a determinati prodotti o servizi offerti e/o visualizzati in qualsiasi modo su una piattaforma online, comprese categorie specificamente definite di servizi di social media online”.

Le linee guida precisano che i metodi di stima dell'età possono integrare le tecnologie di verifica dell'età e possono essere utilizzati in aggiunta alle prime o come alternativa temporanea, in particolare nei casi in cui non siano ancora disponibili misure di verifica che rispettino i criteri di efficacia delle soluzioni di verifica dell'età.

Di particolare rilevanza ai fini della presente trattazione è il paragrafo 6.1.3.2 relativo alle “Age verification technologies”. Lungi dall'essere mere indicazioni tecniche, infatti, gli orientamenti della Commissione sul tema devono essere messi in relazione, come si proverà a fare nel prosieguo della presente analisi, con quanto al momento si sta definendo nella maggior parte dei paesi europei in tema di portafogli di identità digitale e anche con le indicazioni già rese a livello nazionale dall'AGCom in attuazione del c.d. “decreto Caivano”.

Ebbene, secondo le linee guida, le tecnologie di verifica dell'età devono configurarsi come un processo autonomo e distinto rispetto ad altre attività di trattamento dei dati personali, limitandosi a fornire esclusivamente la conferma del rispetto della soglia anagrafica richiesta. Tali metodologie devono presentare un livello di robustezza adeguato, idoneo a prevenire efficacemente la possibilità di elusione da parte di utenti minorenni, assicurando così l'effettiva tutela dell'accesso ai servizi.

¹³⁰ Tali rischi sono elencati in via esemplificativa all'interno dell'allegato alle linee guida cfr. 5C Typology of online risks to children.

In particolare, i meccanismi basati unicamente su autodichiarazioni (*self-declaration*) non sono considerati sufficientemente affidabili, in quanto facilmente aggirabili e pertanto incompatibili con i requisiti di efficacia e sicurezza richiesti.

Tra le soluzioni ritenute conformi vi sono quelle fondate sull'utilizzo di documenti di identità ufficiali, il cui impiego non comporta il trasferimento di ulteriori dati personali alle piattaforme, attraverso l'emissione di token anonimizzati da parte di soggetti terzi indipendenti rispetto ai gestori delle piattaforme medesime. L'applicazione di protocolli crittografici avanzati, quali le prove a conoscenza zero (*zero-knowledge proofs*), consente di attestare l'età dell'utente senza trasmettere ulteriori informazioni personali.

Le Linee guida ricordano sul punto che, nell'ambito del quadro normativo europeo, la Commissione sta promuovendo l'implementazione del Portafoglio di Identità Digitale dell'Unione europea¹³¹, che consentirà agli utenti di condividere in maniera selettiva e riservata esclusivamente l'informazione relativa al superamento di una determinata soglia anagrafica, garantendo contestualmente elevati standard di sicurezza e protezione dei dati personali. In via transitoria, fino alla piena operatività di tale strumento, la Commissione ha avviato sperimentazioni su una soluzione UE di verifica dell'età indipendente, destinata a costituire uno standard di riferimento per l'adozione di metodi conformi ai requisiti di efficacia, minimizzazione dei dati, non tracciabilità e interoperabilità sanciti dal regolamento.

Inoltre, le Linee guida raccomandano l'adozione di procedure di verifica dell'età basate su meccanismi "*double-blind*", volti a garantire che né il gestore della piattaforma né il fornitore della verifica possano acquisire simultaneamente informazioni riguardanti l'identità dell'utente e la natura del servizio fruito, assicurando così il rispetto dei principi di *privacy by design* e rafforzando la fiducia degli utenti nell'ecosistema digitale.

Preme precisare, infine, che, al di là di quanto previsto dalla normativa e dalle disposizioni attuative, la protezione dei minori è stata individuata come una delle aree prioritarie nell'ambito del Digital Services Act. Ciò è comprovato dalle indagini¹³² avviate dalla Commissione nei confronti di una serie di piattaforme pornografiche¹³³ per sospette violazioni del DSA in materia di protezione dei minori¹³⁴.

¹³¹ Per un approfondimento sul tema cfr. cap. II.

¹³² Cfr. ec.europa.eu/commission/presscorner/detail/en/ip_25_1339.

¹³³ Si tratta delle piattaforme Pornhub, Stripchat, XNXX e XVideos.

¹³⁴ Le indagini sono state avviate dopo che queste piattaforme erano state classificate come "grandi piattaforme digitali" ai sensi del DSA. I siti coinvolti hanno successivamente presentato ricorso e le cause sono attualmente tuttora in corso.

5.3. Il quadro normativo nazionale in tema di verifica dell'età. SPID per i minori: le Linee Guida dell'Agenzia per l'Italia digitale.

A livello nazionale, il tema dell'identità digitale del minore e della verifica dell'età è stato affrontato, oltre che nell'ambito della normativa in materia di protezione dei dati personali, anche dall'Agenzia per l'Italia digitale con riferimento all'identificazione dei minori utenti di servizi digitali.

Tale agenzia, ai sensi dell'art. 14-*bis* CAD, comma 2, lett. a), infatti, emana linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme del Codice dell'amministrazione digitale, 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 europea¹³⁵.

Nel contesto normativo appena descritto, il 3 marzo nel 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"¹³⁶. 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 SPID¹³⁷ devono attuare 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.

¹³⁵ Per un approfondimento sulla normativa in materia di trasformazione digitale e in particolare di identità digitale, nonché sul ruolo dell'Agenzia per l'Italia digitale cfr. cap. II.

¹³⁶ Cfr. testo integrale "*Linee guida operative per la fruizione dei servizi SPID da parte dei minori*".

¹³⁷ Per un approfondimento sul funzionamento dello SPID e sulla normativa di riferimento cfr. cap. II.

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 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 in oggetto 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 in materia 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 neomaggiorenne acquisisce il pieno controllo della propria identità digitale, con la possibilità di revocare o mantenere l'identità precedentemente rilasciata. In effetti, tale principio risulta 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, occorre svolgere alcune riflessioni sul documento in oggetto e sui limiti dello stesso.

La prima è che SPID per i minori si inserisce in 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 finanziati dal PNRR, puntava a diffondere l'identità digitale presso fasce sempre più ampie della popolazione.

Come approfondito nell'ambito del capitolo II, inoltre, tale strumento, nonostante gli investimenti effettuati anche ad opera del Piano Nazionale di Ripresa e Resilienza italiano (PNRR), presenta ancora diversi limiti. Sebbene, come esposto, 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"¹³⁸. È proprio, però, con riferimento ai servizi privati, soprattutto i *social network*, che si avverte da anni l'esigenza di regolarne l'accesso.

Si aggiunge, infine, che, dal punto di vista tecnico – come emerge dai principi sottesi alle linee guida – la soluzione non garantisce un livello di anonimizzazione reciproca tra le parti paragonabile a quello auspicato dall'EDPB in materia di protezione dei dati dei minori e richiamato, in termini generali, nelle linee guida adottate dalla Commissione europea ai sensi dell'art. 28 DSA, nonché imposto come si vedrà, dall'AGCOM.

Al contrario, l'impostazione delle Linee guida SPID minori, adottate dall'AgID nel 2022, prevede che il genitore, ricevuta la notifica, possa valutare l'opportunità di consentire al minore, su cui esercita la responsabilità genitoriale, l'accesso a uno specifico servizio.

5.4. L'impatto del "Decreto Caivano".

Come evidenziato, la normativa sovranazionale richiama l'esigenza di meccanismi di *age assurance*, 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 d.l. 15 settembre 2023, n. 123, convertito con mod.

¹³⁸ Per un approfondimento cfr. E. Belisario, S. Pagnotta, F. Ricciulli, *Amministrazione digitale: guida ragionata agli "switch off"*, Santarcangelo di Romagna, 2021.

dalla l. n. 159 del 2023, recante “Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale”¹³⁹.

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 diciotto¹⁴⁰.

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’Italia¹⁴¹.

In ragione di ciò, l’AGCOM è stata incaricata ai sensi del comma 3 della medesima disposizione, di stabilire con proprio provvedimento, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del “Decreto Caivano”, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i gestori di siti web e i fornitori delle piattaforme di condivisione video a carattere pornografico 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.

Sempre l’art. 13-*bis* prescrive che entro sei mesi dalla data di pubblicazione del provvedimento dell’AGCom, i soggetti obbligati devono dotarsi di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni impartite nel già menzionato provvedimento.

¹³⁹ 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*”.

¹⁴⁰ La disposizione è stata introdotta in sede di conversione in legge del “decreto Caivano”, tramite emendamento parlamentare 13.0.1 firmato anche da esponenti politici di gruppi di maggioranza e minoranza.

¹⁴¹ Cfr. art. 15 d.l. 15 settembre 2023, n. 123, convertito con modificazioni dalla l. 13 novembre 2023, n. 159, rubricato “*Designazione del coordinatore dei servizi digitali in attuazione del Regolamento (UE) 2022/2065 sui servizi digitali*”.

Quanto al monitoraggio del rispetto degli obblighi, l'Autorità per le garanzie nelle comunicazioni vigila sulla corretta applicazione e, in caso di inadempimento, può contestare, anche d'ufficio, la violazione¹⁴².

Sul piano normativo, vale la pena menzionare le rilevanti modifiche apportate negli ultimi anni al TUSMA.

In particolare, il summenzionato decreto legislativo 8 novembre 2021, n. 208, così come modificato dal decreto legislativo del 25 marzo 2024, n. 50, ha introdotto, all'art. 3, comma 1, lett. c) nell'ordinamento italiano la definizione di servizio di piattaforma per la condivisione di video quale *“un servizio, quale definito dagli articoli 56 e 57 del Trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso, di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi o video generati dagli utenti destinati al grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento”*.

Lo stesso testo normativo ha il merito, inoltre, di dedicare, nella sua attuale formulazione, due specifiche norme alla disciplina dei servizi di piattaforma per la condivisione di video: si tratta degli artt. 41 e 42.

In particolare, l'art. 41 del TUSMA, fornisce i criteri per identificare i fornitori di detti servizi stabiliti o che si considerano stabiliti in Italia. Inoltre, detta previsione ha introdotto nell'ordinamento italiano, una specifica disciplina rivolta ai fornitori di tali servizi stabiliti in un altro Stato membro i cui contenuti ivi diffusi sono rivolti al pubblico italiano. Al riguardo al comma 7 dell'art. 41 stabilisce che: fatti salvi gli artt. da 14 a 17 del d.lgs. 9 aprile 2003, n. 70, e fermo quanto previsto ai commi precedenti, la libera circolazione di programmi, video generati dagli utenti e comunicazioni commerciali audiovisive veicolati da una piattaforma per la condivisione di video il cui fornitore è stabilito in un altro Stato membro e diretti al pubblico italiano può essere limitata, con provvedimento dell'Autorità, secondo la procedura di cui all'art. 5, commi 2, 3 e 4 del d.lgs. n. 70 del 2003, per i seguenti fini: a) la tutela dei minori da contenuti che possono nuocere al loro sviluppo fisico, psichico o morale a norma dell'art. 38, comma 1.

¹⁴² Come previsto dall'art. 13-*bis* del decreto n. 123 del 2023, in caso di contestazione di violazione, l'AGCom applica le disposizioni di cui all'art. 1, comma 31, del d.lgs. 31 luglio 1997, n. 249 e può diffidare i soggetti obbligati ad adeguarsi entro venti giorni. In caso di inottemperanza alla diffida, l'AGCom adotta ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino, da parte dei soggetti intimati, di condizioni di fornitura conformi ai contenuti della diffida dell'Autorità.

Ai sensi dell'art. 42, commi 1 e 6, dello stesso TUSMA, inoltre, è previsto che *“1. Fatti salvi gli articoli da 14 a 17 del decreto legislativo 9 aprile 2003, n. 70, i fornitori di piattaforme per la condivisione di video soggetti alla giurisdizione italiana devono adottare misure adeguate a tutelare: a) i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale a norma dell'articolo 38, comma 3; 6. Ai fini della tutela dei minori di cui al comma 1, lettera a), i contenuti maggiormente nocivi sono soggetti alle più rigorose misure di controllo dell'accesso”*.

L'art. 42, invece, disciplina le nuove regole da applicare ai fornitori di servizi di piattaforma per la condivisione di video stabiliti o che si considerano in Italia.

Con specifico riferimento agli strumenti di verifica dell'età, al comma 7 dell'art. 42 del TUSMA, è previsto che: *“7. I fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a: [omissis] f) predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori; [omissis] h) dotarsi di sistemi di controllo parentale sotto la vigilanza dell'utente finale per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori”*.

5.5. I principi affermati dal Regolamento AGCOM in tema di verifica dell'età.

L'AGCOM è da ultimo intervenuta sul tema con la delibera n. 96/25/CONS dell'8 aprile 2025 in attuazione delle disposizioni dell'art. 13-bis del decreto-legge 15 settembre n. 123 convertito con modificazioni dalla Legge 13 novembre 2023, n. 159.

In particolare, come previsto dalla disposizione citata, l'AGCOM ha individuato, a seguito di una consultazione pubblica e del parere favorevole dell'Autorità garante per la protezione dei dati personali, nonché sentita la Commissione europea, le misure tecniche e di processo che siti e piattaforme, che diffondono contenuti pornografici, devono implementare per autorizzare l'accesso ai propri servizi ai soli utenti maggiorenni¹⁴³.

Di estrema rilevanza, ai fini della presente trattazione, sono le seguenti circostanze.

¹⁴³Cfr. allegato A alla delibera n. 96/25/CONS recante modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai fini dell'accesso a determinati servizi forniti dai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, ai sensi dell'art. 13-bis, d.l. n. 123/2023.

La prima è la cedevolezza del Regolamento in oggetto rispetto alle Linee guida adottate dalla Commissione europea. Nelle versione finale del Regolamento, a valle delle osservazioni della Commissione europea, infatti, è stata inserita la previsione di un meccanismo espresso per modificare, revocare o abrogare, laddove necessario, le misure adottate a livello nazionale con riferimento ai soggetti stabiliti in altri Stati membri, a decorrere dalla data di entrata in vigore degli orientamenti adottati ai sensi dell'art. 28 del Regolamento (UE) 2022/2065, al fine di adeguarsi alla normativa europea sopravvenuta¹⁴⁴.

Ciò sarà certamente necessario alla luce delle incongruenze che si registrano tra i due documenti.

Del resto, la fretta dell'Autorità nazionale, dovuta ai tempi stretti previsti dal "Decreto Caivano", la ha costretta ad approvare regole tecniche in assenza di quelle che la Commissione avrebbe dovuto approvare ai sensi dell'art. 28, comma 4 DSA (che, come esposto, sono state pubblicate in versione definitiva solo il 10 ottobre 2025). Ciò ha portato ad un evidente cortocircuito, che dovrà essere ben presto sanato alla luce della già menzionata cedevolezza della normativa nazionale rispetto a quella sovranazionale e per evitare effetti negativi sulla concorrenza.

Si registra, infatti, un rilevante disallineamento su ambito di applicazione, natura giuridica, e requisiti tecnici specifici per l'accertamento dell'età.

Entrambe le fonti mirano a proteggere i minori online e promuovono principi come la proporzionalità e la protezione dei dati, il provvedimento AGCOM è una normativa più specifica e dettagliata, con requisiti più stringenti sull'anonimato e la frequenza della verifica per i contenuti pornografici. Le linee guida della Commissione, invece, offrono un quadro più ampio e flessibile per tutte le piattaforme online, incoraggiando l'innovazione tecnologica che rispetti rigorosi standard di privacy.

Più in particolare si evidenziano di seguito le questioni più rilevanti a parere della scrivente:

- **Ambito di applicazione:** il "Decreto Caivano", influenzando così il Regolamento emanato in attuazione dello stesso, si preoccupa esclusivamente dei contenuti pornografici mentre le Linee guida della Commissione si riferiscono ad un più ampio spettro di contenuti. Sul punto preme comunque rilevare che AGCOM si era già premurata, per quanto in via di suggerimento, di allargare il campo anche ad altri soggetti e altri contenuti nocivi per i minori anche oltre a quelli pornografici¹⁴⁵. Dunque, dal punto di vista soggettivo, il Regolamento si applica specificamente ai gestori di siti web e piattaforme di condivisione di video che diffondono in Italia

¹⁴⁴ Cfr. art. 4 su "Entrata in vigore e clausola di rivedibilità", nel quale, al comma 3, si legge che "A decorrere dalla data di entrata in vigore degli orientamenti adottati ai sensi dell'articolo 28 del Regolamento (UE) 2022/2065, l'Autorità, laddove necessario, si impegna a modificare ed adeguare il presente provvedimento alla normativa europea sopravvenuta con riferimento ai soggetti stabiliti in altri Stati membri".

¹⁴⁵ Il riferimento è, ad esempio, alle categorie previste dalla delibera 9/23/CONS dell'AGCom.

immagini e video a carattere pornografico¹⁴⁶ indipendentemente da dove sono stabiliti¹⁴⁷. Dal punto di vista dell'ambito oggettivo di applicazione, sebbene raccomandi l'applicazione delle stesse modalità anche ad altre tipologie di contenuti che potrebbero nuocere ai minori, il suo mandato diretto è circoscritto alla pornografia.

- **Natura giuridica e obbligatorietà:** il Regolamento AGCOM è un atto normativo specifico che stabilisce le “modalità tecniche e di processo” che devono essere adottate dai soggetti individuati. Rappresenta una “soluzione transitoria” che sarà rivista e aggiornata per assicurare la piena conformità con gli orientamenti della Commissione Europea. Le Linee Guida della Commissione Europea, dal canto loro, sono orientamenti che descrivono le misure che la Commissione “ritiene” che i fornitori debbano adottare per garantire un elevato livello di privacy, sicurezza e protezione dei minori. Sebbene costituiscano un “punto di riferimento significativo” per la Commissione nell'applicazione dell'art. 28 del Regolamento (UE) 2022/2065, l'adozione di tali misure “non comporta automaticamente la conformità”. In altre parole, apparentemente non hanno la stessa cogenza della regolamentazione nazionale. La relazione tra le due linee guida, tuttavia, viene risolta dalla clausola di cedevolezza inserita appositamente all'interno del Regolamento AGCOM.

- **Enfasi sul doppio anonimato:** il Regolamento AGCOM richiede in modo esplicito e stringente il “doppio anonimato”. Di conseguenza, il fornitore di contenuti pornografici non deve poter riconoscere un utente che ha già utilizzato il sistema di verifica dell'età. Inoltre, il fornitore della prova dell'età non deve sapere a quale servizio specifico l'utente sta cercando di accedere. Sulla scorta di tale indicazione, AGCOM arriva a criticare esplicitamente il sistema SPID per non essere pienamente conforme a tale requisito, in quanto, come anticipato¹⁴⁸, il gestore dell'identità (Identity Provider) potrebbe conoscere il nome del dominio del sito visitato. Il modello preferito da AGCOM prevede che la “prova dell'età” venga

¹⁴⁶ Detti soggetti sono individuati in una lista compilata e aggiornata dall'Autorità, nonché comunicata dalla stessa alla Commissione europea.

¹⁴⁷ Al fine di stabilire se un contenuto diffuso da un fornitore stabilito in un altro Stato membro sia diretto al pubblico italiano deve essere soddisfatto almeno uno dei seguenti criteri: a) l'utilizzo prevalente della lingua italiana all'interno del servizio online, da valutare in relazione alla presenza di elementi testuali realizzati in lingua italiana nell'interfaccia utente, nonché alla disponibilità della funzione multilingua che includa la lingua italiana; b) il raggiungimento da parte del servizio online di un significativo numero medio di utenti unici mensili sul territorio italiano sulla base dei dati forniti da organismi dotati della massima rappresentatività dell'intero settore di riferimento, anche alla luce dei processi di convergenza multimediale, la cui organizzazione risponda altresì a principi di terzietà, autonomia e indipendenza; c) il conseguimento da parte del fornitore del servizio di piattaforma per la condivisione di video di ricavi realizzati in Italia, anche se contabilizzati nei bilanci di società aventi sede all'estero Tali servizi sono individuati in un elenco/lista compilata e aggiornata dall'Autorità che ne cura anche la comunicazione alla Commissione europea; d) il servizio è promosso o commercializzato anche per gli utenti italiani; e) il servizio ha un dominio in Italia o fornisce un indirizzo di contatto e/o un numero di telefono in Italia.

¹⁴⁸ Cfr. cap. II.

trasmessa solo all'utente, che poi la presenta al sito, garantendo che né il fornitore della prova né il sito conoscano l'identità completa dell'utente o il servizio specifico utilizzato. Le linee guida della Commissione europea, invece, come esposto, incoraggiano i “metodi di verifica dell'età a doppio cieco” (“*double-blind*”), che si allineano al concetto di doppio anonimato AGCom, assicurando che la piattaforma online non riceva identificativi utenti oltre all'età e che il fornitore della verifica dell'età non conosca il servizio utilizzato. Le linee guida menzionano protocolli crittografici come le “*zero-knowledge proofs*” come base adatta per la protezione della privacy. Sebbene il principio sia lo stesso, dunque, AGCom fornisce un'interpretazione più dettagliata e stringente sulla sua implementazione pratica, escludendo espressamente tecnologie e sistemi esistenti.

- **Frequenza della verifica dell'età (per contenuti pornografici):** secondo il Regolamento AGCOM, per l'accesso a contenuti pornografici, la verifica deve avvenire a ogni consultazione del sito o della piattaforma. È richiesta una nuova verifica se la sessione viene interrotta, il browser viene chiuso, il sistema operativo va in stand-by o dopo 45 minuti di inattività effettiva (per dispositivi condivisi). Questa è una regola molto specifica e frequente. Le linee guida della Commissione europea raccomandano che la verifica dell'età venga effettuata “dove possibile al momento della creazione dell'account” per contribuire a un'esperienza appropriata all'età. Non specificano una frequenza così alta (“a ogni consultazione” o “ogni 45 minuti”) per tutte le tipologie di contenuto ad alto rischio, sebbene indichino che le piattaforme con contenuti per adulti non dovrebbero consentire la condivisione delle credenziali e dovrebbero condurre la verifica “ad ogni istanza” di accesso, il che si avvicina alla posizione AGCom per quel tipo di servizio.

- **Proibizioni esplicite di metodi di trattamento dati:** il Regolamento AGCOM elenca esplicitamente sistemi non conformi per motivi di privacy: la raccolta diretta di documenti d'identità da parte del gestore del sito pornografico, la stima dell'età basata sulla cronologia di navigazione e il trattamento di dati biometrici (es. riconoscimento facciale per confronto con foto ID/selfie) ai fini di identificazione/autenticazione. Le linee guida della Commissione europea, pur promuovendo la minimizzazione dei dati e scoraggiando la profilazione, non stabiliscono proibizioni così esplicite per tutte le tecnologie citate. Menzionano il riconoscimento facciale come metodo di stima dell'età e l'uso di tecnologie biometriche come “rischi”, ma l'approccio generale è quello di valutare se tali tecnologie, se usate con protocolli di privacy avanzati come token anonimi o zero-knowledge proofs, possano soddisfare i criteri di non intrusività e minimizzazione dei dati. Le linee guida sembrano più aperte all'evoluzione tecnologica, purché siano rispettati rigorosi principi di protezione della privacy.

- **Riferimento a strumenti futuri (EU Digital Identity Wallet):** il Regolamento AGCOM menziona l'utilità del futuro EU Digital Identity Wallet come soluzione promettente per la verifica dell'età, ma si concentra principalmente sulla definizione dei requisiti per le soluzioni *attuali* e *transitorie*. Le Linee Guida

Commissione Europea promuovono attivamente l'EU Digital Identity Wallet e la propria soluzione europea di verifica dell'età in fase di test come lo standard ideale per una verifica dell'età interoperabile, privacy-preserving e data-minimizing, che facilita l'uso di "age tokens" riutilizzabili. La riusabilità della prova dell'età è un concetto centrale nel loro approccio.

Al momento in cui si scrive, il divieto di accesso dei minori a contenuti pornografici e l'obbligo per i gestori dei siti web di verifica dell'età degli utenti è entrato in vigore, in linea teorica, dal 12 novembre 2025 con effetto per i soli soggetti stabiliti in Italia¹⁴⁹.

Quanto ai soggetti non stabiliti in Italia, l'Allegato A alla Delibera AGCOM fissa una diversa scadenza: *“Le disposizioni del presente provvedimento si applicano altresì ai gestori di siti web e alle piattaforme di condivisione di video che diffondono in Italia immagini e video a contenuto pornografico, a prescindere dallo Stato membro di stabilimento, a decorrere tre mesi dalla pubblicazione della lista di cui all'articolo 1 del presente provvedimento”* (l'art. 1 definisce i criteri per l'individuazione dei siti a contenuto pornografico e l'ambito di applicazione delle modalità tecniche di accertamento dell'età). AGCOM ha reso pubblica tale lista dei 45 soggetti obbligati alla verifica dell'età soltanto il 31 ottobre¹⁵⁰; tuttavia, tutte le piattaforme che distribuiscono contenuti pornografici accessibili dall'Italia – comprese quelle non incluse nella lista – sono comunque tenute a conformarsi alle disposizioni normative. Pertanto, la data di pubblicazione della lista costituisce il riferimento per l'avvio del termine temporale, e l'entrata in vigore dell'obbligo di verifica non va più calcolata al 12 novembre 2025, ma al 1° febbraio 2026.

