



**Università
degli Studi
di Palermo**

Corso di dottorato in “Diritti umani: evoluzione, tutela e limiti” (Ciclo XXXVII)

Dipartimento di Giurisprudenza

NUOVE TECNOLOGIE E IDENTITÀ DIGITALE: SFIDE E PROSPETTIVE

COORDINATORE

CHIAR.MO PROF. PASQUALE DE SENA

RELATORE

CHIAR.MO PROF. RICCARDO URSI

CANDIDATA

DOTT.SSA LAURA CALANDRIELLO

A.A. 2024/2025

Indice

Introduzione.....	5
Inquadramento generale del tema.....	8
1. L'identità digitale nel nuovo millennio	8
1.1. <i>Dall'identità personale all'identità digitale</i>	<i>10</i>
1.2. <i>Le 'dimensioni' dell'identità digitale.....</i>	<i>14</i>
1.3. <i>L'identità digitale come diritto soggettivo autonomo?</i>	<i>17</i>
2. L'organizzazione multilivello dell'identità digitale.....	21
2.1. <i>Il d.lgs. 82/2005 (CAD)</i>	<i>23</i>
2.2. <i>Il regolamento 910/2014 (eIDAS)</i>	<i>27</i>
2.3. <i>Il regolamento 1183/2024 (eIDAS 2)</i>	<i>31</i>
3. Il sistema pubblico di identità digitale italiano (SPID).....	36
3.1. <i>Gli operatori e i livelli di sicurezza.....</i>	<i>38</i>
3.2. <i>Il ruolo dell'Agenzia per l'Italia Digitale</i>	<i>41</i>
3.3. <i>La cittadinanza digitale.....</i>	<i>42</i>
Tecnologie emergenti e ridefinizione dell'identità	47
1. Le nuove frontiere tecnologiche dell'identità digitale.....	47
1.1. <i>Intelligenza artificiale e machine learning.....</i>	<i>50</i>
1.2. <i>I sistemi di riconoscimento biometrico</i>	<i>57</i>
1.3. <i>La blockchain e le Distributed Ledger Technologies</i>	<i>63</i>
2. Identità digitale, profilazione e sorveglianza	68
2.1. <i>Tra sorveglianza e 'capitalismo'</i>	<i>69</i>
2.2. <i>Lo stato dell'arte dell'Internet governance e la 'terza via' europea</i>	<i>73</i>
3. Tipologie di sistemi di gestione dell'identità digitale	76
3.1. <i>Il modello centralizzato</i>	<i>78</i>
3.2. <i>Il modello federato</i>	<i>81</i>
3.3. <i>Il modello decentralizzato</i>	<i>83</i>
Quale futuro per l'identità digitale?.....	86
1. I futuri ostacoli della cittadinanza digitale	86
1.1. <i>Il digital divide</i>	<i>88</i>
1.2. <i>L'educazione digitale. Tra diritto sociale e cittadinanza</i>	<i>93</i>
2. Verso un nuovo paradigma di 'identità legale digitalizzata'	96
2.1. <i>Colmare il divario identitario con le tecnologie digitali</i>	<i>98</i>
2.2. <i>La centralizzazione e i limiti del tradizionale approccio all'identità digitale.....</i>	<i>100</i>
2.3. <i>Il nuovo paradigma dell'identità digitale auto-sovrana</i>	<i>103</i>
2.4. <i>L'identità digitale auto-sovrana nell'ottica della tutela dei diritti umani: sfide e prospettive</i>	<i>106</i>
3. Conclusioni. Il futuro dell'identità digitale tra realtà e mito	111

Bibliografia	116
---------------------------	------------

*Che sia con la macchina della verità di una blockchain
o con qualche altra tecnologia distribuita e libertaria,
abbiamo il dovere nei confronti dell'umanità
di restituire al soggetto umano
il compito di essere semplicemente al mondo.*

(M.J. Casey, P. Vigna, *La macchina della verità*)

Introduzione

La transizione digitale ha ridefinito i presupposti dell'agire individuale e collettivo, imponendo una riconsiderazione delle categorie giuridiche che governano i rapporti tra individuo, mercato e pubblici poteri.

In questo orizzonte, il concetto di identità si colloca al centro di un processo di trasformazione che incide sia sugli aspetti tecnico-funzionali (identificazione, autenticazione, imputazione degli atti), sia su quelli personali e sociali (rappresentazione di sé, reputazione, autonomia informativa).