In definitiva, allo stato, i principali operatori del settore della pornografia online risultano, esonerati dall'obbligo, e l'AGCOM potrà procedere all'irrogazione delle eventuali sanzioni – previste, come si è visto, sino all'importo massimo di 250.000 euro – non prima del 1° febbraio 2026.

¹⁴⁹ La data del 12 novembre deriva dalla previsione del citato art. 4 dell'allegato A alla delibera AGCom 96/25 nel quale si fissa l'entrata in vigore dell'obbligo a 6 mesi decorrenti dalla pubblicazione del provvedimento AGCom (avvenuta il 12 maggio).

¹⁵⁰ In particolare, deve ricorrere il soddisfacimento di almeno uno dei seguenti criteri: a) l'utilizzo prevalente della lingua italiana all'interno del servizio online, da valutare in relazione alla presenza di elementi testuali realizzati in lingua italiana nell'interfaccia utente, nonché alla disponibilità della funzione multilingua che includa la lingua italiana; b) il raggiungimento da parte del servizio online di un significativo numero medio di utenti unici mensili sul territorio italiano sulla base dei dati forniti da organismi dotati della massima rappresentatività dell'intero settore di riferimento, anche alla luce dei processi di convergenza multimediale, la cui organizzazione risponda altresì a principi di terzietà, autonomia e indipendenza; c) il conseguimento da parte del fornitore del servizio di piattaforma per la condivisione di video di ricavi realizzati in Italia, anche se contabilizzati nei bilanci di società aventi sede all'estero; d) il servizio è promosso o commercializzato anche per gli utenti italiani; e) il servizio ha un dominio in Italia o fornisce un indirizzo di contatto e/o un numero di telefono in Italia.

5.6. Le più recenti novità della normativa italiana in materia di verifica dell'età.

Al momento in cui si scrive è altresì in fase di istruttoria presso la Commissione VIII del Senato il ddl 1136 del 2024 intitolato “*Disposizioni per la tutela dei minori nell’ambiente digitale*”. Per quanto ancora in fase embrionale, non ci si può esimere dall’analisi di tale disegno di legge poiché, se dovesse concludere l’iter legis, introdurrebbe rilevanti novità con riferimento a tutta la disciplina ricostruita nella presente trattazione. Peraltro, si nota già dal titolo una certa assonanza con il capo del “decreto Caivano” esaminato. La sovrapposizione risulta solo parziale perché il ddl aspira a regolare un più ampio raggio di fattispecie e tipologie di contenuti.

Il testo si compone di pochi articoli e si apre con la definizione dell’ambito di applicazione soggettivo. In particolare, le disposizioni dovrebbero applicarsi ai fornitori di servizi della società dell’informazione che offrono le loro prestazioni in Italia, “*indipendentemente dal luogo di stabilimento*”.

L’art. 2 è dedicato alla verifica dell’età dell’utente e fissa un generale obbligo per tutti i fornitori di servizi della società dell’informazione che offrono le loro prestazioni in Italia di verificare l’età degli utenti. Prevede, poi, che l’AGCOM, entro sessanta giorni dalla data di entrata in vigore della legge, deve definire le modalità tecniche e di processo che i soggetti obbligati devono adottare per accertare l’età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo.

Il comma 3 dell’art. 2 vuole chiarire a chi effettivamente, tra la moltitudine di fornitori di servizi dell’informazione, si applichi l’obbligo e precisa: “*Le disposizioni in materia di obbligo di verifica dell’età degli utenti di cui al comma 1 si applicano ai fornitori di servizi della società dell’informazione a condizione che registrino un numero di accessi unici mensili superiore a quello stabilito, con proprio provvedimento, dall’Autorità per le garanzie nelle comunicazioni entro sessanta giorni dalla data di entrata in vigore della presente legge*”.

L’art. 4 del ddl, poi, prevede l’abrogazione dell’art. 2-quinquies del Codice privacy sul quale ci si è soffermati *supra* con riferimento all’età fissata dalla normativa nazionale in materia di protezione dei dati personali per il consenso. L’idea del nuovo disegno di legge è portarla a quindici anni. Allo stesso tempo, infatti, l’art. 3 del ddl stabilisce la nullità dei contratti stipulati dai minori di quindici anni con i fornitori di servizi digitali. Tali contratti, se nulli, non possono costituire una base giuridica per il trattamento dei dati personali. Sono validi solo se conclusi per conto del minore da chi esercita la responsabilità genitoriale o dal tutore. I fornitori devono provare che i contratti siano stati stipulati da maggiorenni o da minori assistiti.

L’art. 5 disciplina la pubblicazione abituale dell’immagine di minorenni sotto i quindici anni sulle piattaforme digitali. La norma si applica quando il minore

è il protagonista dei contenuti e quando tali attività generano, o mirano a generare, guadagni diretti o indiretti superiori a 10.000 euro all'anno. In queste circostanze è necessario ottenere il consenso di chi detiene la responsabilità genitoriale e l'autorizzazione della Direzione provinciale del lavoro. Le somme che eccedono la soglia dei 10.000 euro devono essere depositate su un conto corrente intestato al minore e non possono essere utilizzate dai genitori, salvo situazioni eccezionali di necessità approvate dal Tribunale per i minorenni.

Infine, l'art. 6 impone ai provider di servizi digitali di integrare nelle proprie piattaforme e app un sistema che permetta ai minori di quindici anni di avviare rapidamente una chiamata o un messaggio verso il numero di emergenza per l'infanzia 114. Il funzionamento di questo servizio sarà sostenuto da un contributo economico pari allo 0,035% del fatturato annuale delle aziende che superano i cinquanta milioni di euro di ricavi.

6. Il fenomeno dello “sharenting” e dei cc.dd. “baby influencers”: identità personale e digitale eteroimposte e impatti sulla dignità del minore.

Analizzata la dimensione più estrinseca dell'identità, legata agli strumenti di identificazione del minore, spesso utilizzati per verificarne l'età, vale la pena soffermarsi su un profilo più strettamente connesso alla dimensione sostanziale, relativo al diritto di essere sé stessi e di essere correttamente rappresentati, anche nella dimensione digitale.

Con il termine “sharenting”¹⁵¹, che risulta utilizzato per la prima volta nel 2012 da Steven Leckhart, si indica il fenomeno della condivisione da parte dei genitori di contenuti riguardanti i propri figli (come, ad esempio, foto e video). Il neologismo unisce i termini “share” (condividere) e “parenting” (genitorialità)¹⁵². Si tratta di un fenomeno trasversale e interdisciplinare, che solleva, tra le altre, anche rilevanti questioni di natura antropologica, psicologica, sociologica, nonché pedagogica.

Partendo dall'analisi del fenomeno, le motivazioni sottese alla condivisione da parte dei genitori sembrano essere le più varie e talvolta possono anche sovrapporsi tra loro. Di solito si tratta della volontà del genitore di apparire, ricevere

¹⁵¹ Cfr, tra gli altri, B. Shmueli, A. Blecher-Prigat, *Privacy for Children*, in *Columbia Human Rights Law Review*, 2011, 759 ss.; A.H. Cooley, *Guarding Against a Radical Redefinition of Liability for Internet Misrepresentation: The United States v. Drew Prosecution and the Computer Fraud and Abuse Act*, in *Journal of Internet Law*, 2011, 23 ss.; A. McPeak, *Social Media Snooping and Its Ethical Bounds*, in *Arizona State Law Journal*, 2014, 1 ss.; S. Livingstone, J. Carr, J. Byrne, *One in Three: Internet Governance and Children's Rights*, in *Report Series*, 2015, 1 ss.; S.B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, in *Emory Law Journal*, 2017, 839 ss.; S. Donovan, *Sharenting: The Forgotten Children of the GDPR*, in *Peace Human Rights Governance*, Padova University Press, 2020, 35 ss.; M. Foglia, *Sharenting e riservatezza del minore in rete*, in *Actualidad Jurídica Iberoamericana*, 2022, 3552 ss.

¹⁵² S. Leckhart, *The Facebook-Free Baby Are you a mom or dad whos' guilty of 'oversharenting'? The cure may be ot not share at all*, in *The Wal Street Journal*, 2012, 1 ss.

apprezzamento, ottenere successo, profitto o maggiori interazioni, di costruire o consolidare un percorso professionale per sé o per il minore¹⁵³.

È proprio la finalità di profitto, a parere della maggior parte della dottrina, che caratterizza un ulteriore fenomeno diverso ma collegato a quello dello “sharenting”. Si tratta del fenomeno dei cc.dd. “baby influencers”, “kidfluencer” o “micro-microcelebrità”¹⁵⁴. Con tali termini ci si riferisce specificamente ai bambini che appaiono sui social media al fine di promuovere prodotti o servizi¹⁵⁵ per mezzo dei canali dei genitori o talvolta con autonomi profili social¹⁵⁶.

Può essere utile precisare con riferimento al tema dello “sharenting”, che, naturalmente, si fa riferimento all’attitudine “patologica” o, citando Guido Scorza, “ossessiva” dei genitori di condividere le foto dei propri figli¹⁵⁷, mentre resta fuori dal perimetro dell’analisi una condivisione equilibrata e oculata di contenuti relativi a minori. Come evidenziato da alcuni autori, la sovraesposizione dei minori sui *social media* da parte dei genitori evidenzia come questi ultimi, nel fare delle piattaforme digitali un elemento centrale della propria esperienza genitoriale, non siano sempre consapevoli delle conseguenze che tale condotta può avere sui figli¹⁵⁸.

Dal punto di vista giuridico, quale che sia la motivazione che spinge l’adulto a condividere contenuti online che ritraggono i minori, numerosissime sono le

¹⁵³ La finalità professionale porta alla nascita dell’ulteriore fenomeno dei cc.dd. “baby influencers” o “kidfluencer”. Con tali termini ci si riferisce specificamente ai bambini che appaiono sui social media al fine di promuovere prodotti o servizi. La proposta di legge n. 1800/2024 correttamente introduce una ulteriore distinzione tra due tipi di fenomeni: il primo consiste nell’introduzione dei minori nell’ambito della narrazione che il genitore fa di sé nel proprio profilo (account). In questo caso, i bambini servono a innescare sentimenti di vicinanza e identificazione con il pubblico, a rendere il profilo più autentico e a costruire un consenso basato sul coinvolgimento emotivo, perché le persone possono identificarsi con le esperienze genitoriali attraverso quei contenuti o provare tenerezza ed empatia nei confronti dei piccoli. Il secondo tipo di fenomeno riguarda, invece, i profili in cui i contenuti sono tutti incentrati sul minore, il quale inizia poi a collaborare con alcuni marchi commerciali (brand) per la pubblicazione di contenuti a pagamento.

¹⁵⁴ Cfr. C. Abidin, *Micromicrocelebrity: Branding babies on the Internet*, in *M/C Journal*, 2015, 1 ss.

¹⁵⁵ Come si rileva nella proposta di legge n. 1771/2024 sul tema, i fenomeni sono spesso attigui sicché risulta difficile stabilire quali siano i rispettivi confini. Si pensi, ad esempio, ai casi di esposizione mediatica di minori, figli di personaggi famosi e di cosiddetti «influencer», la cui esposizione mediatica è comunque funzionale al giro di affari del genitore.

¹⁵⁶ Sul punto risulta efficace il parallelismo di G. Scorza, E. Meligrana, *La privacy degli ultimi*, Catanzaro, 2022, 46, ove gli AA., muovendo dalla storia del noto Ryan Kaji, l’influencer di nove anni che nel 2020 è stato lo youtuber più pagato di sempre, rilevano che il minore è presente sulla piattaforma perché ospitato dai genitori e scrivono che “è un pò come se un adulto comprasse un pacchetto di sigarette per un ragazzino accanto a lui al banco della tabaccheria e glielo consegnasse davanti al sorriso compiaciuto del tabaccaio, più preoccupato di proteggere il suo business che la salute del bambino. Certo il divieto di vendita di sigarette ai minori sarebbe stato rispettato, ma l’obiettivo ovviamente mancato”.

¹⁵⁷ Si tratta del “modo in cui si urlano al mondo” gli eventi campali della vita del minore.

¹⁵⁸ Cfr. V.L. Miglietti, *La sovraesposizione digitale dei minori e i suoi effetti. Note comparative sul fenomeno del cd. sharenting negli ordinamenti francese e italiano*, in *Dir. comp.*, 2024, 204 ss., ove l’A. evidenzia come “sovente taluni genitori smarriscono (anzi, sembrano non aver mai trovato) la giusta modalità e misura attraverso cui gestire la presenza dei loro figli sulle principali piattaforme e, in generale, negli ambienti digitali in cui trascorrono parte delle giornate”.

implicazioni¹⁵⁹. In questa sede, lasciando in disparte le altre questioni giuridiche pure di grande rilevanza, ci si concentra esclusivamente sui rischi derivanti dalla sovraesposizione e sul diritto del minore a formare e sviluppare autonomamente la propria identità, nonché a veder rispettate tale identità e la propria dignità.

Come già anticipato, è ormai frequente il caso della creazione dell'identità digitale di un soggetto già a partire dalla prima infanzia e, a volte, addirittura ancor prima della sua nascita¹⁶⁰.

Nei casi, ad esempio, di condivisione sui *social networks* delle ecografie, i genitori creano un'identità digitale al nascituro ben prima che lo stesso abbia la possibilità di svilupparne una personale¹⁶¹. Ciò avviene nella maggior parte dei casi senza il consenso espresso del minore e, anche nei casi in cui il bambino abbia una personale tendenza ad esporsi, certamente, in ragione dell'età, in assenza di un suo consenso consapevole circa la sensibilità del contenuto, la sua destinazione e le conseguenze legate alla sua diffusione, peraltro diverse a seconda del canale utilizzato. Ciò avviene, ormai, in un mondo in cui è diventata la regola, in assenza di disapprovazione sociale, essendo percepito spesso, anzi, come comportamento dovuto¹⁶².

Ebbene, alla luce della fisiologica mutevolezza che contraddistingue l'identità del minore, risulta altamente improbabile che, a distanza di anni¹⁶³, l'interessato – divenuto adulto – possa riconoscere nell'immagine o nella reputazione che a quel punto lo rappresentano all'esterno quanto effettivamente intenda proiettare di sé, qualora queste siano state, in tutto o in parte, determinate

¹⁵⁹ Si vedano, ad esempio, le problematiche di natura lavoristica connesse allo sfruttamento del lavoro minorile o alla destinazione dei proventi percepiti dal minore, nonché le eventuali implicazioni di diritto penale qualora il materiale diffuso venga successivamente riutilizzato a fini pornografici. Per un approfondimento cfr. D. Caccioppo, *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*, Riv. it. inf. dir., 2024, 385 ss.; A. Maceratini, *Sharenting e tutela dei minori, riflessioni informatico-giuridiche tra diritto alla privacy e diritto all'immagine*, in *Rivista di scienze della comunicazione e di argomentazione giuridica*, 2024, 120 ss.; L. Miglietti, *La sovraesposizione digitale dei minori e i suoi effetti. Note comparative sul fenomeno del cd. sharenting negli ordinamenti francese e italiano*, cit., 209-211.

¹⁶⁰ S. Donovan, *Sharenting: The Forgotten Children of the GDPR*, cit.; I.A. Caggiano, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecnoregolazione*, in *Famiglia*, 2018, 3 ss.; G. Mascheroni, *"Datizzati" alla nascita: a rischio i diritti delle nuove generazioni*, in *Agendadigitale.eu*.

¹⁶¹ La Commissaria per l'Infanzia in Inghilterra (Children's Commissioner for England) ha pubblicato un rapporto –Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data, novembre 2018 – sul fenomeno della datificazione dell'infanzia e sui rischi connessi, a breve e a lungo termine, evidenziando come l'attuale rappresenti la prima generazione sottoposta a processi di datificazione sin dalla nascita.

¹⁶² Cfr. G. Scorza, E. Meligrana, *La privacy degli ultimi*, cit., 43. Gli AA. rilevano che, a distanza di tre anni, lo stesso comportamento prima criticato diventa accettato, in quanto "consuetudine". Si legge che "nessuna critica. L'esibizione via social dei neonati sembra, in appena qualche anno, diventata la regola".

¹⁶³ Nell'ambito del podcast ufficiale dell'Autorità garante per la protezione dei dati personali Guido Scorza mette in guardia anche rispetto alle nuove tecnologie come la biometria o i sistemi basati su intelligenza artificiale che, anche a distanza di molti anni, possono ricollegare l'individuo a immagini di sé del passato.

da contenuti divulgati dai genitori e ormai irrimediabilmente dispersi nell'ambiente digitale.

Il soggetto in questione potrebbe, ad esempio, non voler vedere la propria immagine accostata ad un prodotto commerciale che all'epoca ha sponsorizzato o magari esercitare il diritto all'oblio per il desiderio di sparire *in toto* dalla dimensione digitale nella quale ha fatto ingresso a sua insaputa o in una fase di completa o parziale incoscienza. L'individuo potrebbe ritenere, poi, che i contenuti diffusi e dei quali è oggetto siano lesivi della propria dignità.

Del resto, da una prospettiva costituzionalistica, la condivisione sistematica di immagini, informazioni e dati personali da parte dei genitori o di soggetti esercenti la responsabilità genitoriale determina, di fatto, la costruzione eteronoma ed eteroimposta dell'identità digitale del minore, anticipando e talvolta cristallizzando elementi che, in condizioni ordinarie, sarebbero frutto di scelte autonome e progressive¹⁶⁴. Tale fenomeno può tradursi in una compressione del diritto all'autodeterminazione informativa e, più in profondità, del diritto a definire liberamente la propria personalità, che costituisce espressione della dignità personale. In un contesto in cui la memoria digitale tende a essere permanente, il minore rischia di subire effetti pregiudizievoli duraturi, sia sul piano relazionale sia su quello reputazionale, vedendo compromessa la possibilità di controllare la narrazione pubblica di sé¹⁶⁵. Ciò laddove il minore ha, invece, diritto a costruire la propria identità digitale e, in base al principio del *best interest of the child*, tale diritto impone un limite anche alla libertà di espressione dei genitori¹⁶⁶.

Ma vi è di più. Il fenomeno evoca anche il tema della reificazione o, volendo coniare un neologismo, della "contentificazione", rischiando di ridurre il minore da soggetto titolare di diritti autonomi, peraltro vulnerabile, a oggetto della narrazione genitoriale sotto forma di contenuto digitale o, peggio, di prodotto.

Inoltre, numerosi autori segnalano i rischi connessi alla sorveglianza e alla profilazione dei minori, alimentati, tra l'altro, dalla produzione e diffusione su larga scala di contenuti sin dalla prima infanzia. Alle criticità riconducibili alla pratica dello "sharenting", infatti, si aggiungono l'utilizzo di tecnologie indossabili e dispositivi IoT, nonché altre forme di monitoraggio dei minori. In particolare, in una società caratterizzata dalla cultura della sorveglianza e della

¹⁶⁴ Cfr. proposta n. 1771/2024 nella quale si legge che "*la pubblicazione di foto di minori crea vere e proprie tracce digitali incontrollate che si sedimentano nella rete creando un'identità digitale del giovane*", con cui il medesimo dovrà fare i conti per tutta la vita, oltre al fatto che "*il caricamento indiscriminato di contenuti multimediali concernenti i bambini sarà la causa dei due terzi dei furti di identità che i giovani dovranno affrontare entro la fine del decennio*".

¹⁶⁵ Cfr. G. Scorza, E. Meligrana, *La privacy degli ultimi*, cit., 44, ove gli AA. parlano di "*se e quando di sé stesso raccontare al mondo*" e rilevano che, anche alla luce del fatto che i processi di addestramento delle intelligenze artificiali si fondano sulla raccolta massiccia di dati, "*nessuno potrà mai dirsi certo di riuscire a rendere di nuovo privato ciò che abbiamo reso pubblico*".

¹⁶⁶ M. Foglia, *Sharenting e riservatezza del minore in rete*, cit., 16.

autosorveglianza¹⁶⁷ si rischia la normalizzazione del monitoraggio della vita quotidiana, anche grazie alla condivisione massiva di contenuti¹⁶⁸.

Lo *sharenting*, dunque, in sintesi, rischia di minare sia la capacità del minore di discernere la propria identità personale da quella digitale sia quella di concepire la dignità in quanto valore anche nel corso del suo sviluppo¹⁶⁹.

È in questa prospettiva che il fenomeno si configura non solo come una questione di tutela della privacy, ma della stessa identità-dignità della persona intesa quale diritto fondamentale della persona.

Dal punto di vista normativo, il riferimento primo non può che essere la Costituzione, che, all'art. 30, tratta dei doveri di istruzione ed educazione dei genitori nei confronti dei figli e, all'art. 31, prevede che lo Stato protegga l'infanzia e la gioventù, favorendo gli istituti necessari a tale scopo.

Nell'ambito della normativa primaria, sono certamente da tenere in considerazione ai fini della presente analisi gli artt. 147 e 315 bis c.c., che parlano del diritto del figlio di essere mantenuto, educato, istruito e assistito moralmente dai genitori, *“nel rispetto delle sue capacità, delle sue inclinazioni naturali e delle sue aspirazioni”* e del diritto *“di essere ascoltato in tutte le questioni e le procedure che lo riguardano”*, indipendentemente dall'età, se ha capacità di discernimento.

Tale normativa richiama evidentemente l'art. 24 della Carta dei diritti fondamentali, sui diritti del bambino, il quale enuncia che: *“I bambini hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione; questa viene presa in considerazione sulle questioni che li riguardano in funzione della loro età e della loro maturità. In tutti gli atti relativi ai bambini, siano essi compiuti da autorità pubbliche o private, l'interesse superiore del bambino deve essere considerato preminente”*.

Con riferimento alle disposizioni a presidio del trattamento dei dati dei minori nella dimensione digitale e ai termini del consenso, si rinvia a tutto quanto esposto nei paragrafi precedenti. Può essere utile aggiungere che l'art. 50 del Codice privacy, rubricato *“Notizie o immagini relative a minori”* afferma che *“Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti*

¹⁶⁷ Per un approfondimento sul tema cfr. Byung-Chul Han, *Infocrazia*, Torino, 2023, 23. L'A., spiegando il concetto di “Infocrazia” e di “regime dell'informazione”, afferma che *“ci crediamo liberi, mentre la nostra vita è sottoposta a una protocollazione totale finalizzata al controllo psicopolitico del comportamento. Nel regime dell'informazione neoliberale il funzionamento del potere è garantito non dalla coscienza della sorveglianza permanente, bensì dalla libertà percepita”*.

¹⁶⁸ A. Maceratini, *Sharenting e tutela dei minori, riflessioni informatico-giuridiche tra diritto alla privacy e diritto all'immagine*, cit., 121.

¹⁶⁹ D. Caccioppo, *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*, cit., 7.

giudiziari in materie diverse da quella penale” e che *“La violazione del divieto di cui al presente articolo è punita ai sensi dell’articolo 684 del codice penale”*. Ciò in linea con il Codice deontologico dei giornalisti e con la Carta di Treviso.

Quanto al diritto all’immagine, come noto, il consenso della persona interessata rende legittima la pubblicazione della sua immagine (artt. 10 c.c., 96 e 97 della l. n. 644/1941 sul diritto d’autore). Tuttavia, ove l’interessato sia un minore, soggetti legittimati a prestare il consenso sono i genitori o, comunque, coloro i quali esercitano la responsabilità genitoriale, in accordo tra loro, nel rispetto della normativa sulla rappresentanza del minore (art. 320 c.c.). L’esercizio di tale potestà è congiunto in capo ai genitori anche laddove sia stato disposto il regime di affidamento condiviso del minore; solo con il consenso congiunto di entrambi i genitori, dunque, uno di essi ha la facoltà di pubblicare le foto del figlio¹⁷⁰. Per numerosità dei casi, si può affermare che la fattispecie più frequentemente analizzata dalla giurisprudenza e dalle Autorità indipendenti competenti è quella in cui si ravvisa un contrasto tra genitori sulla pubblicazione di contenuti relativi al figlio, quindi in cui manca il consenso di uno dei due¹⁷¹.

Sul tema, invece, del consenso espresso dal minore vale la pena menzionare alcune interessanti pronunce. La prima è un’ordinanza emessa dal Tribunale di Roma nel 2017¹⁷² che riguarda un sedicenne posto sotto la responsabilità di un tutore a valle della sospensione della responsabilità genitoriale di entrambi i genitori. In quel caso, il Giudice, alla luce delle condotte della madre ritenute *“persecutorie di massiccio utilizzo dei social network per diffondere immagini e dettagli sulla vicenda del figlio”*, ha ordinato, a tutela del minore e per evitare la diffusione di dati personali e contenuti relativi alla vicenda giudiziaria, la cessazione immediata della pubblicazione da parte della madre di immagini, informazioni e notizie sul figlio sui social network, nonché la loro rimozione entro i termini indicati in dispositivo. Al fine di impedire la diffusione da parte di terzi, ha autorizzato il tutore a diffidare soggetti diversi dalla madre e a richiedere la

¹⁷⁰ Si tratta di un atto che eccede l’ordinaria amministrazione e che ha ad oggetto il trattamento di dati personali sensibili, tra cui vi rientra l’immagine del soggetto minore.