È in questo snodo che prende forma l'identità digitale, crocevia in cui tecnologia, potere e diritti fondamentali si incontrano e talvolta collidono. Seppur correlata all'identità personale, l'analisi ricerca dei tratti propri: l'identità digitale si configura al contempo come infrastruttura tecnica e componente della soggettività, in quanto struttura accessi, ruoli, reputazioni e, non di rado, occasioni di cittadinanza nello spazio dei servizi e dei mercati.

Il presente lavoro si inserisce in tale quadro proponendo una lettura sistematica dell'identità digitale non soltanto come infrastruttura abilitante di diritti, ma anche come luogo di tensione in cui convergono esigenze di sicurezza, istanze di autodeterminazione e piani di *governance* multilivello. Ne derivano, accanto a nuove forme di partecipazione, simmetriche possibilità di esclusione che la trattazione intende mettere a fuoco nei loro presupposti teorici e nelle ricadute applicative.

L'elaborato si articola in tre capitoli che, pur distinti per obiettivi e metodo, concorrono a una ricostruzione unitaria del fenomeno.

Il primo capitolo intende chiarire le premesse teoriche e lessicali dell'indagine, ricostruendo il percorso che conduce dall'identità personale all'affermazione di una identità 'digitale', distinguendone altresì le principali 'dimensioni'. Una volta illustrata una possibile tassonomia dei concetti, il capitolo ricostruisce il quadro regolatorio multilivello, con attenzione agli attori coinvolti e ai livelli di garanzia.

Il secondo capitolo si concentra sul versante tecnico-operativo: esamina i tre 'motori di innovazione' (intelligenza artificiale, biometria, *blockchain*), evidenziandone promesse e criticità, dal rafforzamento della verificabilità e della sicurezza, ai rischi di profilazione e sorveglianza. Inoltre, la comparazione tra tre

archetipi architeturali di sistemi identitari – centralizzato, federato, decentralizzato – mostra come la tecnica non sia neutra: ogni modello distribuisce poteri, seleziona responsabilità, condiziona la profilazione e incide sulla resilienza del sistema.

Il terzo capitolo adotta invece una prospettiva proiettiva del fenomeno. Muovendo dalle acquisizioni teoriche e applicative precedenti, l'analisi valuta le ricadute dell'assetto esaminato sulla cittadinanza digitale.

Particolare spazio è infine riservato all'identità digitale auto-sovrana o *Self-Sovereign Identity* (SSI), considerata non solo come paradigma teorico ma come ipotesi operativa. Spostando il baricentro sull'utente, la SSI ridisegna la catena della fiducia e promette minimizzazione strutturale, portabilità transfrontaliera e assenza di archivi centrali.

La tesi ne analizza l'impatto giuridico in contesti differenti, interrogandosi, se e a quali condizioni possa favorire la costruzione di un'«identità legale digitalizzata» per soggetti oggi privi di *status* riconosciuti. Esamina inoltre le condizioni necessarie affinché l'attribuzione e la spendibilità di credenziali verificabili si traducano in riconoscimento opponibile *erga omnes*, oltre la fase sperimentale.

L'indagine non elude le criticità che oggi alimentano la «disillusione» nei confronti della SSI: l'usabilità dei *wallet*, la *governance* delle infrastrutture, il divario digitale – con il rischio connesso di una selettività sociale dell'innovazione – la compatibilità con i diritti di rettifica e cancellazione.

Dunque, il lavoro intreccia analisi concettuale, inquadramento normativo e valutazione istituzionale muovendo da una premessa da sottoporre a verifica critica: allo stato dell'arte non esiste identità senza Stato. L'innovazione, infatti, può decentralizzare custodia e presentazione, ma il riconoscimento, la validazione e la revoca restano probabilmente ancorati a un ordinamento che attribuisce effetti *erga omnes* agli attributi e presidia i conflitti.

Al tempo stesso, il lavoro non intende confondere la necessità di Stato con il centralismo informazionale. Sul solco dell'«umanesimo digitale»¹, la tesi esplora come una regia pubblica possa coesistere con la massima autodeterminazione

¹ Sul punto si rinvia a G. Gallone, *Riserva di umanità e funzioni amministrative*, Padova, 2023 e a J. Nida-Rümelin, N. Weidenfeld, *L'umanesimo digitale. Un'etica per l'epoca dell'Intelligenza Artificiale*, Milano, 2019.

dell'utente e la minima correlabilità dei dati, coniugando innovazione, sicurezza e inclusione.