¹⁷¹ Cfr. Cass. civ., sez. I, ord. 21 agosto 2024, n. 23018; nonché, Trib. Pavia, ord. 30 luglio 2024; Trib. Rieti, sent. 17 ottobre 2022, n. 443; Trib. Trani, ord. 30 agosto 2021; Trib. Ravenna, sent. 15 ottobre 2019, n. 1038; Trib. Pistoia, sez. I, ord. 7 luglio 2018; Trib. Mantova, ord. 19 settembre 2017. Le pronunce richiamate riguardano i conflitti tra genitori sulla pubblicazione di immagini, dati e informazioni del figlio minore sui social network o altri mezzi, volte a tutelare l’interesse del minore, garantire la riservatezza, la protezione psicologica e, in molti casi, imporre la rimozione dei contenuti senza il consenso di entrambi i genitori.

¹⁷² Trib. Roma, sez. I civ., ord. 23 dicembre 2017. La controversia verteva sulla ferma e reiterata volontà del minore di proseguire gli studi all’estero, in particolare negli Stati Uniti, motivata dalla necessità di sottrarsi alle pressioni derivanti dalla diffusione, da parte della madre, di immagini, informazioni e dettagli sulla sua vita privata e sulle vicende giudiziarie familiari sui social network. Il minore lamentava che tale condotta comprometteva la possibilità di condurre una vita normale in Italia e ostacolava le prospettive future. Il provvedimento del giudice tutelare autorizzava il tutore a iscriverlo al College statunitense, prevedendo strumenti di monitoraggio psicologico e scolastico per garantire il suo benessere e la prosecuzione regolare del percorso di studi.

rimozione dei contenuti anche ai gestori dei motori di ricerca, configurando un diritto all'oblio a favore del minore. Per garantire l'osservanza degli obblighi di fare, il Tribunale ha applicato altresì l'astreinte ex art. 614-bis c.p.c.: la madre, dunque, è stata condannata al pagamento di una somma in caso di mancata ottemperanza all'ordine di cessazione e rimozione dei contenuti.

In diverso caso il Giudice ha imposto a entrambi i genitori il divieto di pubblicazione di foto del minore, in assenza di consenso esplicito dell'interessato (ormai entrato nel diciassettesimo anno d'età)¹⁷³.

Come emerge dalle sentenze appena esaminate, in assenza di una normativa specifica sul tema, in effetti, la giurisprudenza si è trovata spesso a cercare un equilibrio tra la libertà del singolo genitore o di entrambi i genitori di esprimere la propria dimensione familiare e il diritto del figlio alla riservatezza, alla tutela dei dati personali e alla possibilità di costruire in modo autonomo la propria immagine nel contesto sociale. Vale la pena evidenziare altresì che, al momento, si tratta più che altro di giurisprudenza di merito, essendo scarsa, ancora, sul tema, la giurisprudenza di legittimità¹⁷⁴.

Grande interesse sul tema è stato manifestato anche dall'Autorità per la protezione dei dati personali. L'Autorità, oltre all'attività di informazione e sensibilizzazione sul tema¹⁷⁵, ha pubblicato un *vademecum* contenente indicazioni per i genitori¹⁷⁶ al fine di proteggere i figli. Il documento, oltre a mettere in guardia i genitori rispetto alle pratiche di *sharenting*, fornisce alcune importanti indicazioni nel caso in cui gli stessi decidessero comunque di pubblicare contenuti digitali relativi ai minori.

L'Autorità ha emanato altresì un provvedimento sul tema nell'ambito del quale ha ribadito che, per pubblicare immagini di minori di 14 anni, è necessario il consenso di entrambi i genitori, anche in regime di affidamento condiviso. In quel caso, ha emesso un ammonimento e imposto il divieto di ulteriori pubblicazioni

¹⁷³ Cfr. Trib. Chieti, 21 luglio 2020, n. 403.

¹⁷⁴ Sempre sul conflitto dei genitori sulla pubblicazione di foto del figlio, cfr. Cass. civ., sez. III, 15 settembre 2006, n. 190694. Nella specie, la S.C. ha cassato con rinvio la sentenza con la quale era stata rigettata la domanda di risarcimento danni proposta dalla madre di un fanciullo in conseguenza della riproduzione su una rivista settimanale del figlio minore – ritratto senza particolari cautele per renderlo non riconoscibile – vicino ad una famosa attrice in *topless* nel mentre trovavasi su una spiaggia in un atteggiamento di lotta scherzosa con il padre del bambino, all'epoca ancora non separato legalmente dalla madre, sul presupposto che, dal contesto del servizio relativo a fatti svoltisi in pubblico, non potesse derivare alcun pregiudizio alla riservatezza, nonché al decoro e alla reputazione per il minore – indicato, nel relativo articolo, come un parente dell'uomo – e per la di lui madre.

¹⁷⁵ Cfr., ad esempio, la campagna informativa del Garante privacy a tutela dei minori del gennaio 2025 dal titolo "La sua privacy vale molto più di un like". Del resto, l'art. 57, par. 1, lett. b) del GDPR prevede espressamente tra le attività delle Autorità di controllo quella di promuovere la consapevolezza e favorire la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Precisa in questo senso che "sono oggetto di particolare attenzione le attività destinate specificamente ai minori".

¹⁷⁶ *Vademecum*, Minori e nuove tecnologie, consigli ai "GRANDI" per un utilizzo sicuro da parte dei "PICCOLI".

senza autorizzazione, con obbligo di rendicontazione entro 30 giorni¹⁷⁷. Il ragionamento giuridico seguito dall’Autorità garante per la protezione dei dati personali nell’ambito di tale provvedimento, si allinea in pieno, quindi, con l’orientamento della giurisprudenza di merito già citato relativo alla necessità del consenso di entrambi i genitori.

Va infine rilevato che, sebbene parte della dottrina non sia unanime sul punto – ritenendo, infatti, già sufficienti i presidi normativi esistenti – sono state presentate, negli ultimi mesi, quattro diverse proposte di legge in materia: si tratta delle proposte nn. 1771/2024; 1800/2024; 1863/2024; 1217/2024.

La proposta di legge n. 1771/2024¹⁷⁸, presentata alla Camera dei deputati il 12 marzo 2024, si articola su due direttrici principali: la disciplina del lavoro minorile svolto sulle piattaforme digitali (*baby influencer*) e la regolamentazione della diffusione online di immagini e contenuti riguardanti i minori (*sharenting*).

Sul versante del lavoro minorile in ambito digitale e in particolare dei baby influencers¹⁷⁹, l’intervento estende l’applicazione della legge n. 977/1967 alle prestazioni a contenuto multimediale, imponendo che l’attività svolta dal minore a fini di lucro sia assistita da un contratto regolare e subordinata ad autorizzazione preventiva della Direzione provinciale del lavoro, con validità semestrale e possibilità di sospensione o revoca in caso di pregiudizio per il minore. Sul piano patrimoniale, i proventi eccedenti una determinata soglia devono essere versati su un conto intestato al minore e amministrato da un curatore speciale fino alla maggiore età, con facoltà di utilizzo parziale solo a partire dai sedici anni e nell’esclusivo interesse dell’avente diritto.

Quanto allo *sharenting*¹⁸⁰, la proposta qualifica la pubblicazione di immagini o contenuti multimediali del minore come atto di straordinaria amministrazione, consentito esclusivamente se conforme al suo interesse primario, tenendo conto della volontà del minore in relazione alla sua età e maturità. Si riconosce, inoltre, al minore che abbia compiuto quattordici anni il diritto di ottenere in ogni momento la rimozione dei contenuti che lo riguardano (*diritto all’oblio*). Le piattaforme digitali sono tenute ad adottare codici di condotta specifici, elaborati in collaborazione con AGCom, il Garante per la protezione dei

¹⁷⁷ Cfr. provvedimento del 13 novembre 2024.

¹⁷⁸ Proposta di legge n. 1771/2024, presentata il 12 marzo 2024 (Sportiello) recante “*Modifiche alla legge 17 ottobre 1967, n. 977, in materia di impiego dei minori nell’ambito delle piattaforme digitali di condivisione di contenuti multimediali, nonché disposizioni sulla diffusione dell’immagine e di contenuti multimediali di minori*”.

¹⁷⁹ Definiti come “*minori che diventano famosi sul web e la cui presenza nell’ambito delle piattaforme digitali genera introiti: si va dalla pubblicizzazione diretta di prodotti o servizi destinati ai coetanei dei minori medesimi ovvero a situazioni che indirettamente forniscono un sostegno alla pubblicizzazione o sponsorizzazione di prodotti e servizi destinati agli adulti, solitamente i genitori*”.

¹⁸⁰ Definito come “*fenomeno diverso da quello dei baby influencer, che non comprende lo sfruttamento commerciale, ma consiste nella pratica dei genitori di condividere sui social media contenuti multimediali (foto, audio, video) dei propri figli*”.

dati personali e il Garante per l'infanzia e l'adolescenza. Infine, si propone l'innalzamento da quattordici a sedici anni dell'età minima per il consenso al trattamento dei dati personali, in coerenza con il Regolamento (UE) 2016/679.

La seconda proposta di legge, la n. 1800/2024¹⁸¹, disciplina la tutela dei minori in ambito digitale attraverso tre principali articolazioni normative. In primo luogo, apporta modifiche all'art. 37 del Testo unico dei servizi di media audiovisivi, prevedendo che l'utilizzo dell'immagine del minore in contesti digitali a fini di visibilità o profitto richieda un'autorizzazione preventiva al fine di salvaguardarne l'integrità psicofisica e prevenire forme di sfruttamento. Quanto ai proventi derivanti dallo sfruttamento del contenuto riguardante il minore, devono essere versati da chi esercita la responsabilità genitoriale o dai rappresentanti legali in un deposito bancario intestato al minore medesimo e sono inutilizzabili fino al compimento del diciottesimo anno di età. Eventuali prelievi possono essere autorizzati dall'autorità giudiziaria in caso di emergenza e in via eccezionale. In secondo luogo, viene riconosciuto il diritto all'oblio al minore quattordicenne, il quale può richiedere la rimozione dei propri dati e contenuti personali dai motori di ricerca e dalle piattaforme online, garantendo la tutela della propria identità digitale e della sfera privata. Infine, la proposta prevede l'adozione di un codice di autoregolamentazione da parte delle piattaforme digitali, volto a stabilire standard operativi per la gestione responsabile dei contenuti che riguardano i minori, incluse misure preventive e linee guida per l'uso corretto delle immagini e dei dati dei soggetti più giovani.

La relazione illustrativa della seconda proposta si sofferma sul tema dell'eterostruzione dell'identità digitale dei più giovani rilevando che *“dobbiamo poi considerare il benessere psicologico dei bambini: le reti sociali telematiche sono il regno dell'automediazione, poiché siamo noi a scegliere cosa condividere di noi stessi, come autorappresentarci. Ai minori, invece, questa scelta viene negata; la cosiddetta «generazione Alpha», ossia quella dei nati dopo il 2012, è la prima che si dovrà confrontare, una volta cresciuta, con un archivio digitale della propria vita costruito sulla base di centinaia di immagini, video o altri contenuti che non ha scelto di condividere e di commenti da parte di sconosciuti”*.

Correttamente, sul tema dell'identità digitale, la relazione pone l'accento sulla particolare delicatezza dei momenti ripresi e diffusi dai genitori – talvolta riguardanti i più piccoli in situazioni estremamente intime, come pianti, malattie, manifestazioni di disagio o difficoltà – ma non giunge a evocare espressamente il tema della dignità del minore, limitandosi a evidenziare esclusivamente i rischi

¹⁸¹ Proposta di legge n. 1800/2024, presentata il 22 marzo 2024 (Bonelli et altri) in materia di *“Modifiche all'articolo 37 del testo unico dei servizi di media audiovisivi, di cui al decreto legislativo 8 novembre 2021, n. 208, in materia di impiego dei minori nell'ambito delle piattaforme digitali per la condivisione di video, audio e immagini, e disposizioni concernenti il diritto del minore alla rimozione dei dati e dei contenuti che lo riguardano dalla rete internet e dai motori di ricerca”*.

legati alla condivisione di tali circostanze (come la sessualizzazione). Si parla, poi, correttamente, di “*mercificazione dell’infanzia*”.

Nella proposta di legge n. 1863/2024¹⁸², si chiede che ai fornitori di servizi della società di informazione sia imposto di predisporre all’interno delle loro piattaforme un numero telefonico di emergenza specifico per l’infanzia (numero 114).

Infine, rileva l’interessante iniziativa n. 1217/2024¹⁸³, che contiene un riferimento anche al tema dell’*age verification* e la proposta di modifica del codice privacy. Tale ultima proposta parte dalla constatazione del fatto che in Italia la verifica dell’età è fondata su un criterio di autocertificazione ed è molto facile per un minore di 14 anni avere comunque accesso alle piattaforme on line, usando false date di nascita. Ciò anche in ragione del fatto che la legge italiana non prevede alcun obbligo per i produttori di dispositivi di comunicazione elettronica di garantire nei sistemi operativi installati la disponibilità di applicazioni di controllo parentale.

Ebbene, in questo contesto, la proposta, in primo luogo, interviene sull’art. 2-*quinquies* del Codice in materia di protezione dei dati personali, elevando da quattordici a quindici anni l’età minima richiesta affinché i minori possano validamente prestare il proprio consenso autonomo al trattamento dei dati personali connesso alla fruizione dei servizi digitali.

In secondo luogo, prevede un espresso divieto di accesso, per i minori di tredici anni, ai servizi di comunicazione elettronica che presentano specifici profili di rischio per la salute psicofisica, la sicurezza e l’incolumità dei minori. L’individuazione di tali servizi è demandata al Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, previa procedura istruttoria con consultazione dei gestori interessati, sulla base delle caratteristiche tecniche, delle modalità di funzionamento e degli eventuali usi illeciti dei servizi medesimi.

L’accesso a tali servizi sarebbe dunque consentito solo a partire dal compimento dei quindici anni, fatta salva l’applicazione di disposizioni che richiedano la maggiore età. Per i minori di età compresa tra i tredici e i quindici anni, l’accesso è subordinato alla previa autorizzazione da parte dei genitori esercenti la responsabilità genitoriale.

A tutela dell’effettività delle disposizioni, il testo introduce un meccanismo di verifica dell’età basato sulla certificazione anagrafica da parte di prestatori di servizi fiduciari accreditati ai sensi del regolamento (UE) n. 910/2014 (eIDAS). Tale sistema deve garantire l’anonimato delle credenziali di accesso, salvaguardare

¹⁸² Proposta di legge n. 1863/2024, presentata il 13 maggio 2024 (Madia - Mennuni) recante “*Disposizioni per la tutela dei bambini e degli adolescenti nell’utilizzo degli strumenti digitali*”.

¹⁸³ Proposta di legge n. 1217/2024, presentata l’8 giugno 2023 ma il cui esame in Commissione è iniziato il 26 giugno 2024, in ordine alle “*Modifiche al codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, in materia di verifica dell’età degli utenti dei servizi di comunicazione elettronica, e altre disposizioni per la tutela dei minori nella fruizione di tali servizi*”.

la riservatezza dell'identità degli utenti e minimizzare i dati trasmessi ai gestori, nonché i tempi di loro eventuale conservazione. L'infrastruttura potrà avvalersi anche di strumenti già operativi, quali SPID e Carta di identità elettronica, ed è rimessa a specifica disciplina attuativa mediante decreto del Presidente del Consiglio dei ministri.

Le spese di implementazione e integrazione dei predetti sistemi di verifica sono poste a carico dei gestori dei servizi di comunicazione elettronica, mentre le violazioni delle disposizioni introdotte ricadono nell'ambito del quadro sanzionatorio previsto dal Regolamento generale sulla protezione dei dati (GDPR).

Da ultimo, come anticipato, il tema è trattato anche dal menzionato ddl n. 1136 del 2024 attualmente in fase di istruttoria presso la Commissione VIII del Senato. Il testo normativo non sembra preoccuparsi della iperdiffusione di contenuti ritraenti minori laddove non siano finalizzati a monetizzazione. L'art. 5 sopra menzionato, infatti, disciplina esclusivamente i proventi derivanti dalla diffusione di immagini di minori, così liberalizzando da una parte la pratica dello "sharenting" dall'altra quella dei "baby influencers" maggiori di 15 anni. Pur non essendoci un divieto espresso, infatti, la norma sembra dire che sotto i quattordici anni non sia proprio ammessa una diffusione a scopo di lucro. Si ritiene sarebbe stato più efficace inserire un divieto esplicito e farlo anche per i minori di diciotto anni. Del resto, non è detto e non è supportata da dati la circostanza per la quale un maggiore di quindici anni espone con consapevolezza la propria identità digitale a fronte di un provento economico. Anche la soglia dei diecimila euro a fronte della quale le somme guadagnate dal minore devono essere versate su un conto dedicato risulta eccessivamente alta e idonea a prestarsi ad elusioni. Del resto, per come è formulata, la disposizione sembra riferirsi alla singola prestazione (che può ben essere remunerata meno di diecimila euro) e non al complesso delle somme percepite per l'esposizione del minore.

7. Tecniche di regolazione a confronto: l'esempio francese.

Si ritiene utile soffermarsi brevemente sull'esperienza francese. La Francia, infatti, ha adottato, con riferimento all'accesso dei minori ai contenuti pornografici, un approccio simile all'Italia nel merito e in parte nel metodo. In realtà, risulta più corretto affermare che la normativa italiana sul tema è evidentemente ispirata a quella francese sia dal punto di vista dei contenuti che delle Autorità indipendenti coinvolte. Per quanto entrambi i Paesi operino nel solco di quanto tracciato a livello sovranazionale dal Digital services Act e abbiano optato per un approccio repressivo ai contenuti pornografici, la differenza principale, come si proverà ad evidenziare nell'ambito delle conclusioni, è da ricercare probabilmente nel percorso che porta i due Paesi all'adozione delle rispettive normative: in Francia, la regolazione rappresenta il punto di arrivo di analisi di dati e studi condotti sul tema, è adottata con legge ordinaria e si aggiunge ad altre normative adottate a presidio

dei minori; in Italia, come si è visto, si tratta della risposta introdotta con decretazione d'urgenza a drammatici fatti che hanno coinvolto alcuni giovani.

In ogni caso, come emergerà dall'analisi effettuata nei prossimi paragrafi, si ritiene che l'esperienza francese possa essere in generale paradigmatica per la regolazione dei diritti dei minori nella dimensione digitale, in quanto rappresenta un caso concreto di processo regolatorio che potremmo definire "dinamico", nel quale la normazione primaria, la produzione regolamentare, la resistenza degli operatori economici e lo scrutinio giurisdizionale si intrecciano nella ricerca di un equilibrio tra tutela dei minori, protezione dei dati personali e libertà economiche nel contesto digitale¹⁸⁴. Inoltre, essendo la normativa francese sul tema simile ma precedente a quella italiana, la stessa consente di analizzare gli effetti della prima applicazione e trarne alcune conclusioni.

7.1. L'esperienza francese sull'obbligo di verifica dell'età.

A seguito della promulgazione della legge n. 2024-449 del 21 maggio 2024, nota come *loi visant à sécuriser et à réguler l'espace numérique* (cd. Legge "SREN"), il legislatore francese ha introdotto un complesso apparato regolatorio volto a disciplinare l'accesso dei minori ai contenuti pornografici disponibili online¹⁸⁵. La riforma ha sancito il superamento del precedente modello basato sull'autodichiarazione dell'utente, introducendo per i prestatori di servizi l'obbligo di accertare l'età degli utenti, con il supporto di poteri sanzionatori e di ingiunzioni conferiti all'Autorité de régulation de la communication audiovisuelle et numérique (di seguito anche "ARCOM")¹⁸⁶.

In attuazione del mandato legislativo, l'ARCOM – previo espletamento di una consultazione pubblica e acquisito il parere della Commission nationale de l'informatique et des libertés (CNIL) – ha adottato un *référéntiel technique* destinato a specificare le modalità operative della verifica dell'età¹⁸⁷. Il documento introduce un sistema basato sul principio del *double anonymat*, secondo il quale la funzione di accertamento dell'identità dell'utente è attribuita a un prestatore terzo certificato, mentre al sito ospitante i contenuti è trasmessa unicamente la conferma dell'avvenuta verifica, senza alcun dato identificativo¹⁸⁸.

La scadenza per l'adeguamento è stata fissata all'11 gennaio 2025; tuttavia, all'indomani dell'efficacia dell'obbligo, alcuni tra i principali operatori del settore

¹⁸⁴ Per un approfondimento sul tema cfr., nella dottrina straniera, L. Huttner, *Le contrôle de l'accès des mineurs aux sites pornographiques*, 2024; M.P. JolicoeuR, *Vérifier l'âge des internautes sur les sites pornographiques*, 2023; T. Radtke, *Mandatory Age Verification for Online Services under GDPR*, 2023; M. Sas, J.T. Mühlberg, *Trustworthy Age Assurance?*, 2024.

¹⁸⁵ *Loi n° 2024-449 du 21 mai 2024, visant à sécuriser et à réguler l'espace numérique*.

¹⁸⁶ Art. 227-24 Code pénal.

¹⁸⁷ ARCOM, *Référéntiel relatif à la vérification de l'âge*, 11 ottobre 2024.

¹⁸⁸ Sul *double anonymat v. ARCOM*; CNIL, *Avis sur le projet de référentiel*, 26 settembre 2024.

– segnatamente le piattaforme del gruppo Aylo – hanno sospeso l’accesso ai loro servizi dal territorio francese, denunciando il carattere intrusivo e potenzialmente lesivo della riservatezza del nuovo impianto.

Tale iniziativa ha dato origine a un acceso dibattito pubblico e a un contenzioso amministrativo. In particolare, il giudizio ha riguardato la richiesta di un operatore del settore al tribunale amministrativo di Parigi di sospendere in via cautelare il Decreto del 26 febbraio 2025 del Ministro della Cultura e il Ministro Delegato presso il Ministro dell’Economia, delle Finanze e della Sovranità Industriale e Digitale, responsabile per l’Intelligenza Artificiale e gli Affari Digitali¹⁸⁹. Tale Decreto era necessario per la piena attuazione della citata normativa di rango primario, in quanto designava specifici fornitori di servizi di comunicazione pubblica online e piattaforme di condivisione video, compresi operatori stabiliti in altri Stati membri dell’UE, come soggetti agli obblighi di verifica dell’età previsti dagli articoli 10 e 10-1 della LCEN.

Il giudice amministrativo ha sospeso d’urgenza l’esecuzione di tale Decreto sulla base del solo fatto che, a suo avviso, sussistono forti dubbi sulla compatibilità di quanto previsto nello stesso con il diritto dell’unione europea¹⁹⁰. La questione giuridica sottesa al contenzioso concerne il noto principio del “paese d’origine”¹⁹¹, che prevede che un prestatore di servizi digitali è soggetto esclusivamente alle regole del paese in cui è stabilito, anche quando i servizi sono resi disponibili in altri Stati membri dell’UE e che ammette deroghe solo qualora le misure nazionali ricadano in determinati e tassativi ambiti e in ogni caso risultino giustificate da obiettivi imperativi d’interesse generale e siano proporzionate. È in tale cornice che si colloca il controllo da parte del giudice amministrativo francese della compatibilità delle misure di verifica dell’età con i limiti posti dal diritto europeo.

La fase di sospensione è tuttavia cessata con l’intervento del Conseil d’État, che, il 15 luglio 2025, ha annullato l’ordinanza cautelare, riaffermando la piena legittimità del quadro regolatorio e il carattere proporzionato delle misure in relazione all’obiettivo di protezione dei minori¹⁹². Pertanto, l’obbligo di verifica

¹⁸⁹ Arrêté du 26 février 2025 désignant les services de communication au public en ligne et les services de plateforme de partage de vidéos établis dans un autre Etat membre de l’Union européenne soumis aux articles 10 et 10-1 de la loi no. 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique.

¹⁹⁰ Tribunal administratif de Paris, ord. caut. n. 2514377/5 du 16 juin 2025.

¹⁹¹ Sul principio del *country of origin* cfr. la direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell’8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico (art. 3); il *Digital Services Act* – Regolamento 2022/2065/UE (artt. 2, 3 e 26), che conferma e aggiorna l’applicazione del principio ai servizi digitali moderni. Si vedano, altresì, le pronunce della Corte di giustizia dell’Unione europea e, in particolare CGUE, C-314/12, *UPC Telekabel Wien GmbH*, 19 dicembre 2013, e C-511/18, *Glawischnig-Piesczek*, 3 ottobre 2019, ove si chiariscono i limiti delle eccezioni al principio e l’applicabilità degli interessi pubblici imperativi (tutela dei minori, sicurezza pubblica, salute pubblica) come giustificazione per deroghe.

¹⁹² Cfr. Conseil d’État, ord. 15 luglio 2025, n. 505472

dell'età è tornato immediatamente esecutivo nei confronti di tutti i prestatori, a prescindere dal luogo di stabilimento.

Il Consiglio di Stato francese, in particolare, ritiene sia un errore giustificare la sospensione d'urgenza con il solo dubbio di incompatibilità con la normativa sovranazionale e che, in ogni caso, non sussista l'urgenza lamentata dalla ricorrente e riconosciuta dal giudice¹⁹³.

Ci si vuole soffermare, tuttavia, su un *obiter dictum* della pronuncia, in cui il Consiglio di Stato francese stabilisce: “*Il résulte de tout ce qui précède, eu égard également à l'intérêt public qui s'attache à la protection des mineurs contre l'exposition à des contenus à caractère pornographique - à laquelle il ne ressort pas des pièces du dossier, en l'état, que, du fait notamment de l'existence de possibilités de contournement des systèmes de vérification de l'âge, les dispositions législatives rendues applicables par l'arrêté litigieux ne seraient pas propres à contribuer -, que la condition d'urgence prévue par l'article L. 521-1 du code de justice administrative ne peut être regardée comme remplie*”¹⁹⁴.

Con tale inciso, sembra affermare – pur senza entrare nel merito della legittimità sostanziale della legge, poiché la richiesta di sospensione è respinta per mancanza di urgenza – che “anche se gli utenti potrebbero tentare di eludere i controlli, non è dimostrato che ciò renda le misure legislative completamente inefficaci rispetto all'interesse pubblico connesso alla protezione dei minori”, formulando così un giudizio implicito sull'efficacia della legge.

La mobilitazione del 2025 da parte dei principali operatori internazionali del settore ha evidenziato che l'effettiva operatività delle misure di verifica dell'età non può essere valutata unicamente sulla base dei dettami normativi. La temporanea sospensione dei servizi da parte delle piattaforme del gruppo Aylo ha generato una tensione regolatoria in concreta, sollecitando l'intervento del sistema giurisdizionale e mettendo in luce un conflitto intrinseco tra l'esigenza di tutela dei minori, la salvaguardia delle libertà economiche e la protezione della riservatezza

¹⁹³ Hammy Media Ltd invocava tre motivi a sostegno della sospensione urgente del decreto del 26 febbraio 2025: i) perdite economiche derivanti dal calo di traffico e fatturato (la società sosteneva che l'obbligo di verifica dell'età avrebbe sospinto gli utenti adulti verso piattaforme concorrenti, causando gravi perdite pubblicitarie), sicché il Conseil d'État ha rilevato che i dati forniti dalla società riguardavano solo tre Stati USA e non permettevano di stimare l'effettivo impatto sul traffico francese, né sul fatturato globale, concludendo che l'argomento non dimostrava un'urgenza reale; ii) lesione dei diritti degli utenti adulti (libertà di espressione e privacy): la società sosteneva che i sistemi di verifica avrebbero violato tali diritti e in proposito il Conseil d'État ha osservato che la normativa non vieta la distribuzione dei contenuti agli adulti, ma richiede sistemi di verifica conformi alla legge e rispettosi della privacy, in particolare secondo il GDPR e le indicazioni della CNIL, escludendo quindi la lesione dei diritti come base per sospendere il decreto; iii) presunto pregiudizio economico e commerciale nel bilanciamento dei provvedimenti cautelari: Hammy Media Ltd sosteneva che l'applicazione immediata del decreto avrebbe compromesso la gestione del servizio e la posizione sul mercato; in questo caso il Conseil d'État ha affermato che il mero rischio di danno economico non costituisce di per sé urgenza ai sensi dell'art. L. 521-1 del codice di giustizia amministrativa, soprattutto in presenza di un interesse pubblico preminente alla protezione dei minori.

¹⁹⁴ Conseil d'État, ord. 15 luglio 2025, n. 505472, § 16.

dei dati personali. La pronuncia del Conseil d'État del luglio 2025 citata, pur riaffermando la piena legittimità del quadro normativo, testimonia come la regolazione dell'accesso ai contenuti pornografici in ambito digitale si sviluppi secondo una logica dinamica e iterativa, in cui la giurisprudenza assume un ruolo essenziale nel definire i limiti di proporzionalità delle misure adottate. Si sottolinea nuovamente, però, essendo un elemento fondamentale ai fini della presente trattazione, che il Consiglio di Stato francese, esprimendosi sul mancato soddisfacimento della condizione dell'urgenza, non è entrato nel merito della legittimità della pronuncia. Il dubbio sollevato dal giudice francese di primo grado circa la compatibilità della legge con il diritto eurounitario, dunque, permane, soprattutto alla luce della posizione della Corte di Giustizia sul tema del “*country of origin*”¹⁹⁵ e potrebbe ripresentarsi ben presto anche nel contesto italiano.

L'esperienza francese si configura, dunque, con tutte le particolarità del caso di specie, come un laboratorio giuridico e politico d'avanguardia, paradigmatico delle sfide che attendono gli Stati membri nell'implementazione di sistemi di *age assurance* conformi al diritto dell'Unione europea.

¹⁹⁵ Cfr. Conclusions de l'Avocat général M. Maciej Szpunar, présentées le 18 septembre 2025, dans les affaires jointes C-188/24 et C-190/24, *WebGroup Czech Republic, a.s. et NKL Associates s.r.o. c. Ministre de la Culture et Premier ministre, en présence de Osez le féminisme!, Le mouvement du Nid, Les effronté-E-S (C-188/24), et Coyote System c. Ministre de l'Intérieur et des Outre-mer et Premier ministre (C-190/24)*, demande de décision préjudicielle formée par le Conseil d'État (France), «Renvoi préjudiciel – Commerce électronique – Directive 2000/31/CE – Services de la société de l'information – Domaine coordonné – Réglementation pénale interdisant de manière générale la fourniture de contenus pornographiques à des mineurs – Interdiction de rediffusion des informations fournies par les utilisateurs». Al momento in cui si scrive, è ancora pendente la decisione della Corte di giustizia sui rinvii pregiudiziali proposti dal Conseil d'État francese nelle cause riunite C-188/24 e C-190/24 (*WebGroup Czech Republic e NKL Associates e Coyote System*). Le cause riguardano questioni relative agli obblighi imposti dalla normativa francese a fornitori di servizi della società dell'informazione stabiliti all'estero, tra cui misure tecniche di filtraggio o blocco dei contenuti per impedire l'accesso dei minori a materiale pornografico e obblighi di cooperazione con le Autorità. Nelle conclusioni del 18 settembre 2025, l'Avvocato generale Szpunar osserva che “Le “domaine coordonné” défini par la directive englobe l'obligation imposée aux éditeurs de services de communication en ligne d'instaurer des dispositifs techniques destinés à empêcher l'accès des mineurs à des contenus pornographiques”. Secondo l'Avvocato generale, tali obblighi rientrano nel “campo coordinato” della direttiva 2000/31/CE e, di conseguenza, non possono essere imposti unilateralmente da uno Stato membro a prestatori stabiliti in un altro Stato membro, se non nel rispetto delle condizioni e delle procedure previste dalla direttiva (principio del paese d'origine, notifica preventiva, proporzionalità delle misure). Le Conclusioni non si pronunciano direttamente sulla normativa francese specifica (SREN), ma offrono indicazioni interpretative rilevanti per valutare la compatibilità di obblighi nazionali analoghi con il diritto dell'Unione europea.

7.2. L'approccio francese ai fenomeni dello "sharenting" e dei "baby influencer".

La Francia è stata anche pioniera rispetto all'adozione di una specifica normativa in tema di "sharenting" e "baby influencer"¹⁹⁶, fenomeni sui quali ci si è soffermati *supra* e rispetto ai quali, come anticipato, anche l'Italia ha intenti regolatori. Anche in questo caso, sebbene le normative siano molto recenti, può essere utile analizzare i contenuti delle stesse e le prime applicazioni nell'ottica di trarre spunti di riflessione per l'ordinamento italiano, oltre che ispirazione, come, in effetti, sembra si stia già facendo.

Con riferimento al fenomeno dello "sharenting", fino al 2024, in Francia, la tutela del minore era affidata al diritto generale all'immagine e alla vita privata, senza una disciplina specifica applicabile alla diffusione massiva di contenuti digitali¹⁹⁷. La giurisprudenza si presentava frammentaria e non uniforme: talvolta la pubblicazione di immagini da parte di un genitore veniva qualificata come un *acte usuel* nell'ambito della vita familiare, mentre in altri casi i tribunali richiedevano il consenso congiunto di entrambi i genitori¹⁹⁸.

Il punto di svolta normativo è rappresentato dalla Loi n° 2024-120 du 19 février 2024, volta a garantire il rispetto del diritto all'immagine dei bambini¹⁹⁹. La legge inserisce espressamente il diritto all'immagine del minore tra i diritti tutelati nell'ambito dell'autorità parentale, stabilendo che la diffusione di contenuti online richiede il consenso congiunto di entrambi i genitori e che l'opinione del minore, in funzione della sua età e maturità, debba essere considerata²⁰⁰. In caso di pubblicazione pregiudizievole della dignità o dell'integrità morale del minore, il

¹⁹⁶ Tra i contributi sul tem, v. I. Tepelena, *The Legal Framework of Sharenting: Protecting Children's Rights in the Digital Age*, in *International Journal of Rights and Digital Law*, 2023, 93 ss.; D. Caccioppo, *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*, in *Riv. it. inf. dir.*, 2024, 385 ss.; L. Miglietti, *La sovraesposizione digitale dei minori ed i suoi effetti. Note comparative sul fenomeno del cd. sharenting negli ordinamenti francese e italiano*, in *Dir. comparati*, 2024, 204 ss.; R. Suárez-Álvarez, A. Pastor-Rodríguez, *Risks in Children's Digital Visibility and Vulnerability: Sharenting in France, Italy, Spain, and the United Kingdom*, in *European Journal of Children and Media Studies*, 2025/2026, 1 ss.

¹⁹⁷ Si veda Conseil constitutionnel, *décision n° 2020-831 DC du 21 janvier 2020*, in materia di tutela della vita privata e immagine dei minori.

¹⁹⁸ Cass. civ., 1re ch., 5 février 2019, n° 18-10.022, in tema di diritto all'immagine dei minori e consenso dei genitori. Secondo alcuni autori anche prima della approvazione di una legge dedicata era comunque garantita una tutela adeguata al minore dalla normativa previgente.

¹⁹⁹ Cfr. Loi n° 2024-120 du 19 février 2024, *visant à garantir le respect du droit à l'image des enfants*. Per un approfondimento cfr. M. Hervieu, *Point sur la loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants*, Dalloz Actu Étudiant, 14 mars 2024; A. Bourrat-Guèguen, *Respect du droit à l'image des enfants: ce que change la loi du 19 février 2024*; N. Baillon-Wirtz, *L'enfant aussi a une vie privée et un droit à l'image*; G. Haas, *Proposition de loi: l'image des enfants enfin protégée sur internet?*; P. Lingibè, *Le respect du droit à l'image des enfants et les 5 apports de la loi du 19 février 2024*; D. Madji, *Le Droit à l'image des enfants sur internet: nouvelle protection par la loi du 19 février 2024*.

²⁰⁰ Cfr. Z. Garno, *Première analyse de la loi visant à garantir le respect du droit à l'image des enfants*, in *Village-justice.com*, 1 ss.

giudice può adottare misure restrittive, tra cui la limitazione o la delega dell'autorità parentale a terzi, nonché ordinare provvedimenti urgenti di blocco o rimozione dei contenuti²⁰¹. La normativa attribuisce inoltre alla *Commission nationale de l'informatique et des libertés* (CNIL) il potere di vigilanza sulla protezione dei dati personali, con facoltà di intervenire per il blocco di contenuti non conformi²⁰².

Il quadro normativo francese comprende altresì la disciplina dei cosiddetti “baby influencer”, espressione con la quale, come anticipato, ci si riferisce a minori protagonisti di contenuti digitali a scopo commerciale. La Loi n° 2020-126 du 19 octobre 2020 ha introdotto regole specifiche per la tutela dei minori impiegati in contesti digitali a fini promozionali, assimilando tale attività, quando remunerata, a un rapporto di lavoro minorile nel settore dello spettacolo²⁰³.

In particolare, la normativa prevede che: l'impiego del minore come protagonista di contenuti digitali a scopo commerciale richieda un'autorizzazione preventiva da parte delle autorità competenti; i genitori o titolari della responsabilità genitoriale siano informati sui diritti del minore, sui rischi connessi alla diffusione dell'immagine e sugli effetti economici derivanti dall'attività; una quota dei compensi derivanti dall'attività sia vincolata fino al raggiungimento della maggiore età del minore; il minore possa esercitare un diritto autonomo di rimozione dei contenuti, in analogia al principio del “diritto all'oblio digitale”.

L'intervento normativo del 2020, integrato dalla legge del 2024, ha costituito un modello completo di regolamentazione dell'impiego mediatico o commerciale dei minori, combinando la tutela dell'immagine, le garanzie relative ai dati personali e le regole sul lavoro minorile. Nonostante la chiarezza normativa, la sua efficacia pratica dipenderà dall'applicazione da parte dei tribunali e delle autorità amministrative e dalla consapevolezza dei genitori circa i rischi connessi all'esposizione digitale dei minori.

8. L'impatto dell'intelligenza artificiale sull'identità digitale del minore: stato dell'arte, profili di rischio e opportunità.

Oramai i minori, sin dalle prime fasi dello sviluppo, entrano quotidianamente in contatto con sistemi di intelligenza artificiale²⁰⁴ in molteplici contesti. Tali sistemi, del resto, comprendono, tra l'altro, assistenti virtuali e chatbot educativi, motori di raccomandazione su piattaforme audiovisive e musicali,

²⁰¹ Cfr. Loi n° 2024-120, artt. 2, 4, 6 e 7.

²⁰² CNIL, *Rapport annuel 2024 – Protection des données personnelles des mineurs*, Paris, 2024.

²⁰³ Loi n° 2020-126 du 19 octobre 2020, *relative à l'exercice de l'image des mineurs sur les plateformes en ligne*.

²⁰⁴ L'art. 3, § 1, n. 1 dell'AI Act definisce un “sistema di IA” come “un sistema automatizzato, progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali”.

applicazioni di gaming interattivo e strumenti di realtà aumentata, nonché piattaforme di supporto scolastico basate su IA, finalizzate al tutoring personalizzato e alla valutazione automatizzata²⁰⁵. Anche i giochi spesso sono intelligenti²⁰⁶.

Già da tempo si riconosce come l'intelligenza artificiale possa offrire opportunità ai minori²⁰⁷, comportando però anche possibili rischi per la tutela dei loro diritti²⁰⁸. Sono noti i casi, ormai anche al vaglio della giurisprudenza di cause intentate contro produttori di modelli e sistemi di IA per istigazione al suicidio di minorenni²⁰⁹.

La regolamentazione è intervenuta con ritardo anche per quanto riguarda le interazioni tra minori e algoritmi, nonché con modelli e sistemi di intelligenza artificiale²¹⁰.

²⁰⁵ Sui relative rischi cfr. Statement on AI and Children, 11 October 2024.

²⁰⁶ Cfr. vademecum del Garante per la protezione dei dati personali sugli Amart toys (giocattoli intelligenti). In dottrina cfr. G. Scorza, E. Meligrana, *La privacy degli ultimi*, cit., 39 ss.

²⁰⁷ Cfr., ancora, Statement on AI and Children, 11 October 2024.

²⁰⁸ Per un approfondimento sul tema cfr. V. Charisi, S. Chaudron, R. Di Gioia, R. Vuorikari, M. Escobar Planas, J.I. Sanchez Martin, E. Gomez Gutierrez, *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy*, in *Publications Office of the European Union*, Luxembourg, 2022. Il rapporto intende fornire elementi per un'agenda integrata di ricerca e di policy sui diritti dei bambini e l'intelligenza artificiale. L'obiettivo è connettere le evidenze scientifiche con l'elaborazione delle politiche, acquisire una visione dell'interazione tra i diversi attori coinvolti e andare oltre la mera individuazione di linee guida etiche, verso metodi di implementazione pratica per il futuro. Viene presentata una rassegna delle principali iniziative politiche rilevanti, seguita da una panoramica della ricerca su tre applicazioni di IA selezionate per i bambini: agenti conversazionali, sistemi di raccomandazione e sistemi robotici, analizzate attraverso la lente dei diritti dell'infanzia. Successivamente, vengono illustrati i risultati di due workshop con bambini e ragazzi, e di tre workshop con portatori di interesse provenienti dal mondo delle politiche e della ricerca sui diritti dei minori e l'IA. Sulla base di questi contributi, viene fornito un insieme di raccomandazioni per un'agenda integrata e per le future direzioni della ricerca e delle politiche. Infine, il rapporto include le riflessioni di esperti invitati del settore, che hanno partecipato e contribuito a questo studio.

²⁰⁹ OpenAI è attualmente coinvolta in sette procedimenti giudiziari, ove si contesta che la chatbot basata su intelligenza artificiale (ChatGPT), abbia indotto individui al suicidio o a gravi delusioni, anche in assenza di precedenti condizioni di salute mentale. I ricorsi, depositati lo scorso novembre presso i Tribunali statali della California, contestano all'azienda responsabilità per morte ingiusta, istigazione al suicidio, omicidio colposo e negligenza. I procedimenti, promossi a nome di sei adulti e di un minore dal Social Media Victims Law Center e dal Tech Justice Law Project, sostengono che OpenAI ha rilasciato prematuramente il modello GPT-4o, nonostante avvertimenti interni circa la sua tendenza a comportamenti eccessivamente adulativi e alla capacità di influenzare psicologicamente gli utenti in maniera manipolativa.

²¹⁰ Per una distinzione tra "algoritmo" e "intelligenza artificiale" cfr. sentenza Cons. Stato, 25 novembre 2021, n. 7891 ove si legge che "non v'è dubbio che la nozione comune e generale di algoritmo riporti alla mente "semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato" (questa la definizione fornita in prime cure). Nondimeno si osserva che la nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare. Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di machine learning e crea un sistema che non si limita solo ad

Anche in questo ambito, per lungo tempo, il principale punto di riferimento è stato rappresentato dal Regolamento europeo sulla protezione dei dati personali. In particolare, l'art. 22 GDPR garantisce all'interessato il diritto a non essere soggetto a decisioni basate esclusivamente su trattamenti automatizzati, inclusa la profilazione, qualora tali decisioni producano effetti giuridici o incidano significativamente sulla sua persona²¹¹.

Il manifestarsi del vuoto normativo, divenuto particolarmente evidente con la diffusione massiva di sistemi di intelligenza artificiale generativa²¹², ha indotto l'Autorità Garante per la protezione dei dati personali a porsi come primo attore istituzionale nella gestione delle relative problematiche.

Nel febbraio 2023, l'Autorità ha disposto con effetto immediato la limitazione provvisoria del trattamento dei dati personali degli utenti italiani da parte di un'applicazione basata sull'intelligenza artificiale che genera un "amico virtuale". Tale provvedimento era motivato in ragione dei paventati rischi per i minori e le persone emotivamente fragili. L'Autorità ha rilevato che l'applicazione presenta risposte assolutamente inadeguate al grado di sviluppo dei minori e che le sue caratteristiche, che mirano a intervenire sull'umore dell'utente per migliorare il benessere emotivo e gestire l'ansia, possono accrescere i rischi per soggetti in fase di sviluppo o in stato di fragilità emotiva. È stata riscontrata, inoltre, la totale assenza di meccanismi di verifica dell'età. Infatti, non ci sono filtri per i minori né blocchi dell'app, anche se l'utente dichiara di essere minorenne ma la piattaforma si limita a richiedere solo nome, e-mail e genere per la creazione dell'account, nonostante i termini di servizio indichino un divieto di utilizzo per i minori di 13 anni e l'idoneità per maggiori di 17 anni negli App Store. Inoltre, le "risposte" della chatbot sono risultate spesso in palese contrasto con le tutele rafforzate per i minori e i soggetti più fragili, con diverse recensioni che lamentavano contenuti sessualmente inappropriati²¹³. La Società è stata successivamente sanzionata. Dagli accertamenti tecnici effettuati, infatti, è emerso che il sistema di verifica dell'età

applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico".

²¹¹ Cfr. art. 22 GDPR. Si tratta di una tutela pensata per evitare che talune scelte rilevanti – ad esempio in materia di credito, assunzione o accesso a servizi – vengano assunte senza alcun margine di valutazione umana. Il divieto non è assoluto. Il legislatore europeo, infatti, ammette eccezioni qualora la decisione sia necessaria all'esecuzione di un contratto, sia prevista da una norma di legge che garantisca misure adeguate di salvaguardia, oppure si fonda sul consenso esplicito dell'interessato. In queste ipotesi, tuttavia, il titolare del trattamento è obbligato ad assicurare specifiche garanzie, tra cui la possibilità di intervento umano, il diritto dell'interessato di esprimere la propria opinione e di contestare la decisione. Inoltre, l'articolo vieta che decisioni automatizzate di questo tipo si basino su categorie particolari di dati personali, come quelli relativi alla salute o alle convinzioni religiose, salvo talune eccezioni accompagnate da ulteriori misure di protezione.

²¹² Trattasi di una particolare intelligenza artificiale, dotata della capacità di interpretare il linguaggio umano, riconoscere immagini e apprendere dai dati, in grado di produrre output quali testo, immagini, ecc.

²¹³ Cfr. provvedimento del 2 febbraio 2023.

successivamente implementato dal titolare continuava, al momento del provvedimento sanzionatorio, ad essere carente sotto molteplici aspetti. Per tali ragioni, oltre alla sanzione, l'Autorità ha ingiunto alla società di conformare i trattamenti alle disposizioni del Regolamento.

Poco dopo l'Autorità è intervenuta per disporre anche l'ulteriore blocco urgente di un'applicazione di intelligenza artificiale generativa per varie ragioni, tra le quali la mancanza di meccanismi di verifica dell'età. In particolare, nonostante la stessa indicasse di rivolgersi a utenti di età superiore ai 13 anni, il Garante ha rilevato l'assenza di meccanismi effettivi per la verifica dell'età, esponendo così i minori a rischi legati all'accesso a contenuti inappropriati e alla raccolta illecita di dati personali²¹⁴. La Società, anche sulla scorta di quanto affermato nel frattempo dal Comitato europeo per la protezione dei dati (EDPB) con parere adottato sull'uso dei dati personali per lo sviluppo e la diffusione di modelli di IA²¹⁵, è stata successivamente sanzionata dall'Autorità²¹⁶.

Sempre l'Autorità italiana ha contribuito all'approvazione, nell'ottobre 2024, delle dichiarazioni su IA e minori nell'ambito del G7 tra Garanti²¹⁷.

In questo contesto, il 13 giugno 2024 è stato approvato il Regolamento (UE) 2024/1689, noto anche come "AI Act".

Il Regolamento, si propone di stabilire norma armonizzate sull'intelligenza artificiale, prevede un'applicazione graduale delle sue disposizioni²¹⁸ e stabilisce

²¹⁴ Cfr. provvedimento del 30 marzo 2023. Con successivo provvedimento dell'11 aprile 2023, l'Autorità – a fronte delle informazioni acquisite e della disponibilità manifestata dalla Società a porre in essere una serie di misure concrete a tutela dei diritti e delle libertà degli interessati, i cui dati sono stati trattati per l'addestramento degli algoritmi strumentali all'erogazione del servizio – ha autorizzato a procedere alla rivalutazione della sussistenza dei presupposti del provvedimento di limitazione provvisoria, adottando le conseguenti determinazioni, a condizione che la Società provvedesse ad attuare concretamente una serie di misure e prescrizioni specificamente individuate, che venivano ingiunte alla Società ai sensi dell'art. 58, par. 2, lett. d), del Regolamento. Con riferimento ai minori, in particolare, si legge che *“in sede di eventuale riattivazione del servizio dall'Italia, inserire la richiesta, a tutti gli utenti che si collegano dall'Italia, ivi inclusi quelli già registrati, di superare, in sede di primo accesso, un age gate che escluda, sulla base dell'età dichiarata, gli utenti minorenni; 8. sottoporre al Garante, entro il 31 maggio 2023, un piano per l'adozione di strumenti di age verification idoneo a escludere l'accesso al servizio agli utenti infratredicenni e a quelli minorenni in assenza di un'espressa manifestazione di volontà da parte di chi esercita sugli stessi la responsabilità genitoriale. L'implementazione di tale piano dovrà decorrere, al più tardi, dal 30 settembre 2023”*.

²¹⁵ Cfr. parere n. 28/2024 sugli aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA. Il parere è stato richiesto dall'Autorità irlandese per la protezione dei dati (DPA) al fine di conseguire l'armonizzazione normativa a livello europeo.

²¹⁶ Tra le motivazioni della sanzione si rinviene anche il fatto che la Società titolare del modello *“non avrebbe previsto meccanismi per la verifica dell'età, con il conseguente rischio di esporre i minori di 13 anni a risposte inadeguate rispetto al loro grado di sviluppo e autoconsapevolezza”*. Il Tribunale di Roma, sez. XVIII civ., ha disposto, con ordinanza del 21 marzo 2025, la sospensione cautelare del provvedimento, subordinatamente alla prestazione di cauzione, nel procedimento iscritto al n. R.G. 4785/2025.

²¹⁷ Statement on AI and Children, 11 October 2024.