CAPITOLO I

Inquadramento generale del tema

1. L'identità digitale nel nuovo millennio

L'avvento dell'era digitale e delle nuove tecnologie ha comportato una ridefinizione dei rapporti tra le persone e tra queste e le Istituzioni². Ciò a seguito di un'imprescindibile metamorfosi dei concetti di spazio e di tempo³, ma soprattutto del concetto di identità dell'individuo⁴ all'interno di una fase storica definita dalla dottrina come “quarta rivoluzione”⁵. Tale mutamento delle coordinate spazio-temporali tradizionali ha condotto verso l'enucleazione di due esistenze parallele, seppur interconnesse: quella biologica e quella virtuale⁶.

In tale contesto accanto al concetto di identità personale si è affermato quello di identità digitale. Seppur suscettibile di differenti declinazioni, quest'ultima può essere definita genericamente come la rappresentazione elettronica di un soggetto⁷, ma anche quell'insieme di dati e informazioni immesse in rete e riferibili a uno specifico soggetto-utente⁸.

² Preambolo della *Dichiarazione dei diritti in Internet*, approvata il 28 luglio 2015 dall'Ufficio di Presidenza della Camera dei deputati, su proposta della Commissione di studio istituita nel 2014 e presieduta da Stefano Rodotà. La Dichiarazione, sebbene priva di forza cogente, rappresenta il primo tentativo di sistematizzare, in chiave costituzionale, i diritti fondamentali nell'ecosistema digitale (diritto di accesso, neutralità della rete, tutela dei dati personali, diritto all'autodeterminazione informativa, diritto all'identità, protezione dell'anonimato, diritto all'oblio). Per un approfondimento si rimanda a L. Nannipieri, *Sulla “Dichiarazione dei diritti in Internet”. Alcune annotazioni critiche*, in *Inf. dir.*, 2/2014, 127 ss.

³ Si rinvia agli studi di N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2001.

⁴ Si veda Z. Bauman, *Intervista sull'identità*, Roma-Bari, 2003.

⁵ L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2007, 76-77. L'Autore definisce la “quarta rivoluzione” (il cui padre è il matematico Alan Turing) – dopo quella copernicana, darwiniana e freudiana – come il passaggio a un'epoca in cui gli uomini diventano organismi informazionali, reciprocamente connessi e parte di un ambiente informazionale (l'“infosfera”), condiviso con altri agenti informazionali, naturali e artificiali capaci di processare informazioni in modo logico e autonomo.

⁶ M. Farina, *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale: riflessioni (meta)giuridiche tra crisi di identità e necessità di tutela dei diritti fondamentali dell'individuo*, in *Rivista elettronica di Diritto, Economia, Management*, 1/2020, 42.

⁷ M. Nastri, *Identità digitale e identità personale: un percorso di sintesi*, in R. Giordano et al. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, 4.

⁸ G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in *Dir. fam.*, 3/2021, 1505.

L'identità digitale può essere dunque riferita all'identità impiegata nelle attività informatiche e, più in particolare, nelle variegate applicazioni di *Internet*⁹. Su tali premesse, comprendere il multiforme concetto di identità digitale costituisce un passaggio necessario per cogliere la portata stessa dell'era digitale¹⁰.

Sul piano strettamente funzionale l'identità digitale si compone di due momenti: l'accertamento dell'esistenza fisica di una persona e l'attribuzione a quest'ultima di credenziali informatiche (*password*, fattori biometrici, dispositivi crittografici) che consentono di stabilire un legame certo tra l'azione *online* e il suo autore¹¹.

Tale infrastruttura si è rivelata cruciale durante la crisi pandemica che, nell'accelerare il processo di digitalizzazione, ha evidenziato la necessità di disporre di strumenti di identificazione sicuri e affidabili per svolgere attività giuridicamente rilevanti *online* (accesso a prestazioni sanitarie, servizi fiscali, misure di sostegno economico etc.). In risposta a tale esigenza, gli interventi normativi adottati durante e dopo l'emergenza sanitaria hanno rafforzato la valenza giuridica e l'efficacia probatoria di strumenti già esistenti – su tutti SPID¹² e CIE – favorendo l'elaborazione di nuove prospettive normative orientate a una maggiore tutela e protezione dei dati personali e delle transazioni digitali.