²¹⁸ In particolare, la scansione è la seguente: 1° agosto 2024, entrata in vigore del Regolamento; 2 febbraio 2025, applicazione delle disposizioni relative ai sistemi vietati e agli obblighi di

una serie chiara di norme basate sul rischio²¹⁹ per gli sviluppatori e i deployer di IA per quanto riguarda gli usi specifici dell'IA.

Il Regolamento non contiene, in effetti, disposizioni dedicate specificamente ai minori. Molto raramente (6 volte per la precisione) si rinviene nel lungo testo un riferimento ai soggetti minori. Sebbene il testo non li menzioni esplicitamente, le sue disposizioni implicano una protezione indiretta per questa fascia di utenti vulnerabili.

Anzitutto, il Regolamento vieta pratiche di IA che manipolano le decisioni delle persone o sfruttano le loro vulnerabilità, come la profilazione basata su comportamenti sociali o tratti personali. Tali pratiche sono particolarmente rischiose per i minori, che sono più suscettibili a influenze esterne. Pertanto, sebbene non vi sia una menzione esplicita, queste disposizioni contribuiscono indirettamente alla protezione dei minori dall'uso improprio dell'IA.

Inoltre, i sistemi ad alto rischio, come quelli utilizzati in ambiti educativi, sanitari o per la selezione del personale, sono soggetti a requisiti più stringenti. Anche se non vi è un riferimento diretto ai minori, l'applicazione di questi sistemi in contesti che coinvolgono minori implica l'adozione di misure preventive per garantire la loro protezione.

Quanto alla normativa nazionale, è stata di recente approvata la Legge n. 132 del 2025, Legge italiana sull'intelligenza artificiale. La legge introduce una norma specifica per la tutela dei minori nell'uso dell'intelligenza artificiale. In particolare, stabilisce che i minori di 14 anni possano accedere a tecnologie di IA e al relativo trattamento dei dati personali solo con il consenso di chi esercita la responsabilità genitoriale, in conformità al GDPR e al Codice Privacy. I minori tra i 14 e i 18 anni, invece, possono prestare autonomamente il proprio consenso, a condizione che le informazioni fornite siano facilmente accessibili e comprensibili. Il testo sottolinea inoltre l'obbligo di garantire una comunicazione chiara e semplice sui rischi connessi all'uso dell'IA, così da assicurare la consapevolezza degli utenti e il loro diritto di opporsi al trattamento dei dati²²⁰.

Sempre partendo dalla circostanza per cui è evidente la diffusione di sistemi di intelligenza artificiale anche tra i minori, il 30 novembre scorso, il Garante per la protezione dei dati personali ha pubblicato la versione aggiornata del vademecum "La scuola a prova di privacy", che affronta le tematiche connesse al trattamento

alfabetizzazione sull'IA; 2 agosto 2025, applicazione delle norme di *governance* e degli obblighi per i modelli di IA generali; 2 agosto 2026, applicazione delle disposizioni per la maggior parte dei sistemi di IA ad alto rischio; 2 agosto 2027, applicazione delle disposizioni per i sistemi di IA ad alto rischio incorporati in prodotti regolamentati.

²¹⁹ Per un approfondimento sull'approccio basato sul rischio cfr. G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024, *passim*.

²²⁰ Cfr. art. 4, comma 4, l. n. 132/2025. Tale disposizione, come precisato nel dossier n. 289 del Servizio studi del Senato n. 1146 Disposizioni e deleghe al Governo in materia di intelligenza artificiale - A.S. n. 1146 del 27 giugno 2025, ricalca la disciplina prevista dall'art. 2-*quinquies* del codice privacy sul consenso del minore in materia di protezione dei dati personali.

dei dati personali nelle istituzioni scolastiche, anche alla luce dei nuovi strumenti di intelligenza artificiale.

Se da un lato i modelli e i sistemi di intelligenza artificiale pongono evidenti rischi quando vengono utilizzati dai minori, dall'altro tali tecnologie avanzate possono offrire importanti opportunità a sostegno dei soggetti più vulnerabili.

In particolare, nei documenti che analizzano i possibili metodi di implementazione dei sistemi di *age assurance*, l'intelligenza artificiale è spesso menzionata come strumento utile in questo ambito, soprattutto con riferimento alle tecniche di *age estimation*.

La stima dell'età comprende, infatti, l'insieme di metodi volti a determinare, con un certo grado di probabilità, l'età di un utente, la fascia di età a cui appartiene oppure se sia maggiore o minore di una determinata soglia.

Queste tecniche possono basarsi sull'analisi automatizzata di dati comportamentali e contestuali, osservando ad esempio il modo in cui un utente interagisce con un dispositivo o con altri soggetti della stessa età. Possono inoltre includere l'elaborazione di metriche relative ai movimenti corporei, il riconoscimento facciale, o l'analisi delle competenze e delle conoscenze dimostrate. Rientrano tra i metodi di stima dell'età anche quelli che si avvalgono di algoritmi e di soluzioni fondate su tecnologie di intelligenza artificiale.

Una serie di piattaforme ha implementato questo tipo di sistemi.

Tra le altre, in un'iniziativa volta a rafforzare le salvaguardie digitali per la sua utenza giovanile, YouTube ha intrapreso l'implementazione di una tecnologia di stima dell'età basata sull'apprendimento automatico. Tale sistema è progettato per discernere tra utenti minorenni e adulti, garantendo la fruizione di esperienze di prodotto adeguate all'età e l'applicazione di protezioni specifiche²²¹. L'approccio metodologico prevede l'impiego di intelligenza artificiale per analizzare una pluralità di segnali comportamentali – inclusi i tipi di contenuti cercati, le categorie di video visualizzati e la longevità dell'account – al fine di inferire se un utente sia maggiore o minore di diciotto anni. Questa inferenza algoritmica opererà indipendentemente dalla data di nascita dichiarata nell'account. Qualora il sistema identifichi un utente come minorenne, verranno automaticamente attivate specifiche misure di protezione e personalizzazione, tra cui: la disabilitazione della pubblicità personalizzata, l'attivazione di strumenti per il benessere digitale e l'introduzione di salvaguardie nelle raccomandazioni, con particolare riferimento alla limitazione di visualizzazioni ripetitive di determinati generi di contenuto. È altresì contemplato un meccanismo di rettifica per i casi di stima errata: gli utenti ritenuti erroneamente minorenni avranno la facoltà di verificare la propria maggiore età attraverso documenti identificativi ufficiali, quali carta di credito o documento

²²¹ Cfr. Extending our built-in protections to more teens on YouTube official blog. Questa implementazione, inizialmente introdotta per un ristretto gruppo di utenti negli Stati Uniti, sarà oggetto di un attento monitoraggio prima di una sua espansione progressiva su scala più ampia negli USA e, successivamente, in altri mercati internazionali.

governativo. Solamente gli utenti la cui età sia stata inferita o verificata come superiore ai diciotto anni avranno accesso a contenuti con restrizioni d'età potenzialmente inappropriati per fasce di pubblico più giovani.

Risulta, peraltro, dai pareri resi con riferimento al Regolamento adottato dall'AGCOM sul tema, che l'Autorità per la protezione dei dati italiana sia favorevole all'implementazione di tale tipo di sistemi di stima dell'età²²².

Un esempio, differente ma comunque significativo delle potenzialità dell'intelligenza artificiale a beneficio dei minori, è l'iniziativa di Google LLC, che, come riportato dal *New York Times*, ha scelto di rendere disponibile il sistema Gemini anche ai ragazzi sotto i tredici anni per finalità di studio²²³. In particolare, l'iniziativa prevede l'estensione dell'accesso al sistema di intelligenza artificiale anche a utenti di età inferiore ai tredici anni, purché titolari di un account gestito attraverso la piattaforma di parental control Family Link. Il modello delineato consente al minore di abilitare autonomamente il servizio, con successiva notifica ai genitori o ai titolari della responsabilità genitoriale, ai quali è riconosciuta la facoltà di disattivare l'accesso. Google ha precisato che, per tali account, i dati personali dei minori non saranno utilizzati per l'addestramento dei modelli algoritmici e che l'interazione con Gemini avverrà in un contesto dotato di specifiche misure di salvaguardia volte a ridurre l'esposizione a contenuti non appropriati.

9. Prime considerazioni conclusive su tutela e prospettive dell'identità digitale del minore.

Ebbene, risulta a questo punto possibile svolgere alcune prime considerazioni conclusive con specifico riferimento all'identità del minore negli ambienti digitali.

Può essere utile mantenere la dicotomia tra identità “sostanziale” e “anagrafica” utilizzata nell'ambito dell'intera trattazione.

Dal punto di vista dell'identità “sostanziale” del minore, essa è stata analizzata in questo capitolo non solo sotto il profilo del diritto a essere sé stessi e a essere correttamente rappresentati, anche nell'ambiente digitale, ma anche in relazione ai fenomeni del “sharenting” e dei “baby influencer”, intesi come questioni che implicano il diritto all'autodeterminazione del minore nella

²²² Si legge, infatti, nel parere finale sullo schema di provvedimento AGCOM recante la disciplina relativa alle modalità tecniche e di processo che i soggetti individuati dalla norma sono tenuti ad adottare per la verifica della maggiore età degli utenti, ai sensi della l. 13 novembre 2023, n. 159 (c.d. AGE VERIFICATION) del 17 luglio 20 che “avuto riguardo al parere reso in merito alla citata deliberazione AGCOM relativa all'avvio della consultazione pubblica (provvedimento n. 88 dell'8 febbraio 2024) con il quale il Garante aveva posto l'attenzione sull'opportunità di far riferimento anche ai metodi di stima dell'età effettuati mediante algoritmi e il ricorso a tecnologie basate sull'intelligenza artificiale in relazione alla definizione di “Age estimation”.

²²³ Cfr. *New York Times* del 2 maggio 2025, *Google Plans to Roll Out Its A.I. Chatbot to Children Under 13*.

costruzione della propria identità e nella gestione consapevole della propria presenza nella dimensione digitale.

Sul punto non può che ribadirsi come, anche in questo caso, nelle more dell'adozione di normative specifiche di cui, come si è visto, esistono diverse proposte, l'identità sostanziale del minore sia divenuta totalmente appannaggio della normativa in materia di protezione dei dati personali e della relativa Autorità. L'Autorità garante per la protezione dei dati personali si è prodigata, oltre che in provvedimenti, in iniziative di ogni sorta volte alla sensibilizzazione e alfabetizzazione sul tema, prima di tutto, dei genitori.

Quanto alle proposte legislative sul tema, al di là della loro provenienza politica, esse appaiono, a parere della scrivente, indicative della marcata confusione che persiste in merito ai principi fondamentali da porre a fondamento di normative di questo tipo, ossia ai valori e criteri ispiratori. In altre parole, non risulta chiaro quale sia l'obiettivo finale del legislatore italiano rispetto a questioni centrali per una regolamentazione coerente in materia, quali: l'età del consenso, che nelle diverse proposte oscilla tra i tredici e i sedici anni; il divieto o la liberalizzazione di pratiche come quella dei "baby influencer"; i limiti allo "sharenting", ambito nel quale sembra mancare la determinazione necessaria a definire una posizione netta e univoca. L'esperienza francese esaminata conduce a considerazioni analoghe, pur distinguendosi per la presenza di una normativa già approvata e attualmente in corso di applicazione; quindi, su cui la politica ha trovato un compromesso. Ciò risulta particolarmente evidente con riferimento ddl n. 1136 del 2024, attualmente in fase istruttoria presso la Commissione VIII del Senato.

Quanto all'identità "anagrafica", è stata qui presa in esame in relazione all'identificazione del minore e alle politiche legate all'identificazione finalizzata alla verifica dell'età.

Gli strumenti di verifica dell'età, attualmente incentivati a livello europeo, rivestono, in generale, un ruolo centrale, in quanto consentono di accertare la maggiore o minore età degli utenti e, di conseguenza, di regolare l'accesso a contenuti e servizi online. L'analisi ha evidenziato come tale *favor* delle istituzioni europee per tale soluzione non derivi da un approccio paternalistico o da un intento di controllo di massa, ma rappresenti piuttosto una risposta fondata su dati empirici tratti da numerosi studi condotti da esperti di diversi settori, che non possono più essere trascurati. Del resto, la trattazione ha preso in considerazione anche gli anni precedenti, in cui le istituzioni europee hanno evitato di intervenire, con conseguenze – drammatiche per i minori – ormai evidenti. In tale prospettiva, come si è visto, le istituzioni europee promuovono con determinazione strumenti di verifica dell'età conformi al DSA e alle Linee guida di attuazione, le quali adottano un approccio equilibrato tra la tutela dei minori e le esigenze operative dei gestori di siti e piattaforme. La normativa europea, inoltre, non demonizza specifici contenuti, quali quelli pornografici, ma adotta un approccio orizzontale volto a

scoraggiare l'accesso dei minori a tutta una serie di contenuti ritenuti inappropriati o potenzialmente pericolosi.

Anche da uno sguardo al contesto internazionale, sul quale volutamente non ci si è soffermati, emerge che, alla luce dei dati allarmanti presi in esame nella presente analisi, molti Paesi hanno preso la via della verifica dell'età per garantire il rispetto del divieto di accesso ai servizi di *social networking* sotto una determinata età. Si pensi alla normativa approvata in Australia, pienamente efficace dal 10 dicembre 2025, che prevede un divieto assoluto di accedere ai *social network* per i minori di sedici anni²²⁴. Si noti, peraltro, che l'Australia non ha inteso trovare un punto di equilibrio con i gestori delle piattaforme, che sono tenuti a implementare meccanismi efficaci di verifica dell'età e che saranno ritenuti gli unici responsabili in caso di violazione del divieto da parte dei minori²²⁵. Nello Stato del Texas, addirittura, se dovesse essere approvato in via definitiva l'House Bill 186 (HB 186), i *social network* saranno vietati ai minori di diciotto anni, qualificati indistintamente nel testo normativo come "children"²²⁶.

Ciò posto, si ritiene che l'impiego di sistemi di verifica dell'età, in ogni caso, non debba mai limitarsi a mero approccio tecnico di filtraggio dei contenuti,

²²⁴ Nel corso del 2024 il governo australiano ha avviato un articolato processo legislativo finalizzato a introdurre, mediante una modifica dell'Online Safety Act 2021, un'età minima obbligatoria per l'accesso alle principali piattaforme di social media. Tale iniziativa ha condotto, nel 2025, alla definizione della nuova Part 4A – Social Media Minimum Age, destinata a entrare in vigore il 10 dicembre 2025. La disciplina prevede che i fornitori di servizi di social networking siano tenuti a impedire la creazione e il mantenimento di account da parte di soggetti di età inferiore ai sedici anni, adottando sistemi di *age assurance* idonei a verificarne l'età. Analoga scelta è stata fatta dalla Malesia con l'Online safety Act 2025, che verrà implementato nel corso del 2026.

²²⁵ L'obbligo ricade integralmente sulle piattaforme, cui è imposto di implementare "misure ragionevoli" di accertamento, pena l'applicazione di sanzioni pecuniarie di rilevante entità. L'inottemperanza a tali obblighi, infatti, espone i gestori delle piattaforme a conseguenze sanzionatorie particolarmente severe: l'autorità competente, l'eSafety Commissioner, è infatti legittimata a irrogare sanzioni amministrative pecuniarie che possono raggiungere importi molto elevati, fino a 49,5 milioni di dollari australiani o, alternativamente, una percentuale significativa del fatturato annuo globale dell'impresa, secondo il criterio che risulti maggiormente dissuasivo. Oltre alle sanzioni pecuniarie, il quadro normativo prevede anche la possibilità di emanare *enforcement notices* e *compliance notices*, imponendo al gestore di adottare senza indugio misure correttive specifiche, nonché la facoltà, nei casi di reiterata o grave violazione, di disporre ordini di cessazione del servizio o di imporre restrizioni operative sul territorio australiano.

²²⁶ Lo Stato del Texas ha adottato un approccio normativo rigoroso in materia di accesso dei minori ai servizi di social networking. Il House Bill 186 (HB 186) prevede un divieto per soggetti di età inferiore ai diciotto anni, imponendo alle piattaforme obblighi stringenti di verifica dell'età (*age verification*) e responsabilità diretta, con sanzioni pecuniarie e intervento del Procuratore Generale in caso di inosservanza, inquadrabili nelle pratiche commerciali ingannevoli (*deceptive trade practices*). In parallelo, lo SCOPE Act istituisce strumenti di controllo genitoriale, obblighi di trasparenza e limitazioni alla fruizione di contenuti dannosi per i minori, nonché misure di protezione dei dati personali. L'analisi congiunta di tali iniziative evidenzia una strategia normativa bifronte: una regolazione proibitiva, volta a escludere i minori dall'accesso diretto ai social, e una regolazione funzionale, finalizzata a rafforzare la tutela dei minori e il controllo genitoriale senza divieto assoluto. L'approccio texano mira a proteggere i minori dai rischi digitali ma è suscettibile di profili di illegittimità costituzionale in relazione alla libertà di espressione del primo emendamento. Alla data del dicembre 2025, HB 186 ha superato la Camera ma è pendente presso il Senato, mentre alcune disposizioni del SCOPE Act sono state sospese giudizialmente.

ma piuttosto essere inserito in una strategia complessiva volta a favorire l'avvicinamento e l'uso consapevole e responsabile delle tecnologie digitali da parte dei minori. In questa prospettiva, l'attenzione dovrebbe concentrarsi non solo sul rispetto formale delle regole ma soprattutto sulla effettiva comprensione del minore circa il trattamento dei propri dati personali, le implicazioni sui diritti fondamentali e la potenziale irreversibilità di alcune scelte effettuate online.

Si aggiunge che la scelta di tale strumento deve essere integrata con politiche di alfabetizzazione digitale dei minori, finalizzate a sviluppare competenze critiche, consapevolezza dei rischi e capacità di gestione autonoma delle informazioni digitali. In questo senso, il citato documento elaborato nell'ottobre 2024 dal G7 delle Autorità garanti per la protezione dei dati, che si sofferma lungamente sulla “*digital literacy*”, offre indicazioni concrete su iniziative educative e preventive, sebbene il suo ambito sia, al momento, concentrato prevalentemente su una prospettiva *privacy-oriented*²²⁷. Il modello di combinare protezione e educazione digitale trova già riscontro in alcune normative europee, come dimostra l'AI Act²²⁸, che riconosce come fondamentale l'AI Literacy per qualsiasi approccio all'utilizzo dell'intelligenza artificiale.

Del resto, anche a distanza di pochi mesi dall'entrata in vigore del complesso dei testi normativi europei presi in esame nella presente trattazione, sono già emersi tutti i limiti legati alla loro applicazione. Al momento in cui si scrive, con risoluzione non vincolante, il Parlamento europeo ha espresso fortissime preoccupazioni alla luce dei dati emersi nel 2025²²⁹ e chiesto un'applicazione più rigorosa del Digital services Act. In particolare, pur salutando con favore gli sforzi della Commissione per sviluppare una app dell'Ue per la verifica dell'età e il portafoglio europeo di identità digitale, i parlamentari sottolineano che i sistemi di garanzia dell'età devono essere accurati e rispettare la privacy e che, in ogni caso, non sollevano le piattaforme dalla responsabilità di garantire che i loro prodotti siano sicuri e appropriati per i minori.

²²⁷ Cfr. Statement on AI and Children, 11 October 2024.

²²⁸ Cfr. art. 4 AI Act, recante “*Alfabetizzazione in materia di IA*” si prevede che “*I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati*”.

²²⁹ Il 97% degli adolescenti accede a internet quotidianamente e il 78% dei ragazzi tra i 13 e i 17 anni consulta i propri dispositivi almeno una volta ogni ora. Parallelamente, un giovane su quattro manifesta un utilizzo dello smartphone definibile come “problematico” o “disfunzionale”, caratterizzato da schemi comportamentali assimilabili a forme di dipendenza. Stando ai dati dell'eurobarometro 2025, oltre il 90% dei cittadini europei considera prioritario adottare misure di tutela per i minori nel contesto digitale. Le principali preoccupazioni riguardano l'impatto potenzialmente nocivo dei social media sul benessere psicologico dei giovani (93%), la diffusione del cyberbullismo (92%) e l'esigenza di disporre di strumenti realmente efficaci per limitare l'accesso a contenuti non adeguati alla loro età (92%).

Peraltro, anche nel contesto sovranazionale, emerge con evidenza una certa confusione e parziale sovrapposizione tra tutte le normative recentemente approvate. Si rinvia ai capitoli precedenti per quanto riguarda l'ipertrofia normativa sul tema delle tecnologie e le esigenze di semplificazione attualmente emerse. In tale contesto, il minore, che gode già di una protezione specifica per via del suo *status*, assume anche - rispetto ai servizi digitali - i ruoli di "utente", "interessato" e "consumatore", nonché di "utilizzatore", se questi ultimi sono anche basati su sistemi di intelligenza artificiale. Come anticipato, ad esempio, è molto pervasivo il ruolo assunto nella tutela dei minori nella dimensione digitale dall'Autorità garante per la protezione dei dati personali in Italia. 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, come rilevato nell'ambito della presente analisi, solo 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 a livello nazionale e sovranazionale può 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.

Con specifico riferimento al contesto italiano, si riscontrano serie criticità legate alla qualità della regolazione. Dopo anni di sostanziale disinteresse sul tema da parte del Legislatore e in cui l'unico strumento dedicato ai minori e solo per l'accesso ad alcuni servizi pubblici era SPID minori, si è registrato un netto cambio di rotta con il "Decreto Caivano". Tale Decreto, adottato dall'attuale Governo, assumendo un approccio di tipo prevalentemente repressivo (è previsto il divieto di accesso a contenuti pornografici ma non altre misure di accompagnamento) e al contempo settoriale (si tratta dei soli contenuti pornografici), rischia di non fornire una risposta adeguata ai reali pericoli che incombono sui minori nell'ambiente digitale.

Allo stato, permangono grossi dubbi sulla efficacia delle misure introdotte dal "Decreto Caivano" e dal conseguente Regolamento AGCOM²³⁰ e sulle criticità già riscontrate nella loro applicazione, oltre che sulla legittimità delle stesse.

²³⁰ Diverse sono le questioni che si pongono sul tema dell'efficacia. Da un lato, la verifica dell'età prevista dalla normativa italiana impone agli operatori di mercato di adeguarsi in tempi ristretti e con costi significativi, in un contesto in cui i requisiti tecnico-organizzativi restano ancora non definiti nel dettaglio. Dall'altro, l'efficacia delle misure appare limitata: i minori possono infatti aggirare agevolmente i blocchi tramite VPN o altri strumenti, con il rischio di spostarsi verso piattaforme non regolamentate e quindi maggiormente pericolose. Inoltre, l'obbligo rischia di introdurre barriere all'ingresso che penalizzano l'innovazione e la competitività delle startup digitali. Per la valutazione di sistemi alternativi, cfr. V. Natale, *Tutela dei minori online: possibili soluzioni per un'accurata verifica dell'età*, in *Agenda Digitale.eu*, 6 giugno 2024.

Sarebbe auspicabile che il Legislatore – o, in sua vece, il Governo – non si limitasse a interventi dettati dall’urgenza del momento, come accaduto con il “Decreto Caivano”, o circoscritti a singoli settori, ma che piuttosto orientasse la sua azione verso una strategia complessiva e integrata di gestione dei rischi legati al digitale, con particolare attenzione anche ad altri fenomeni di grande impatto sociale, come, ad esempio, il gioco d’azzardo online. Un approccio regolatorio di tipo emergenziale, piuttosto che sistematico e strutturale, a un fenomeno come quello in oggetto – che è tutt’altro che episodico o contingente, ma anzi, come si è visto, stabile e strutturale nella società digitale contemporanea – si rivela chiaramente nella scelta dello strumento della decretazione d’urgenza²³¹. Tale modalità, concepita dal costituente come eccezionale e limitata a situazioni straordinarie di necessità e urgenza, tradisce in questo caso una mancanza di visione strategica e di coordinamento normativo, con il rischio di produrre soluzioni parziali e disallineate rispetto sia al diritto europeo sia agli standard internazionali di tutela dei minori nel contesto digitale. La stessa AGCOM ha fortemente raccomandato di estendere gli obblighi relativi alla verifica dell’età previsti dal “decreto Caivano” anche ad altre tipologie di contenuti, ulteriori rispetto a quelli di carattere pornografico, che risultano comunque potenzialmente pregiudizievoli per lo sviluppo fisico, psichico o morale dei minori²³². La questione della qualità della regolazione, come noto, non si esaurisce in un profilo di mera opportunità politica, ma investe anche la legittimità degli atti normativi. Come si è tentato di mettere in luce nella presente trattazione, sono numerosi i disallineamenti tra il quadro normativo europeo e quello italiano, pur in presenza della clausola di cedevolezza prevista dalla normativa interna²³³. Si profila, inoltre, per quanto il contesto sia parzialmente diverso, il rischio di ripetere in fase di applicazione la vicenda francese, almeno per gli operatori stabiliti al di fuori dell’Italia. Come esposto, ci sono forti dubbi, infatti, sulla compatibilità con la normativa sovranazionale in tema del “paese di origine” di normative, come quella italiana, che impongono nuovi oneri a carico di fornitori di servizi della società dell’informazione stabiliti al di fuori dello Stato. Il citato disegno di legge sulla tutela dei minori online – attualmente in fase di discussione presso l’VIII Commissione del Senato – poi, rischia di stratificare ulteriormente il quadro, introducendo nuove regole che non risultano coerenti con tutta la normativa già vigente a livello nazionale e sovranazionale.

²³¹ Sulla illegittimità costituzionale di decreti-legge emanati in assenza dei presupposti previsti dall’art. 77 Cost, cfr. Corte cost. 28 gennaio 1995, n. 29; Id. 2 maggio 2007, n. 171; Id. 25 settembre 2019, n. 226.

²³² Cfr. allegato A alla delibera n. 96/25/CONS recante “Modalità tecniche e di processo per l’accertamento della maggiore età degli utenti ai fini dell’accesso a determinati servizi forniti dai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, ai sensi dell’articolo 13-bis del decreto-legge 5 settembre 2023, n. 123 convertito con modificazioni dalla legge 13 novembre 2023, n. 159”

²³³ Cfr. delibera n. 96/25/CONS sulla “Adozione delle modalità tecniche e di processo per l’accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159”.

Infine, come anticipato anche con riferimento alla regolazione europea, si ritiene che la verifica dell'età, senza una parallela incentivazione di altre misure educative, contribuisca a consolidare un approccio prevalentemente repressivo, anziché promuovere una reale cultura dell'educazione digitale. A questo proposito, al momento in cui si scrive, è in fase di discussione un disegno di legge di iniziativa governativa contenente disposizioni sul consenso informato in ambito scolastico per tutte le attività extracurricolari e gli ampliamenti dell'offerta formativa, riguardanti in particolare tematiche attinenti all'ambito sessuale²³⁴. L'Italia, poi, è tra i pochissimi Paesi in Europa a non prevedere educazione sessuale obbligatoria nelle scuole, nonostante i dati dimostrino, tra le altre cose, che un'educazione completa alle relazioni e alla sessualità aiuta a prevenire la violenza contro le donne²³⁵. In questo quadro, va colto come segnale positivo l'art. 14 del “decreto Caivano”, che, almeno sulla carta, interviene cercando di riequilibrare l'impianto normativo, spostando l'attenzione anche sulla promozione di competenze digitali e mediatiche tra minori, famiglie ed educatori. Esso prevede infatti l'elaborazione di linee guida per un uso sicuro dei dispositivi digitali, il rafforzamento del ruolo dei Centri per la famiglia nell'offrire servizi di alfabetizzazione e supporto, nonché l'avvio di campagne informative annuali dedicate all'uso consapevole della rete e alla prevenzione dell'esposizione a contenuti nocivi. Accanto agli strumenti repressivi, vengono quindi introdotte misure orientate alla formazione e alla responsabilizzazione, supportate da un sistema di monitoraggio annuale affidato all'AGCOM e all'autorità politica competente relativamente all'impatto delle misure repressive introdotte con gli artt. 13 e 13-*bis* del decreto. Sebbene tali previsioni rappresentino un passo verso un approccio più educativo e sistemico, la loro efficacia dipenderà dalla capacità delle istituzioni di integrarle realmente nelle politiche rivolte ai minori e di supplire alle carenze strutturali, come l'assenza di un'educazione sessuale obbligatoria nel contesto scolastico. Anche alla luce di quanto rilevato nel Capitolo II con riferimento ai diritti digitali, occorrerebbe dare attuazione all'art. 8 CAD che, nel prevedere che lo Stato e i soggetti di cui all'art. 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini, si rivolge più specificamente ai minori e alle categorie a rischio di esclusione.

Risulta doveroso, infine, provare a rispondere agli ulteriori quesiti di ricerca posti alla base del presente capitolo.

L'analisi condotta conferma la centralità del principio del *best interest of the child* (BIC) come criterio guida per la regolazione dell'accesso dei minori ai servizi digitali, ma – alla luce delle trasformazioni indotte dalle tecnologie digitali e dall'intelligenza artificiale – si rileva la necessità di aggiornarne la nozione.

²³⁴ Si tratta di ddl AC 2423-A.

²³⁵ <https://www.unesco.org/en/articles/international-technical-guidance-sexuality-education-evidence-informed-approach>.

In particolare, tale principio, storicamente sviluppato nel diritto internazionale e nazionale in ambito fisico e sociale, sta subendo una progressiva estensione al dominio digitale. Tradizionalmente, il BIC si concentrava sulla tutela della salute, dell'istruzione e della sicurezza dei minori, nonché sulla partecipazione alle decisioni che li riguardano. Nell'era digitale, il principio si declina anche nella protezione dell'identità digitale, nella gestione dei dati personali e nella sicurezza online, affrontando rischi prima inesistenti come la profilazione automatizzata, l'esposizione a contenuti nocivi o l'interazione con soggetti potenzialmente pericolosi.

Questa evoluzione implica un approccio multilivello: il BIC non garantisce più solo protezione passiva, ma promuove anche l'alfabetizzazione digitale e l'acquisizione di competenze critiche sui dati e sulle tecnologie. In tal modo, si favorisce l'autonomia responsabile dei minori, senza escludere l'intervento delle famiglie, delle istituzioni educative e delle piattaforme tecnologiche nella progettazione di servizi *child-centered* e *privacy-by-design*.

Inoltre, la dimensione digitale del BIC integra protezione e partecipazione, riconoscendo ai minori il diritto all'informazione chiara sul trattamento dei dati, la possibilità di esprimere preferenze sull'accesso ai contenuti online e il supporto educativo necessario per un'interazione sicura con le tecnologie. L'obiettivo, dunque, non è solo proteggere i minori dai rischi immediati, ma garantire uno sviluppo equilibrato della loro identità digitale e della capacità di interazione autonoma e consapevole con le piattaforme online.

Per rendere effettiva tale tutela, tuttavia, si ritiene sia indispensabile riconsiderare anche la nozione di "trasparenza". L'approccio tradizionale, basato sulla mera trasparenza formale che abbiamo visto fallire in materia di protezione dei dati personali²³⁶, si è dimostrato insufficiente a proteggere i minori, in quanto non sembra consentire una reale comprensione dei rischi né la partecipazione attiva alla gestione dei propri dati. La trasparenza deve quindi essere reinterpretata come uno strumento operativo, che renda accessibili e comprensibili i processi decisionali

²³⁶ Il Regolamento n. 2016/679/UE attribuisce apparentemente grande rilievo alla trasparenza. Inoltre, il Regolamento impone al titolare di comunicare in modo chiaro e trasparente all'interessato i diritti che gli spettano. In particolare, i diritti *conoscitivi* dell'interessato includono: il diritto a ricevere ogni informazione utile circa i trattamenti che coinvolgono i suoi dati (cfr. artt. 13 e 14 GDPR), attraverso un documento (c.d. "informativa sul trattamento dei dati personali" o "informativa privacy") che deve includere le informazioni sull'identità e i dati di contatto del titolare e del responsabile, sulle finalità del trattamento, sugli eventuali destinatari a cui sono comunicati i dati e se il titolare del trattamento sia intenzionato a comunicare tali dati a Paesi terzi non appartenenti all'Unione europea; il titolare deve indicare il periodo di conservazione (o i criteri per determinare tale periodo), il diritto dell'interessato di chiedere l'accesso, il diritto di revocare il consenso, le possibili conseguenze della mancata comunicazione dei dati quando questi siano raccolti per dare esecuzione ad un contratto, se è eventualmente svolta attività di profilazione; il diritto di accesso, ossia il diritto di ottenere dal titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, il diritto di ottenere l'accesso ad una serie di informazioni indicate dall'art. 15 del Regolamento; il diritto alla comunicazione (art. 34) in caso di violazione dei dati personali che lo riguardano.

automatizzati e le implicazioni del trattamento dei dati personali sui diritti fondamentali dei minori.

In conclusione, la verifica dell'età, da sola, non può costituire una soluzione esaustiva.

Considerazioni di sintesi della ricerca

A questo punto dello studio è possibile provare a svolgere alcune prime riflessioni conclusive sul tema oggetto della presente trattazione.

La ricerca ha tentato di offrire, anzitutto, una ricostruzione dell'identità personale nella sua accezione giuridica, dalla sua emersione in dottrina e nella prima giurisprudenza fino alla codificazione e agli sviluppi più recenti.

In particolare, sull'identità personale si è osservato, con riferimento alla declinazione “sostanziale”, che la stessa si è sviluppata inizialmente in dottrina e nella prima giurisprudenza come diritto a essere correttamente rappresentati, per poi evolversi, nella giurisprudenza costituzionale, nel diritto ad essere sé stessi. Più precisamente, si è analizzata la genesi di entrambe le accezioni dell'identità “sostanziale”, che possiamo definire rispettivamente “esterna” e di matrice civilistica, e “interna” e di matrice costituzionalistica. La prima, delineata dalla Corte di Cassazione nel 1985, riguarda il diritto a essere rappresentati correttamente nella propria dimensione sociale. La seconda, più introspettiva, è quella indicata dalla Corte costituzionale nella sentenza n. 13 del 1994 come diritto ad essere sé stessi. In particolare, quando si discute di “identità” dal punto di vista costituzionale, si fa riferimento soprattutto ai cosiddetti “nuovi diritti”, sviluppati dalla Corte costituzionale e ricondotti, attraverso l'interpretazione combinata degli artt. 2, 3 e 13 della Costituzione, ai diritti fondamentali della persona. Analogo percorso è stato seguito dalla Corte EDU, a partire dalla Convenzione europea dei diritti dell'uomo.

Considerata l'espansione del contenuto di questo diritto, si è quindi cercato – in parte facendo riferimento alle classificazioni proposte dalla dottrina più recente e in parte sviluppando ricostruzioni alternative – di sintetizzare i diversi diritti che, nel tempo, sono stati ricondotti all'identità personale, soprattutto in ambito giurisprudenziale. Ci si è inoltre soffermati sui diritti ricondotti all'identità personale dal legislatore o dalla dottrina. In tal senso, è consueto parlare di “diritti di identità personale” al plurale, piuttosto che di “diritto di identità personale”.

Quanto alla tutela dell'identità personale nella sua accezione di corretta rappresentazione della persona, si è constatato, anche alla luce delle teorie elaborate sul tema, che, oltre alle diverse corti nazionali e sovranazionali, un ruolo crescente è stato assunto dalla normativa sulla protezione dei dati personali e dall'Autorità

garante competente, la cui “giurisprudenza” ha ormai assorbito gran parte della casistica sul tema.

Dopo aver approfondito le molteplici direzioni in cui l’identità personale si è sviluppata dal punto di vista giuridico, si è fatto ritorno alla sua accezione più tradizionale, quella “anagrafica”, da cui si è deciso di partire per esplorare la connessione con il tema dell’identità digitale, oggetto principale dello studio.

Come emerge dal quadro normativo evocato, l’identità anagrafica è un concetto giuridico e amministrativo che comprende l’insieme delle informazioni fondamentali che identificano un individuo all’interno del sistema anagrafico dello Stato. Queste informazioni, registrate negli appositi registri, costituiscono la base giuridica per l’identificazione della persona nei rapporti con lo Stato e con terzi.

Nella presente trattazione si è provato a ricostruire il sistema delineato dall’ordinamento al quale è sottesa una logica sequenziale in cui ogni passaggio legittima il successivo, garantendo certezza e tracciabilità dell’identità di ciascun cittadino: lo stato civile definisce lo status giuridico della persona e registra gli eventi fondamentali della sua vita; l’anagrafe aggiorna e conserva tali informazioni, creando un database ufficiale della popolazione; i documenti di identità attestano concretamente l’identità della persona, permettendo il riconoscimento legale in ambito pubblico e privato.

L’identificazione anagrafica assume una duplice funzione: in alcuni contesti è un presupposto abilitante, necessario per esercitare diritti o accedere a servizi pubblici o privati, come prestazioni sanitarie, istruzione o rapporti bancari; in altri, è strumento di tutela, assicurando che i diritti e i servizi siano riconosciuti esclusivamente al titolare dell’identità, garantendo la correttezza e la sicurezza dei rapporti giuridici e amministrativi. Si è osservato come, storicamente, l’identità anagrafica sia sempre stata legata al territorio di riferimento, sia per nascita sia per residenza, con il comune che fungeva da archivio amministrativo e da punto di riferimento per l’esercizio dei diritti civili, sociali e politici. La territorialità, più che un vincolo formale, costituiva un principio organizzativo fondamentale: determinava l’accesso ai servizi pubblici, la partecipazione alla vita politica locale e la tutela giuridica del cittadino. Tuttavia, si è ricostruito come si trattasse di una percezione più che di una realtà, poiché l’anagrafe è un servizio nazionale gestito dai comuni, mentre la legislazione sulla cittadinanza, stato civile e anagrafi è di competenza esclusiva dello Stato. La gestione locale, affidata al sindaco come

ufficiale di governo, rappresenta una forma di prossimità al cittadino, senza modificare la titolarità del servizio, che rimane al Ministero dell'Interno.

Con l'istituzione dell'Anagrafe Nazionale della Popolazione Residente, il paradigma tradizionale, basato sulla decentralizzazione, ha subito una trasformazione radicale: la centralizzazione dei dati, accessibili uniformemente su tutto il territorio nazionale, supera i confini comunali come elemento vincolante dell'identità. L'identità anagrafica diventa così un'entità digitale, riconosciuta e certificata attraverso strumenti informatizzati, con valore giuridico indipendente dal contesto comunale di appartenenza.

Questa evoluzione interessa anche l'anagrafe stessa, che da registro diventa piattaforma digitale per semplificare l'accesso ai servizi. L'espansione dell'identità anagrafica, oltre i confini locali, trova prosecuzione a livello europeo: l'identità digitale unica promossa dall'UE consente ai cittadini di accedere a servizi pubblici e privati in ogni Stato membro, affermando un modello di identità sovranazionale e digitale. In questo contesto, la territorialità viene progressivamente superata, pur preservando certezza giuridica ed efficienza amministrativa.

In conclusione, il passaggio dall'identità anagrafica locale a quella nazionale e successivamente europea rappresenta una profonda trasformazione del concetto stesso di cittadinanza e riconoscimento giuridico. Il principio di territorialità, un tempo costitutivo dell'identità, viene sostituito da un paradigma digitale e transfrontaliero, garantendo continuità dei diritti e dei servizi in una dimensione sempre più ampia e sovranazionale, ridefinendo la relazione tra individuo e Stato e aprendo nuove prospettive sulle funzioni centrali dell'identificazione nell'ordinamento giuridico.

Partendo dall'analisi dell'identità "anagrafica" e alla luce della sua evoluzione più recente, la ricerca si è successivamente concentrata sull'identità digitale.

Anche in ambito digitale si è registrata la persistenza della dicotomia tipica dell'identità personale, distinguendo tra una nozione sostanziale dell'identità digitale, collegata al diritto a essere sé stessi e a essere correttamente rappresentati online, intimamente legata alla persona e ai suoi diritti fondamentali, e una nozione anagrafica, basata sull'identificazione del soggetto nella dimensione digitale.

L'identità digitale "sostanziale" trova oggi tutela soprattutto grazie alla normativa in materia di protezione dei dati personali, in particolare nel

Regolamento (UE) 2016/679 – GDPR, che disciplina il trattamento e la circolazione dei dati personali. In un contesto in cui ogni individuo diffonde quotidianamente informazioni online, la tutela di tali diritti si concretizza principalmente nel controllo sui propri dati e sulla loro circolazione, nonché sulla propria identità come somma di essi. Si evidenzia, quindi, un punto di contatto con quanto osservato con riferimento alla identità personale nella sua accezione “sostanziale” nella dimensione analogica. A tendere, come dimostrano le esperienze di paesi quali Danimarca e California prese in esame nella presente trattazione, si ritiene che la tutela dell’identità digitale sarà rafforzata tramite l’integrazione dei presidi previsti dalla privacy con strumenti legati alla proprietà intellettuale e al diritto d’autore, in particolare quando la gestione dei contenuti digitali individuali si intreccia con la sfera identitaria della persona. Alcune proposte normative prese in analisi prevedono, ad esempio, diritti esclusivi sui tratti facciali, sulla voce e sulle caratteristiche corporee, con protezione anche *post mortem*, analogamente a quanto avviene per le opere dell’ingegno. Del resto, nonostante l’apparente ampliamento dell’identità nella dimensione digitale, sembra si assista più che altro ad una regressione sul fronte dei diritti, fronteggiabile solo attraverso strumenti giuridici creativi, capaci di offrire rimedi giudiziali e stragiudiziali innovativi contro i rischi sempre più sofisticati della rete.

Anche la nozione anagrafica dell’identità nella dimensione digitale suscita riflessioni rilevanti per il costituzionalismo moderno. In particolare, il diritto all’identità digitale come strumento di identificazione per l’accesso ai servizi, alla luce dell’analisi effettuata, può essere considerato la proiezione digitale del corrispondente diritto analogico. Pur non godendo di riconoscimento costituzionale esplicito, esso è tutelato da un sistema articolato di norme diritto primario, ricostruito nella presente analisi. Questi strumenti, nel loro complesso, garantiscono concretamente la tutela dell’identità digitale strumentale all’identificazione, conferendole riconoscimento e configurandola come strumento abilitante all’accesso ai servizi pubblici, più che come semplice supporto tecnologico. Quanto alla tutela effettiva dell’identità digitale, che è uno degli aspetti più critici dei “nuovi diritti”, il sistema è stato progressivamente rafforzato con strumenti di protezione, non solo giudiziali, attivabili in caso di violazione o mancato riconoscimento. Alla luce di quanto esposto, al momento non sembra necessario procedere a una revisione costituzionale.

Anche a livello sovranazionale si è assistito sin dal Regolamento eIDAS ad una progressiva valorizzazione del tema, che vede il suo apice nella recentissima costituzione dell'identità digitale unica europea e del relativo wallet. Di conseguenza, si ritiene che sia nell'ordinamento nazionale che nel contesto dell'Unione Europea, l'identità digitale, l'identità unificata europea e il relativo wallet abbiano assunto il valore di diritti presupposti e necessari per l'esercizio effettivo dei diritti connessi alla cittadinanza, sia statale sia europea.

L'identità digitale rappresenta, dunque, un corollario imprescindibile dei processi di innovazione tecnologica e organizzativa della pubblica amministrazione e una manifestazione avanzata della cittadinanza amministrativa individuale. La strategia europea mostra come la cittadinanza digitale sia strettamente complementare alla cittadinanza dell'Unione, che include tra i suoi attributi la libertà di circolazione e il diritto di soggiorno nell'intero territorio degli Stati membri. L'UE mira a garantire ai cittadini l'accesso ai servizi digitali anche in Stati diversi da quello di residenza, evitando la necessità di creare nuove identità digitali o di fornire ulteriori dati personali, promuovendo interoperabilità transfrontaliera e un ecosistema europeo unitario dell'identità digitale.

In questo quadro, l'identità digitale si configura come attributo personale validato e riconosciuto dall'apparato pubblico, con piena operatività nei rapporti con l'amministrazione e nelle interazioni economiche e sociali. Essa assume una funzione abilitante in un mercato sempre più orientato verso sistemi di identificazione digitale omogenei, interoperabili e in grado di operare senza soluzione di continuità a livello transfrontaliero.

La presente trattazione ha inteso concentrarsi con particolare attenzione, in una prospettiva costituzionalistica, anche sulle tecniche di regolazione. L'analisi consente di svolgere anche alcune prime riflessioni sul punto. Il regime normativo dell'identità digitale si caratterizza per un'architettura multilivello, che combina norme sovranazionali, leggi nazionali di rango primario e secondario, linee guida tecniche e altri strumenti di *soft law*. Il punto di forza di questo sistema risiede nell'attenzione dedicata all'identità, seppur in assenza di una previsione esplicita in Costituzione.

In questo contesto, come avviene per gran parte della regolazione sulle tecnologie, un ruolo determinante è svolto senza dubbio dall'Unione europea. Inoltre risulta preponderante il Governo a livello nazionale e la Commissione

europea a livello sovranazionale. Tra gli esempi paradigmatici, vi è la normativa sull'identità digitale, che, come si è visto, è di derivazione europea e in gran parte attuazione dei Regolamenti eIDAS sul tema.

La normativa italiana sul digitale e sull'identità digitale, inoltre, è spesso frutto di decreti legislativi delegati o d'urgenza. Sul ruolo della Commissione europea, non possono non prendersi ad esempio gli atti di esecuzione relativi all'EUDI Wallet, che definiscono modalità di rilascio, caratteristiche tecniche, requisiti di sicurezza, criteri di interoperabilità e funzioni di certificazione dei portafogli. Tali atti, adottati dalla Commissione europea ai sensi dell'art. 290 TFUE, rappresentano strumenti essenziali per rendere operative le previsioni del Regolamento eIDAS², assicurando l'effettiva implementazione dell'identità digitale europea.

Questo approccio comporta però una redistribuzione del potere normativo, spostando il centro decisionale dal nazionale al sovranazionale e dalla rappresentanza politica del Parlamento a una governance più tecnica, guidata dalla Commissione e dai Governi. Anche nel caso dell'EUDI Wallet, si ripropone il dibattito più ampio sulla regolazione tecnologica, in cui si confrontano l'efficienza normativa, necessaria in un ambito in continua evoluzione, e il pieno controllo democratico del processo regolatorio.

Infine, pur salutando con favore l'attenzione sia a livello nazionale che sovranazionale sul tema dell'identità digitale, va rilevato che la regolazione multilivello può determinare conflitti normativi e di competenze tra autorità, come già osservato in altri settori del diritto, invece di costituire un'efficace tutela per i soggetti interessati, che si trovano nella società digitale ad essere contemporaneamente cittadini nazionali ed europei, utenti, consumatori e interessati.

La società digitale e la stessa identità digitale, peraltro, pongono diverse preoccupazioni. Non possono essere trascurati e in questo senso sono stati presi in analisi nella presente trattazione i rischi e le criticità connessi all'espansione dell'identità digitale, sia in termini territoriali sia dimensionali. L'interoperabilità transfrontaliera per l'accesso ai servizi pubblici e privati nel mercato unico digitale, sebbene aumenti efficienza e integrazione dei servizi, comporta vulnerabilità in materia di protezione dei dati personali e sicurezza informatica, generando potenziali rischi per i cittadini europei.

In questo quadro, in Italia si sta valutando una riforma del Codice dell'amministrazione digitale per adeguare la normativa interna sull'identificazione digitale al mutato contesto delineato dal Regolamento eIDAS2. A livello sovranazionale, l'Europa si sta orientando, tramite il cosiddetto "Digital Omnibus", a una revisione complessiva delle normative digitali, con l'obiettivo di semplificare e armonizzare il quadro regolatorio.

Con riguardo, infine, all'identità del minore negli ambienti digitali, l'analisi ha preso in considerazione, con pari livello di approfondimento, tanto la dimensione dell'identità in senso "sostanziale" quanto quella "anagrafica".

Sotto il profilo dell'identità sostanziale, l'indagine non si è limitata al diritto del minore a essere sé stesso e a essere correttamente rappresentato anche nello spazio digitale, ma si è estesa all'esame di fenomeni quali lo *sharenting* e la figura dei *baby influencer*, intesi quali pratiche idonee a incidere in modo significativo sul diritto del minore all'autodeterminazione nella costruzione della propria identità e nella gestione consapevole della propria presenza online.

In assenza di una disciplina settoriale specifica – nonostante, come si è evidenziato, siano state avanzate numerose proposte normative – la tutela dell'identità sostanziale del minore risulta attualmente affidata quasi esclusivamente alla normativa in materia di protezione dei dati personali e all'azione dell'Autorità garante per la protezione dei dati personali. Quest'ultima ha svolto un ruolo centrale non solo attraverso l'adozione di provvedimenti, ma anche mediante iniziative di sensibilizzazione e di alfabetizzazione digitale, rivolte in primo luogo ai genitori.

Quanto alle proposte legislative presentate sul tema, indipendentemente dalla loro matrice politica, esse appaiono, a giudizio della scrivente, sintomatiche di una persistente incertezza circa i principi fondamentali che dovrebbero informare una regolamentazione organica della materia, vale a dire i valori e i criteri ispiratori di riferimento. In particolare, non emerge con chiarezza quale sia l'obiettivo ultimo perseguito dal legislatore italiano rispetto a snodi essenziali per una disciplina coerente, quali la determinazione dell'età del consenso – variamente fissata, nelle diverse proposte, tra i tredici e i sedici anni – l'introduzione di un divieto ovvero la liberalizzazione di pratiche come quella dei *baby influencer*, nonché la definizione dei limiti allo *sharenting*, ambito nel quale sembra mancare una presa di posizione netta e univoca.

Tali problematiche emergono con particolare evidenza in relazione al disegno di legge n. 1136 del 2024, attualmente all'esame istruttorio della Commissione VIII del Senato.

Considerazioni in parte analoghe possono essere svolte con riferimento all'esperienza francese esaminata, che, pur distinguendosi per l'adozione di una normativa già vigente e in fase di applicazione – esito di un compromesso politico – presenta profili di criticità non dissimili.

Per quanto concerne l'identità “anagrafica”, essa è stata esaminata con riferimento ai meccanismi di identificazione del minore e, in particolare, alle politiche di identificazione funzionali alla verifica dell'età.

Gli strumenti di *age verification*, attualmente fortemente promossi a livello europeo, assumono un ruolo di primaria rilevanza in quanto consentono di accertare la maggiore o minore età degli utenti e, conseguentemente, di modulare l'accesso a contenuti e servizi offerti online. L'analisi ha messo in luce come il favore espresso dalle istituzioni europee nei confronti di tali strumenti non sia riconducibile a un'impostazione paternalistica né a un intento di controllo generalizzato degli utenti, bensì rappresenti una risposta fondata su evidenze empiriche emerse da numerosi studi interdisciplinari, i cui risultati non appaiono più ignorabili. D'altra parte, la ricostruzione ha tenuto conto anche della fase precedente, caratterizzata da un atteggiamento di sostanziale inerzia da parte delle istituzioni europee, le cui conseguenze – oggi chiaramente riscontrabili – si sono rivelate particolarmente gravi per i minori.

In tale prospettiva, come si è visto, l'Unione europea promuove con decisione l'adozione di sistemi di verifica dell'età conformi al Digital Services Act e alle relative Linee guida di attuazione, improntate a un approccio di equilibrio tra l'esigenza di tutela dei minori e le necessità operative dei gestori di siti e piattaforme digitali. La disciplina europea, inoltre, non si fonda sulla stigmatizzazione di specifiche categorie di contenuti, quali quelli pornografici, ma adotta un'impostazione di carattere orizzontale, volta a limitare l'accesso dei minori a una pluralità di contenuti considerati inappropriati o potenzialmente dannosi.

Uno sguardo al contesto internazionale – sul quale, deliberatamente, non ci si è soffermati in modo sistematico – conferma come, alla luce dei dati allarmanti analizzati, numerosi ordinamenti abbiano optato per il ricorso a meccanismi di verifica dell'età al fine di garantire il rispetto dei limiti di accesso ai servizi di social

networking. Emblematico è il caso dell’Australia, la cui normativa, pienamente efficace dal 10 dicembre 2025, introduce un divieto assoluto di accesso ai social network per i minori di sedici anni. In tale ordinamento, peraltro, non si è ricercato un bilanciamento con gli interessi dei gestori delle piattaforme, i quali sono tenuti a implementare sistemi efficaci di verifica dell’età e rispondono in via esclusiva delle eventuali violazioni del divieto. Ancora più radicale si presenta l’approccio prospettato nello Stato del Texas, ove, in caso di approvazione definitiva dell’House Bill 186 (HB 186), l’accesso ai social network sarebbe vietato ai minori di diciotto anni, qualificati indistintamente come “children”.

Ciò posto, l’impiego di sistemi di verifica dell’età non dovrebbe in alcun caso ridursi a un mero strumento tecnico di filtraggio dei contenuti, ma dovrebbe essere inserito all’interno di una strategia complessiva volta a promuovere un uso consapevole, responsabile e progressivamente autonomo delle tecnologie digitali da parte dei minori. In questa prospettiva, l’attenzione non dovrebbe concentrarsi esclusivamente sul rispetto formale delle regole, bensì sulla effettiva comprensione, da parte del minore, delle modalità di trattamento dei propri dati personali, delle implicazioni per l’esercizio dei diritti fondamentali e della potenziale irreversibilità di talune scelte compiute nello spazio digitale.

La scelta di ricorrere a tali strumenti deve, pertanto, essere necessariamente accompagnata da politiche strutturate di alfabetizzazione digitale rivolte ai minori, finalizzate allo sviluppo di competenze critiche, alla consapevolezza dei rischi e alla capacità di gestione autonoma delle informazioni e delle interazioni online.

Del resto, già a pochi mesi dall’entrata in vigore del complesso delle fonti normative europee esaminate nella presente trattazione, sono emersi in modo evidente i limiti connessi alla loro applicazione pratica. Al momento in cui si scrive, il Parlamento europeo, con una risoluzione non vincolante, ha manifestato forti preoccupazioni alla luce dei dati emersi nel 2025, sollecitando un’applicazione più rigorosa del Digital Services Act. In particolare, pur accogliendo favorevolmente gli sforzi della Commissione volti allo sviluppo di un’app europea per la verifica dell’età e del portafoglio europeo di identità digitale, il Parlamento ha sottolineato come i sistemi di *age assurance* debbano essere accurati e rispettosi della privacy e, in ogni caso, non possano esonerare le piattaforme dalla responsabilità di garantire che i propri servizi siano sicuri e appropriati per i minori.

Con specifico riferimento all'ordinamento italiano, emergono rilevanti criticità riconducibili alla qualità complessiva della regolazione. Dopo un lungo periodo di sostanziale inattività legislativa in materia — nel quale l'unico strumento espressamente rivolto ai minori, e peraltro limitato all'accesso ad alcuni servizi pubblici, era rappresentato dallo SPID per minori — si è assistito a un improvviso mutamento di indirizzo con l'adozione del c.d. “Decreto Caivano”. Tale intervento, promosso dall'attuale Governo, si caratterizza per un'impostazione prevalentemente repressiva, incentrata sul divieto di accesso ai contenuti pornografici e priva di un adeguato corredo di misure di accompagnamento, nonché per un approccio settoriale, limitato a una sola categoria di contenuti. Ne consegue il rischio che la disciplina introdotta non sia idonea a fronteggiare in modo efficace la pluralità e complessità dei pericoli cui i minori sono esposti nell'ambiente digitale.

Allo stato attuale, permangono significative perplessità tanto in ordine all'effettività delle misure previste dal “Decreto Caivano” e dal conseguente Regolamento AGCOM, quanto con riguardo alle criticità già emerse nella loro applicazione e ai profili di legittimità delle stesse. Sarebbe auspicabile che il legislatore — ovvero, in via sostitutiva, il Governo — abbandonasse interventi frammentari e dettati dall'urgenza contingente, orientando invece l'azione normativa verso una strategia organica e integrata di gestione dei rischi digitali, capace di includere anche fenomeni di rilevante impatto sociale, quali, ad esempio, il gioco d'azzardo online.

L'adozione di un modello regolatorio di tipo emergenziale, anziché sistematico e strutturale, risulta particolarmente problematica in relazione a un fenomeno che non può essere considerato episodico, ma che si configura come elemento stabile della società digitale contemporanea. Tale impostazione emerge con evidenza dalla scelta dello strumento della decretazione d'urgenza, concepito dal costituente come eccezionale e limitato a situazioni straordinarie di necessità e urgenza. In questo contesto, il ricorso al decreto-legge sembra riflettere una carenza di visione strategica e di coordinamento normativo, con il rischio di produrre soluzioni parziali e disallineate rispetto sia al diritto dell'Unione europea sia agli standard internazionali di tutela dei minori nell'ambiente digitale.

Non a caso, la stessa AGCOM ha raccomandato l'estensione degli obblighi di verifica dell'età previsti dal “Decreto Caivano” anche ad altre tipologie di

contenuti, ulteriori rispetto a quelli pornografici, che possono risultare comunque pregiudizievoli per lo sviluppo fisico, psichico o morale dei minori. La questione della qualità della regolazione, peraltro, non si esaurisce in una valutazione di opportunità politica, ma investe direttamente la legittimità degli atti normativi. Come evidenziato nella presente trattazione, si registrano infatti numerosi disallineamenti tra il quadro normativo italiano e quello europeo, nonostante la clausola di cedevolezza prevista dall'ordinamento interno.

Si profila, inoltre, il rischio di replicare – seppur in un contesto parzialmente differente – le criticità già emerse nell'esperienza francese, in particolare con riferimento ai fornitori di servizi della società dell'informazione stabiliti al di fuori del territorio nazionale. Permangono, infatti, rilevanti dubbi circa la compatibilità con il principio del “paese di origine” di discipline, come quella italiana, che impongono nuovi obblighi a carico di operatori stabiliti in altri Stati. A ciò si aggiunge il rischio di un'ulteriore frammentazione normativa derivante dal disegno di legge sulla tutela dei minori online, attualmente all'esame dell'VIII Commissione del Senato, il quale potrebbe stratificare il quadro regolatorio introducendo disposizioni non pienamente coerenti con la normativa nazionale ed europea già vigente.

Infine, in linea con quanto osservato anche in relazione alla regolazione europea, la verifica dell'età, se non accompagnata da un adeguato investimento in misure educative, rischia di rafforzare un'impostazione prevalentemente repressiva, piuttosto che promuovere una autentica cultura dell'educazione digitale. In tale prospettiva, assume particolare rilievo il contesto nazionale, nel quale è attualmente in discussione un disegno di legge di iniziativa governativa sul consenso informato in ambito scolastico per le attività extracurricolari, con specifico riferimento alle tematiche attinenti alla sfera sessuale. L'Italia, peraltro, si colloca tra i pochissimi Paesi europei a non prevedere l'educazione sessuale obbligatoria nelle scuole, nonostante evidenze empiriche dimostrino l'efficacia di una formazione completa alle relazioni e alla sessualità anche in termini di prevenzione della violenza di genere.

In conclusione, la verifica dell'età, se considerata isolatamente, non rappresenta una soluzione sufficiente. L'analisi conferma la centralità del principio del *best interest of the child* (BIC) quale criterio guida nella regolazione dell'accesso dei minori ai servizi digitali, evidenziando tuttavia la necessità di un

suo aggiornamento alla luce delle trasformazioni introdotte dalle tecnologie digitali e dall'intelligenza artificiale.

Originariamente elaborato in contesti fisici e sociali, il BIC conosce oggi una progressiva estensione alla dimensione digitale, includendo la tutela dell'identità digitale, la protezione dei dati personali e la sicurezza online, nonché la gestione di rischi emergenti quali la profilazione automatizzata e l'esposizione a contenuti nocivi. Tale evoluzione implica un approccio multilivello, in cui alla protezione si affianca la promozione dell'alfabetizzazione digitale e dello sviluppo di competenze critiche, al fine di favorire un'autonomia responsabile dei minori, nel quadro di una corresponsabilità tra famiglie, istituzioni educative e piattaforme.

In questa prospettiva, il BIC integra protezione e partecipazione, riconoscendo ai minori diritti informativi effettivi e strumenti di comprensione delle dinamiche digitali. Per rendere tale tutela concretamente efficace, risulta infine indispensabile ripensare la nozione di trasparenza, superando un modello meramente formale a favore di una trasparenza sostanziale, idonea a rendere intelligibili i processi decisionali automatizzati e le implicazioni del trattamento dei dati sui diritti fondamentali dei minori.

Indice bibliografico

- Abidin C., *Micromicrocelebrity: Branding babies on the Internet*, in *M/C Journal*, 2015, 1.
- Alonzo R., Hussain J., Stranges S., Anderson K.K., *Interplay between social media use, sleep quality, and mental health in youth: A systematic review*, in *Sleep Med. Review*, 56, 2021.
- Alpa G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723.
- Alpa G., *Il diritto di essere sé stessi*, Milano, 2021.
- Andreola E., *Minori e incapaci in Internet*, Napoli, 2019.
- Appiah C.W., *The Ethics of Identity*, Princeton University Press, NJ, 2005.
- Are M., *Interesse alla qualificazione e tutela della personalità*, in *Riv. dir. comm.*, 1965, 81.
- Ascarelli T., *Teoria della concorrenza e dei beni immateriali*, Milano, 1957.
- Astone A., *Il controverso itinerario dell'identità di genere*, in *Nuova giur. civ. comm.*, 2016, 315.
- Astone A., *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019.
- Austen J., *Pride and Prejudice*, Londra, 1813.
- Bachelet V., *Evoluzione del ruolo delle strutture della pubblica amministrazione*, Milano, 1977.
- Baillon-Wirtz N., *L'enfant aussi a une vie privée et un droit à l'image*, in www.leclubdesjuristes, 6 marzo 2024.
- Baldassarre A., *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974.
- Baldassarre A., *Diritti inviolabili voce*, in *Enc. giur.*, vol. XI, Roma, 1989, 1.
- Baldini V. (a cura di), *Che cosa è un diritto fondamentale? Atti del convegno annuale dell'Associazione "Gruppo di Pisa", Cassino 10 e 11 giugno 2016*, Napoli, 2017.
- Barbera A., *Art. 2 Cost.*, in Branca G. (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1975, 50.
- Barbera A., *"Nuovi diritti": attenzione ai confini*, in Califano L. (a cura di), *Corte costituzionale e diritti fondamentali*, Torino, 2004, 19.
- Barile P., *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984.
- Bartolucci L., *L'anteposizione del cognome dell'adottante a quello dell'adottato maggiore d'età. Nota a Corte cost., sentenza n. 135 del 2023*, in *Osservatorio cost.*, n. 2/2024, 1.
- Bassu C., *Il diritto all'identità anagrafica. Il cognome materno tra personalità individuale e principio di eguaglianza*, Napoli, 2021.
- Battelli E., *I soggetti vulnerabili: prospettive di tutela della persona*, in *Dir. fam. pers.*, 2020, 283.
- Battelli E., *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021.

- Bauman Z., *Intervista sull'identità*, Roma-Bari, 2003.
- Bavetta G., voce *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, Milano, 1970, 953.
- Belisario E., *La nuova pubblica amministrazione digitale: guida al Codice dell'Amministrazione Digitale dopo la legge n. 69/2009: diritti digitali, strumenti, obblighi, sanzioni e responsabilità*, Santarcangelo di Romagna, 2009.
- Belisario E., *Il regolamento eIDAS 2.0 e l'impatto sulla gestione documentale delle PA: quali prospettive?*, in Manca G. (a cura di), *Il regolamento eIDAS n. 2024/1183*, in *Riv. elettronica dir. econ. management*, n. spec. 4/2024, 32.
- Belisario E., Ricciulli F., *Legalità algoritmica e vizi procedurali*, in Belisario E., Cassano G. (a cura di), *Intelligenza Artificiale per la Pubblica Amministrazione. Principi e regole del procedimento amministrativo algoritmico*, Pisa, 2023, 149.
- Belisario E., Pagnotta S., Ricciulli F., *Amministrazione digitale: guida ragionata agli switch off*, Santarcangelo di Romagna, 2021.
- Bianca M. (a cura di), *Memoria versus oblio*, Torino, 2019.
- Bianca M., *La filter bubble e il problema dell'identità digitale*, in *Riv. dir. media*, n. 2/2019,1.
- Bilotta F., *Transessualismo* voce, in *Dig. disc. priv.*, VIII Agg., Torino, 2013, 732.
- Bin R., *Chi è il giudice dei diritti? Il modello costituzionale e alcune deviazioni*, in *Riv. AIC*, n. 4/2018, 1.
- Bobbio N., *L'età dei diritti*, Torino, 1990.
- Boccia C., Contessa C., De Giovanni E., *Codice dell'Amministrazione digitale: D.lgs. 7 marzo 2005, n. 82 commentato e annotato per articolo, aggiornato al D.lgs. 13 dicembre 2017, n. 217: con una guida operativa al Codice*, Piacenza, 2018, 297.
- Bourrat-Guèguen A., *Respect du droit à l'image des enfants: ce que change la loi du 19 février 2024*, in www.village-justice.com, 21 marzo 2024.
- Bozzi L., *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, 254.
- Bozzola E., Spina G., Agostiniani R., Barni S., Russo R., Scarpato E., Di Mauro A., Di Stefano A.V., Caruso C., Corsello G., Staiano A., *The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*, in *International Journal of Environmental Research and Public Health*, 19, 2022, 9960.
- Burbergs M., *How the right to respect for private and family life, home and correspondence became the nursery in which new rights are born: Article 8 ECHR*, in Brems E., Gerards J. (a cura di), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights*, Cambridge University Press, Cambridge, 2014, 315.
- Buscema S., *Prospettive per la meccanizzazione integrale*, in *Riv. informazione*, 1970, 110.
- Byung-Chul Han, *Infocrazia*, Torino, 2023.
- Caccia A., *Il ruolo degli standard in eIDAS2*, in Manca G. (a cura di), *Il regolamento eIDAS n. 2024/1183*, in *Riv. elettronica dir. econ. management*, n. spec. 4/2024, 71.

- Caccioppo D., *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*, in *Riv. it. inf. dir.*, 2024, 385.
- Caggiano I.A., *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecnoregolazione*, in *Familia*, 2018, 3.
- Cajani F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n. 93 (conv. con modif. dalla L. 15 ottobre 2013, n. 119)*, in *Cass. penale*, 2014, 1094.
- Camardi C., *Minore e privacy nel contesto delle relazioni familiari*, in Senigaglia R. (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2019, 122.
- Campodonico F.G., *Fine vita e suicidio medicalmente assistito: dalla sentenza n. 242 del 2019 alla recentissima sentenza n. 132 del 2025*, in *Federalismi.it*, n. 30/2025, 78.
- Capeci F., *Generazione 2.0. Chi sono, cosa vogliono, come dialogare con loro*, Milano, 2014.
- Caretti P., Tarli Barbieri G., *I diritti fondamentali. Libertà e diritti sociali*, V ed., Torino, 2022.
- Carlassare L., *Fonti del diritto (diritto costituzionale) voce*, in *Enc. dir.*, Annali, vol. II, Milano, 2008, 536.
- Carlotto I., *La ricerca delle proprie origini nel bilanciamento dei diritti*, Napoli, 2020.
- Cartabia M., *In tema di "nuovi" diritti*, in Aa.Vv., *Studi in onore di Franco Modugno*, Napoli, 2011.
- Cataudella A., *Dignità, decoro e identità personale*, in *Dir. inform. inf.*, 1985, 575.
- Cavallo Perin R., Romano A., *Commentario breve al testo unico sulle autonomie locali*, Padova, 2006.
- Cecchetti M., *La produzione pubblica del diritto dell'ambiente: tra expertise tecnico-scientifico, democrazia e responsabilità politica*, in *DPCE online*, 2020, 1.
- Celano B., *I diritti dello stato costituzionale*, Bologna, 2013.
- Cerri A., *Identità personale voce*, in *Enc. giur.*, IV Agg., Roma, 1995, 1.
- Charisi V., Chaudron S., Di Gioia R., Vuorikari R., Escobar Planas M., Sanchez Martin J.I., Gomez Gutierrez E., *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy*, in *Publications Office of the European Union*, Luxembourg, 2022.
- Cheli E., *Conclusioni*, in *Oss. fonti*, 2021, 2021, 955.
- Christians L.L., *Dimensions philosophiques et religieuses des approches juridiques de l'identité*, in Pousson J., Petit (ed.), *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002.
- Clooley T.M., *Treatise on the Law of Torts*, 1879.
- Cocuccio M.A., *Il diritto all'identità personale e l'identità digitale*, in *Dir. fam. e pers.*, 2016, 949.

- Colapietro C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, n. 22/2018, 1.
- Colapietro C., *Digitalizzazione e Costituzione*, in *Riv. giur. on-line-ISSiRFA*, n. 1/2025, 1.
- Colapietro C., Iannuzzi A., *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in Califano L., Colapietro C., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 85.
- Colapietro C., Ruotolo M., *Diritti e Libertà*, in Modugno F. (a cura di), *Manuale di diritto pubblico*, Torino, 2023, 631.
- Cooley A.H., *Guarding Against a Radical Redefinition of Liability for Internet Misrepresentation: The United States v. Drew Prosecution and the Computer Fraud and Abuse Act*, in *Journal of Internet Law*, 2011, 23.
- Cremona E., *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in *Riv. it. inf. dir.*, 2024, 111.
- Crescioli C., *La tutela penale dell'identità digitale*, in *Dir. pen. contemp.*, 2018, 265.
- Cuocci V., *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale*, Bari, 2022.
- D'Amico G., *Stato e persona. Autonomia individuale e comunità politica*, in Cortese F., Caruso C., Rossi S. (a cura di), *Immaginare la Repubblica. Mito e attualità dell'Assemblea costituente*, Milano, 2018.
- D'Amico M., *I diritti dei "diversi". Saggio sull'omosessualità*, in *Oss. cost.*, 2021, 164.
- D'Ancona S., Provenzano P., *Gli strumenti della Carta della cittadinanza digitale*, in Cavallo Perin R., Galetta D.U. (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 223.
- D'Andrea P.I., *La sentenza della Corte costituzionale sulla rettificazione anagrafica del sesso: una risposta e tanti nuovi interrogativi*, in *Giur. cost.*, 2016, p. 263.
- D'Ippolito G., *Il diritto di accesso ad Internet in Italia: dal 21(-bis) al 34-bis*, in *Riv. dir. media*, 2021, 81.
- Dario A., La Lumia A., *Minori, internet e social network*, Milano, 2021.
- De Crescenzo A., *Le "sunset rules" come strumenti di better regulation. Un possibile equilibrio tra centralità parlamentare in periodi emergenziali e obiettivo di semplificazione normativa*, in *DPCE online*, n. 2/2020, 1.
- De Cupis A., *Il diritto all'identità personale*, Milano, 1949.
- De Cupis A., *La verità nel diritto (Osservazioni in margine a un libro recente)*, in *Foro it.*, 1952, 223.
- De Cupis A., *I diritti della personalità*, in Cicu A., Messineo F. (a cura di), *Trattato di diritto civile e commerciale*, vol. IV, tomo I, Milano, 1982, 32.
- De Giovanni E., *Il Codice dell'amministrazione digitale: genesi, evoluzione. Principi costituzionali e linee generali*, in Boccia C., Contessa C., De Giovanni

- E. (a cura di), *Codice dell'Amministrazione digitale. D.L.gs 7 marzo 2005, n. 82 commentato e annotato per articolo*, Piacenza, 2018, 20.
- Di Ciommo F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in Cuffaro V., D'Orazio R., Ricciuto V. (a cura di), *I dati personali nel diritto europeo: il regolamento generale 2016/479 (e le direttive sul trattamento dei dati in ambito penalistico)*, Torino, 2019, 351.
- Di Lorenzo G., *La dichiarazione giudiziale di paternità e maternità naturale dei figli nati da rapporto incestuoso*, in *Giur. cost.*, 2003, 1.
- Dogliotti M., *Sul concetto di diritto minorile: autonomia, favor minoris, principi costituzionali*, in *Dir. fam. pers.*, 1977, 954.
- Donati D., *Digital divide e promozione della diffusione delle TIC*, in Merloni F. (a cura di), *Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione*, Torino, 2005, 209.
- Donini M., *Antigiuridicità e giustificazione oggi. Una "nuova" dogmatica, o solo una critica per il diritto penale moderno?*, in *Riv. it. dir. proc. pen.*, 2009, 1658.
- Donini M., *La necessità di diritti infelici. Il diritto di morire come limite all'intervento del legislatore penale*, in *Riv. it. med. legale*, 2016, 554.
- Donini M., *Libera nos a malo. I diritti di disporre della propria vita per neutralizzare il male*, in D'Alessandro G., Di Giovine O. (a cura di), *La Corte costituzionale e il fine vita. Un confronto interdisciplinare sul caso Cappato-Antoniani*, Torino, 2020, 221.
- Donovan S., *Sharenting: The Forgotten Children of the GDPR*, in *Peace Human Rights Governance*, Padova University Press, 2020, 35.
- Duni G., *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. amm. republ. It.*, 1978, 407.
- Falco G., *Identità personale voce*, in *Nuovo dig. it.*, Torino, 1938, 649.
- Fantigrossi U., *Automazione e pubblica amministrazione. Profili giuridici*, Bologna, 1993.
- Federico M., *Protezione dei dati personali e tutela collettiva Itinerari di comparazione tra Europa e Stati Uniti*, Venezia, 2024.
- Ferrando G., *Diritto all'informazione e tutela dell'identità personale: note in margine ad un recente convegno*, in *Giust. civ.*, 1980, 581.
- Ferraro L., *La Corte costituzionale e la primazia del diritto alla salute e della sfera di autodeterminazione*, in *Giur. cost.*, 2015, 2054.
- Ferraro L., *Il giudice nel procedimento di rettificazione del sesso: una funzione ormai superata o ancora attuale?*, in *Questione giustizia*, 2016.
- Fiaccavento S., *Tutela della persona e «creazione giurisprudenziale» del diritto*, in *Giust. civ.*, n. 5/1992, 233.
- Finocchiaro G., *Identità personale (diritto alla) voce*, in *Dig. disc. priv.*, V Agg., Torino, 2010, 721.
- Finocchiaro G., *Identità personale su internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf.*, 2012, 383.
- Finocchiaro G., *Identità personale su internet. Il diritto alla contestualizzazione dell'informazione*, in *Dir. inform. inf.*, 2012, 383.

- Finocchiaro G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in Resta G., Zeno Zencovich V. (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, 29.
- Finocchiaro G., *Intelligenza artificiale. Quali regole?*, Bologna, 2024.
- Fioravanti G., Cassioli E., Rossi E., Lucherini Angeletti L., Casale S., Ricca V., Castellini G., *The relationship between problematic Instagram use and eating disorders psychopathology: an explanatory structural equation model*, in *Soc. Psychiatry Psychiatr Epidemiol*, 2024, 59, 1617.
- Foglia M., *Sharenting e riservatezza del minore in rete*, in *Actualidad Jurídica Iberoamericana*, 2022, 3552.
- Friedman L.M., *La società orizzontale*, Bologna, 2002.
- Frosini T.E., *Il Costituzionalismo nella Società tecnologica*, in Aa.Vv., *Liber amicorum per Pasquale Costanzo*, in *Consulta Online*, I, 2020, 1.
- Garno Z., *Première analyse de la loi visant à garantir le respect du droit à l'image des enfants*, in *Village-justice.com*, 1.
- Gatt L., Caggiano I.A., *Consumers and digital environments as a structural vulnerability relationship*, in *European Journal of Privacy Law and Technologies*, 2023, 9.
- Gemma G., *Vita (diritto alla) voce*, in *Dig. IV disc. pubbl.*, vol. XV, Torino, 1999, 671.
- Gemma G., *Dignità ed eutanasia: non c'è antitesi. Note a margine di un'opera recente di una costituzionalista cattolica*, in *Materiali per una storia della cultura giuridica*, n. 1/2016, 253.
- Giubilei A., *Discrezionalità legislativa e garanzia della Costituzione*, Roma, 2023.
- Gleason P., *Identifying Identity. A Semantic History*, in *The Journal of American History*, n. 4/1983, 910.
- Grassi S., Cecchetti M. (a cura di), *Governo dell'ambiente e formazione delle norme tecniche*, Milano, 2006.
- Groebner V., *Storia dell'identità personale e della sua certificazione, Scheda segnaletica, documento d'identità e controllo nell'Europa moderna*, trad. di Michler A. (a cura di), Bellinzona, 2008.
- Guarini P.C., «Maschio e femmina li creò» ... o, forse, no. *La Corte costituzionale ancora sulla non necessità di intervento chirurgico per la rettificazione anagrafica di attribuzione di sesso*, in *Federalismi.it*, n. 8/2018, 1.
- Gutmann V.D., *Le sentiment d'identité. Étude de droit des personnes et de la famille*, Parigi, 2000.
- Haas G., *Proposition de loi: l'image des enfants enfin protégée sur internet?*, in *www.haas-avocats.com*, 15 febbraio 2024.
- Hervieu M., *Point sur la loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants*, in *Dalloz Actu Étudiant*, 14 marzo 2024.
- Heterington K., *Expression of identity. Space, Performance, Politics*, 1998.
- Honorati C. (a cura di), *Diritto al nome e all'identità personale nell'ordinamento europeo*, Milano, 2010.

- Hsin-Chi K., *Universality, Indivisibility and Interdependence of Human Rights: the case of China*, in *Pontifical Academy of Social Sciences*, acta 15, Vatican City, 2010, 359.
- Huttner L., *Le contrôle de l'accès des mineurs aux sites pornographiques*, in *Dalloz IP/IT : droit de la propriété intellectuelle et du numérique*, n. 7/2024, 400.
- Iannuzzi A., *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018.
- Iannuzzi A., *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in Pizzetti F., Calzolaio S., Iannuzzi A., Longo E., Orofino M. (a cura di), *La regolazione europea della società digitale*, Torino, 2024, 13.
- Iannuzzi A., *La qualificazione dei diritti fondamentali nell'ecosistema digitale. Relazione di sintesi del Tavolo n. 3 «Le democrazie costituzionali nella transizione digitale»*, in *Riv. Gruppo di Pisa*, n. spec. 11/2025, 347.
- Iannuzzi A., Colapietro C., *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, in *Riv. it. inf. dir.*, 2024, 333.
- Iannuzzi A., Laviola F., *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in *Dir. cost.*, 2023, 12.
- Intini A., *La identificazione di persone. Lettura dei documenti – Controllo di autenticità – Procedure*, IV ed., Roma, 1996.
- Irti C., *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 2019, 617.
- Jolicoeur M.P., *Vérifier l'âge des internautes sur les sites pornographiques*, in www.lex-electronica.org, 2023.
- Jona E., *Il servizio di anagrafe alle soglie della digitalizzazione*, in *Federalismi.it*, n. 18/2020, 182.
- Jonas H., *Il diritto di morire* (1978), *Il Nuovo Melangolo*, Genova, 1997.
- La Battaglia L., *La tutela del diritto all'identità personale: valori personalistici e circolazione dei dati nel bilanciamento fra diritti costituzionalmente rilevanti*, in Comandé G. (a cura di), *Diritto privato europeo e diritti fondamentali: saggi e ricerche*, Torino, 2004, 270.
- Ladu M., Maccabiani N., *L'autodeterminazione popolare nell'era digitale: tra opportunità normative e tecnologiche*, in *Consulta online*, 2023, 415 ss.
- Ladu M., Maccabiani N., *L'individuo e la realtà digitale. Una questione costituzionale e democratica oltre la virtualità*, Napoli, 2023.
- Landini S., *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. industriale*, 2017, 180.
- Leckhart S., *The Facebook-Free Baby Are you a mom or dad whos' guilty of 'oversharenting'? The cure may be ot not share at all*, in *The Wal Street Journal*, 2012, 1.
- Leopardi G., *Proposta di Premi fatta all'Accademia dei Sillografi*, Roma-Bari, 1928.
- Lingibè P., *Le respect du droit à l'image des enfants et les 5 apports de la loi du 19 février 2024*.
- Livingstone S., Carr J., Byrne J., *One in Three: Internet Governance and Children's Rights*, in *Report Series*, 2015, 1.

- Loiodice A., *Informatica, banche dati e diritto all'informazione*, in Aa.Vv., *Scritti in onore di Costantino Mortati. Aspetti e tendenze del diritto costituzionale*, vol. III, Varese, 1977, 637.
- Longo E., *La legge precaria. Le trasformazioni della funzione legislativa nell'età dell'accelerazione*, Torino, 2017.
- Lorenzetti A., *Diritti in transito*, Milano, 2013.
- Lorenzetti A., *Corte costituzionale e transessualismo: ammesso il cambiamento di sesso senza intervento chirurgico ma spetta al giudice la valutazione*, in *Quad. cost.*, 2015, 1006.
- Losano M.G., *L'automazione delle procedure gestionali e le banche di dati*, in *L'elaborazione elettronica. Principi di calcolo automatico*, Milano, 1979.
- Losano M.G., *Il diritto pubblico dell'informatica*, Torino, 1986.
- Luciani M., *Positività, metapositività e parapositività dei diritti fondamentali*, in Brunelli G., Pugiotto A., Veronesi P. (a cura di), *Scritti in onore di Lorenza Carlassare*, vol. III, Napoli, 2009, 1055.
- Luciani M., *Quale identità?*, in Aa.Vv., *Dialoghi con Guido Alpa*, Roma, 2018, 343.
- Luna R., *Qualcosa è andato storto*, Milano, 2025.
- Lupo N., *La normazione secondaria e il fenomeno della fuga dalla legge n. 400 del 1988 al vaglio del Comitato per la legislazione*, in *Federalismi.it*, n. 3/2017, 1.
- Maceratini A., *Sharenting e tutela dei minori, riflessioni informatico-giuridiche tra diritto alla privacy e diritto all'immagine*, in *Rivista di scienze della comunicazione e di argomentazione giuridica*, 2024, 120.
- Macrì I., Macrì U., Pontevolpe G., *Il nuovo codice dell'Amministrazione digitale*, Milano, 2011.
- Madji D., *Le Droit à l'image des enfants sur internet: nouvelle protection par la loi du 19 février 2024*.
- Manago A.M., *Identity development in the digital age: The case of social networking sites*, in McLean K.C., Syed M. (a cura di), *The Oxford Handbook of Identity Development*, Oxford University Press, 2015, 508.
- Manca G., *Sanità digitale. Manuale pratico per la gestione di identità, dati e documenti alla luce del regolamento eIDAS*, Roma, 2025, 30.
- Manca G., *Spid vivrà altri cinque anni, perché la Cie è un flop: e ora?*, in *Agenda Digitale* del 9 ottobre 2025.
- Maniaci G., *Perché abbiamo un diritto costituzionalmente garantito all'eutanasia e al suicidio assistito*, in *Riv. AIC*, 2019, 262.
- Marcello D., *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo*, Napoli, 2023.
- Marini G., *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, 359.
- Maritain J., *L'uomo e lo Stato* (1951), trad. it., Genova-Milano, 2003.
- Maritain J., *Cristianesimo e democrazia* (1943), trad. it., Firenze, 2007.
- Martoni M., *Identità personale anagrafica (autorizzata) vs identità personale autorappresentativa (manifestata)*, in *Riv. trim. dir. proc. civ.*, n. 1/2020, 179.

- Mascheroni G., *“Datizzati” alla nascita: a rischio i diritti delle nuove generazioni*, in *Agendadigitale.eu*.
- Matucci G., *La dissoluzione del paradigma della verità della filiazione innanzi all’interesse concreto del minore* (Nota a Corte cost., 18 dicembre 2017, n. 272), in *Forumcostituzionale.it*, 15 febbraio 2018.
- Mazzeo A., Nastri M., *Identificazione in rete: identità digitale e identità personale*, in *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 33.
- McPeak A., *Social Media Snooping and Its Ethical Bounds*, in *Arizona State Law Journal*, 2014, 1.
- Meo B., *Il “diritto a essere dimenticati e l’oblio su internet”*, in Belisario E., Scorza G., Riccio G.M. (a cura di), *Commentario GDPR e normativa privacy*, Padova, 2022.
- Meoli C., *La correzione dell’interpretazione sulla correzione del sesso: brevi note a Corte cost., sent. n. 221 del 2015*, in *Giustamm.it*, n. 6/2016, 1.
- Mezzanotte P., *Identità di genere non binaria e altre questioni in una recente pronuncia della Corte costituzionale*, in *Nomos*, 2024, 1 ss.
- Miglietti L., *La sovraesposizione digitale dei minori ed i suoi effetti. Note comparative sul fenomeno del cd. sharenting negli ordinamenti francese e italiano*, in *Dir. comparati*, 2024, 204.
- Mingardo G., *Il riconoscimento delle nuove soggettività e il limite del binarismo di genere nella prospettiva costituzionale*, in *GenIUS*, 24 settembre 2024, 1.
- Modugno F., *I “nuovi diritti” nella giurisprudenza costituzionale*, Torino, 1995.
- Modugno F., *È possibile parlare ancora di un sistema delle fonti?*, in *Riv. AIC*, 2008, 1.
- Morelli A., *I diritti senza legge*, in *Consulta online*, n. 1/2015, 10.
- Morelli A., *Persona e identità personale*, in *BioLaw Journal*, n. 2/2019, 45.
- Morelli A., Pollicino O., *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Riv. AIC*, 2018, 12.
- Morelli M.R., *Oblio (diritto all’) voce*, in *Enc. dir.*, Agg. VI, Milano, 2002, 848.
- Moro A.C., *Manuale di diritto minorile*, Bologna, 2014.
- Mounier V.E., *Il personalismo*, Roma, 2004.
- Musselli L., *La decisione amministrativa nell’età degli algoritmi: primi spunti*, in *Riv. dir. media*, 2020, 20.
- Nannipieri L., *La dimensione costituzionale del digital divide. In particolare, gli ostacoli cognitivi alla proiezione dell’individuo nello spazio virtuale*, in Nisticò M., Passaglia P. (a cura di), *Internet e Costituzione*, Torino, 2014, 189.
- Natale V., *Tutela dei minori online: possibili soluzioni per un’accurata verifica dell’età*, in *Agenda Digitale.eu*, 6 giugno 2024.
- Nativi S., *Le prospettive europee nel futuro prossimo*, in *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 464.
- Neri D., *Eutanasia. Valori, scelte morali, dignità delle persone*, Roma-Bari, 1995.
- Niger S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

- Nitti M., *La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in *Fam. dir.*, 2018, 390.
- Nocco A., *La rettificazione di attribuzione di sesso tra Corte Costituzionale n. 221/2015 e fonti sovranazionali*, in *Questione Giustizia*, 30 novembre 2015.
- Nozick R., *Philosophical Explanations*, Cambridge, Belknap Press, 1981.
- Olivetti M., *Diritti fondamentali e nuove tecnologie*, in *Revista Estudos Institucionais*, vol.6, n. 2/2020, 395.
- Orofino M., *Il DSA tra continuità (solo apparente) ed innovazione*, in Pizzetti F., Calzolaio S., Iannuzzi A., Longo E., Orofino M. (a cura di), *La regolazione europea della società digitale*, Torino, 2024, 144.
- Orofino M., *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 *Riv. dir. media*, 2022, 1.
- Orofino M., Pizzetti F. (a cura di), *Privacy, minori e cyberbullismo*, 337, Torino, 2018.
- Pace A., *Il c.d. diritto all'identità personale e gli art. 2 e 21 della Costituzione*, in *Giur. civ.*, n. 9/1980, 409.
- Pace A., *Problematica delle libertà costituzionali*, Padova, 1985.
- Pace A., *Nome, soggettività giuridica e identità personale*, in *Giur. cost.*, n. 1/1994, 103.
- Pacini F., *Ai confini della normatività. Hard law e soft law in "tempi difficili"*, Relazione al Convegno annuale dell'Associazione "Gruppo di Pisa", *Modello costituzionale e trasformazione del sistema delle fonti nelle crisi economica e pandemica. Emergenza e persistenza*, Firenze, 17-18 giugno 2022.
- Parfit D., *Reasons and Persons*, Oxford, Oxford U.P., 1984.
- Pasquino T., *Identità digitale della persona, diritto all'immagine e reputazione*, in Tosi E. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 93.
- Pedrazzi G., *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, in *Inf. e dir.*, 2017, 437.
- Perlingieri P., *La personalità umana nell'ordinamento giuridico*, Napoli, 1972.
- Piccinni S., *Appunti sui diritti della personalità e sui c.d. nuovi diritti. Tutela e promozione dell'identità personale*, in *Dir. famiglia e persone*, n. 1/2021, 227.
- Pierantoni D., *Minori su Internet: profili di responsabilità*, in *Riv. it. inf. dir.*, 2024, 399.
- Pino G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.
- Pino G., *Teorie e dottrine dei diritti della personalità. Uno strumento di meta-giurisprudenza analitica*, in Aa.Vv., *Materiali per una storia della cultura giuridica*, 2003, 1 ss.
- Pino G., *Il costituzionalismo dei diritti. Struttura e limiti del costituzionalismo contemporaneo*, Bologna, 2017.

- Pino G., *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in Panetta R. (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 257.
- Pino G., *L'identità personale*, in Rodotà S., Zatti P. (diretto da), *Trattato di biodiritto*, Milano, 2010, 297.
- Pizzorusso A., *Sistematica giuridica e sistema delle fonti del diritto*, in Aa.Vv., *Scritti in onore di Lorenza Carlassare*, I, Napoli, 2009, 281.
- Pollicino O., Lubello V., Bassini M. (a cura di), *Identità ed eredità digitali. Stato dell'arte e possibili soluzioni al servizio del cittadino*, Roma, 2016.
- Pollicino O., *Regolazione e innovazione tecnologica nell'ordinamento della rete*, in *Riv. AIC*, 2025, 119.
- Predieri A., *Gli elaboratori elettronici nell'amministrazione dello Stato*, Bologna, 1971.
- Prensky M., *Digital Natives, Digital Immigrants*, in *Digital Natives Digital Immigrants*, 2001, 1.
- Radtke T., *Mandatory Age Verification for Online Services under GDPR*, 2023.
- Raffiotta E., *Appunti in materia di diritto all'identità personale*, in *Forumcostituzionale.it*, 26 gennaio 2010.
- Randazzo A., *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *Dirittifondamentali.it*, n. 3/2021, 1.
- Razzano G., *Dignità nel morire, eutanasia e cure palliative nella prospettiva costituzionale*, Torino, 2014, 13.
- Razzano G., *Sulla sostenibilità della dignità come autodeterminazione*, in *BioLaw*, n. 2/2019, 95.
- Reale C.M., *Corte costituzionale e transgenderismo: l'irriducibile varietà delle singole situazioni*, in *BioLaw Journal*, n. 1/2016, 283.
- Remotti F., *L'ossessione identitaria*, Roma-Bari, 2017.
- Rescigno G.U., *Dal diritto di rifiutare un determinato trattamento sanitario secondo l'art. 32, comma 2, Cost., al principio di autodeterminazione intorno alla propria vita*, in *Dir. pubbl.*, 2008, 102.
- Rescigno P., voce *Personalità* (diritti della), in *Enc. giur.*, vol. XXIV, Roma, 1991, 6 ss.
- Resta F., *commento all'art. 8*, in Belisario E., Scorza G., Riccio G.M. (a cura di), *Commentario del GDPR e normativa privacy*, Padova, 2022, 106.
- Resta G., *Identità personale e identità digitale*, in *Dir. inform. inf.*, 2007, 511.
- Resta G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, 199.
- Ricca M., *Oltre Babele: codici per una democrazia interculturale*, Bari, 2008.
- Riccio G.M., *Chat Control: sorveglianza di massa in nome della protezione dei minori?*, in *Corriere delle comunicazioni*, 16 ottobre 2025.
- Ricciulli F., *L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti*, in *Riv. it. inf. dir.*, 2024, 355.

- Ridola P., *Diritti di libertà e costituzionalismo*, Torino, 1997, 46.
- Rivera I., *Le suggestioni del diritto all'autodeterminazione personale tra identità e diversità di genere. Note a margine di Corte cost. n. 221 del 2015*, in *Consulta online*, n. 1/2016, 175.
- Rodotà S., *Statuti e carte delle libertà*, in *Pol. dir.*, 1980, 170.
- Rodotà S., *Intorno alla privacy. Ipotesi e prospettive*, in AA.VV., *Studi in memoria di Franco Piga*, Milano, 1992, 1.
- Rodotà S., *Tecnologia e diritti*, Bologna, 1995.
- Rodotà S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583.
- Rodotà S., *Prefazione alla Relazione annuale dell'Autorità Garante per la protezione dei dati personali*, 1997.
- Rodotà S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.
- Rodotà S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e diritto privato*, n. 1/2004, 1.
- Rodotà S., *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, 254.
- Rodotà S., *Trasformazioni del corpo*, in *Pol. dir.*, n. 1/2006, 1.
- Rodotà S., *Nuovi soggetti, nuovi diritti, nuovi conflitti*, in Pizzetti F.G., Rosti M. (a cura di), *Soggetti, diritti, conflitti: percorsi di ridefinizione*, Milano, 2007.
- Rodotà S., *Una costituzione per Internet?*, in *Pol. dir.*, 2010, 337.
- Rodotà S., *Il diritto di avere diritti*, Roma-Bari, 2012.
- Rodotà S., *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014.
- Rodotà S., *Elaboratori elettronici e controllo sociale*, rist. anast., Napoli, 2018.
- Rolla G., *Il valore normativo del principio di dignità umana. Brevi considerazioni alla luce del costituzionalismo iberoamericano*, in *DPCE*, 2003, 1880.
- Rorty A.O. (ed.), *The Identities of Persons*, Berkeley, CA, University of California Press, 1976.
- Ruggeri A., *Crisi dello Stato nazionale, dialogo intergiurisprudenziale, tutela dei diritti fondamentali: notazioni introduttive*, in *Consulta online*, 2014, 1.
- Ruggeri A., *Il principio personalista e le sue proiezioni*, in *Federalismi.it*, n. 17/2013, 1.
- Ruggeri A., *Ha ancora un futuro la legge quale strumento primario di normazione e di direzione politica*, in *Oss. fonti*, 2021, 567.
- Ruggeri F., *Minori e privacy*, in Battelli E. (a cura di), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, 141.
- Ruggiano M.E., *Il diritto all'identità di genere: preoccupazioni per la decisione della Corte costituzionale nella sentenza n. 180 del 2017*, in *Stato, Chiese e pluralismo confessionale*, n. 41/2017, 1.
- Santoro Passarelli A., *Stato civile voce*, in *Dig. disc. pubbl.*, vol. XV, Torino, 1999, 44.
- Santoro L., *L'attribuzione del cognome ai figli: dalla discrezionalità del legislatore...alla discrezionalità dei genitori (considerazioni controcorrente a partire dalla ord. n. 18/2021 della Corte costituzionale)*, in *Consulta online*, n. 2/2021, 548.

- Santosuosso A., *Eutanasia, in nome della legge*, in *Micromega*, n. 1/2007, 28.
- Sartori L., *Il digital divide*, Bologna, 2006.
- Sas M., Mühlberg J.T., *Trustworthy Age Assurance?*, 2024.
- Scardullo F., *Stato civile voce*, in *Enc. dir.*, vol. XLIII, 1990, 1.
- Scorza G., Meligrana E., *La privacy degli ultimi*, Catanzaro, 2022.
- Senigaglia R., *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civ. comm.*, 2017, 1023.
- Shmueli B., Blecher, Prigat A., *Privacy for Children*, in *Columbia Human Rights Law Review*, 2011, 759.
- Sica S., Zeno Zencovich V., *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Dir. inf.*, 2010, 384.
- Silvestri G., *La ridefinizione del sistema delle fonti: osservazioni critiche*, in *Pol. dir.*, 1987, 149.
- Simoncini A., *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 2019, 1149.
- Simoncini A., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in Cavallo Perin R., Galetta D.U. (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 1.
- Simoncini A., *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale tra forma di stato e forma di governo*, in *Oss. fonti*, 2021, 727.
- Soro A., *Vulnerable Person: Data Protection and Digital Society*, in *Italian American Bar Ass'N Journal*, 2016, 117.
- Spangaro A., *Anche la Consulta ammette il mutamento di sesso senza il previo trattamento chirurgico*, in *Fam. dir.*, 2016, 639.
- Spoto G., *Disciplina del consenso e tutela del minore*, in Sica S., D'Antonio V., Riccio G.M. (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 111.
- Staiano S., *Legiferare per dilemmi sulla fine della vita: funzione del diritto e moralità del legislatore*, in *Federalismi.it*, n. 9/2012, 9.
- Stanca L., *L'Italia vista da fuori e da dentro*, 2019.
- Stanzione P., *Data protection and Vulnerability*, in *European Journal of Privacy Law and Tech*, 2020, 9.
- Stanzione P., Sciancalepore G., *Minori e diritti fondamentali*, Napoli, 2006.
- Stanzione P., *Transessualità voce*, in *Enc. dir.*, vol. XLIV, Milano, 1992, 874.
- Steinberg S.B., *Sharenting: Children's Privacy in the Age of Social Media*, in *Emory Law Journal*, 2017, 839.
- Stradella E., *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine cui prodest?*, in *Riv. AIC*, 2016, 22.
- Suárez-Álvarez R., Pastor-Rodríguez A., *Risks in Children's Digital Visibility and Vulnerability: Sharenting in France, Italy, Spain, and the United Kingdom*, in *European Journal of Children and Media Studies*, 2025/2026, 1.

- Sullivan C., *Digital Identity: An Emergent Legal Concept. The role and legal nature of digital identity in commercial transactions*, University of Adelaide Press, South Australia, 2011.
- Tega D., *La giurisprudenza costituzionale sul diritto al nome e all'identità personale. Il caso dei figli incestuosi*, in Honorati C. (a cura di), *Diritto al nome e all'identità personale nell'ordinamento europeo*, Milano, 2010, 75.
- Tepelena I., *The Legal Framework of Sharenting: Protecting Children's Rights in the Digital Age*, in *International Journal of Rights and Digital Law*, 2023, 93.
- Tommasi S., *The Liability of Internet Service Providers in the Proposed Digital Services Act*, in *European Review of Private Law*, 2022, 925.
- Tommasini R., *Identità personale tra immagine e onore: autonomia del valore ed utilità dello schema*, in *Rass. dir. civ.*, 1985, 84.
- Tonoletti B., *Fuga dal regolamento e confini della normatività nel diritto amministrativo*, in *Dir. amm.*, 2015, 371.
- Torchia L., *Lo Stato digitale*, Bologna, 2025.
- Torreggiani S., *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *Riv. it. inf. dir.*, 2021, 49.
- Trucco L., *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004.
- Usai A., *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. informazione*, 1993, 163.
- Van Dijk J., *The digital divide*, Cambridge, 2020.
- Varzi A.C., *Parole, oggetti, eventi e altri argomenti di metafisica*, Roma, 2001.
- Veronesi U., *Il diritto di morire. La libertà del laico di fronte alla sofferenza*, Mondadori, Milano, 2005.
- Villone M., *Il diritto di morire*, Napoli, 2011.
- Virgilio M.M., *Rassegna critica di lessico giuridico*, in *Ragion pratica*, 2015, 547.
- Visconti A.C., *Oltre la logica binaria...L'identità di genere tra vecchie e nuove prospettive*, in *Federalismi.it*, n. 15/2023, 240.
- Wagner G. et al., *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, 987.
- Warren S.D., Brandeis L.D., *The Right to Privacy*, in *Harvard Law Review*, 1890, 193.
- Zampetti E. (a cura di), *Lo stato verso l'automazione. L'informatica al servizio della Pubblica Amministrazione*, in *Concretezza*, 1970.
- Zanon N., *Corte costituzionale, evoluzione della "coscienza sociale", interpretazione della Costituzione e diritti fondamentali: questioni e interrogativi a partire da un caso paradigmatico*, in *Riv. AIC*, n. 4/2017, 1.
- Zei A., *Tecnica e diritto tra pubblico e privato*, Milano, 2008.
- Zeno-Zencovich V., *Onore e reputazione nel sistema del diritto civile: uno studio comparato*, Napoli, 1985.
- Zeno-Zencovich V., *Identità personale voce*, in *Dig. disc. priv.*, vol. IX, Torino, 1993, 22.
- Zeno-Zencovich V., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, 1.

Zuddas P., *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Oss. AIC*, 2020, 286.