Se l'accezione appena richiamata descrive l'identità digitale come strumento tecnico-operativo, una seconda accezione – di natura personale e sociale – riguarda, invece, la proiezione dell'identità individuale nel *web*. Profili sui *social network*, tracce di navigazione, interazioni nei sistemi di comunità virtuali concorrono a formare un 'sé' digitale che estende, integra e talvolta trasforma la percezione di sé e degli altri.

Tuttavia, qualunque sia l'angolatura prescelta, l'identità digitale si configura oggi come chiave di accesso imprescindibile alla dimensione virtuale, determinando tanto gli aspetti operativi (autenticazione, sicurezza), quanto quelli esistenziali (autodeterminazione, reputazione).

⁹ M. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam.*, 2/2016, 963.

¹⁰ Cfr. S. Bonavita, *Il corpo elettronico*, in G. Cassano, S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020.

¹¹ G. Resta, *Identità personale e identità digitale*, in *Dir. inform. e inf.*, 3/2007, 515; M. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, cit., 964; G. Garofalo, *Identità digitale e diritto all'oblio*, cit., 1506.

¹² Sul punto *infra* §3.

Il presente capitolo prende le mosse da tali premesse teoriche per analizzare la natura e le implicazioni dell'identità digitale, adottando una prospettiva interdisciplinare che intreccia riflessione giuridica, evoluzione tecnologica e trasformazioni sociali. L'intento è dunque quello di definire il concetto di identità digitale nella sua transizione dall'identità personale (§ 1.1), alla luce delle sue differenti 'dimensioni' (§1.2).

Nel prosieguo, si indagherà circa il possibile riconoscimento dell'identità digitale quale posizione giuridica soggettiva tutelata (§ 1.3) e infine, saranno oggetto di analisi i 'pilastri' regolatori multilivello (§2-3) e il caso-studio del Sistema Pubblico di Identità Digitale (SPID) con l'obiettivo di mostrare come tali fonti e istituti concorrano alla costruzione di una cittadinanza digitale sostanziale.

1.1. Dall'identità personale all'identità digitale

Il concetto di identità digitale, oggetto di indagine, ha origine in ambito più propriamente informatico per riassumere in un'unica nozione i sistemi che individuano le credenziali di accesso a risorse informatiche¹³. Tuttavia, la continua evoluzione della tecnologia ha avvicinato il concetto di identità digitale, inizialmente circoscritto all'identificazione di un'utenza di servizi *online*, a quello di identità personale¹⁴. Ciò ha inevitabilmente comportato un'evoluzione stessa del suo significato per l'emergere di nuove e più complesse esigenze di protezione dell'individuo conseguentemente allo sviluppo delle relazioni via *Internet*.

¹³ M.F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, cit., 2016, 953.

¹⁴ Per un approfondimento sul tema del diritto all'identità personale v. Z. Zencovich, (voce) *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993; G. Finocchiaro, (voce) *Identità personale (diritto alla)*, in *Dig. disc. priv., sez. civ.*, V agg., Torino, 2010; G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003; L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004; G. Resta, *Identità personale e identità digitale*, cit.; E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, in *Forum Quad. Cost.*, 26 gennaio 2010; M. Luciani, *Quale identità?*, in A. Somma et al. (a cura di), *Dialoghi con Guido Alpa*, Roma, 2018; A. Randazzo, *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *dirittifondamentali.it*, 3/2021, 363-392; G. Bavetta, (voce) *Identità (diritto alla)*, in *Enc. dir.*, XIX, Milano, 1979; 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 *Rivista AIC*, 4/2016, 1-29; F. Remotti, *Contro l'identità*, Roma-Bari, 2001; A. Morelli, *Persona e identità personale*, in *BioLaw Journal*, 2/2019; S. Niger, *Il diritto all'identità personale*, in G. Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Padova, 2008, 113 ss.

Tale circostanza ha provocato un'ulteriore complessità nell'individuazione di una definizione univoca di identità digitale lasciando spazio a un'accezione di identità digitale intesa quale sintesi ideale della personalità del soggetto esplicantesi in rete, una proiezione di sé stessi sul *web*¹⁵.

In questa prospettiva, da istituto autonomo, l'identità digitale è confluita progressivamente nel più ampio concetto di identità personale¹⁶.

Basti pensare alla circostanza per cui ogni questione relativa all'identità personale è ormai riproponibile – seppur con altri presupposti e implicazioni¹⁷ – nel mondo digitale¹⁸. Del resto, «la piena affermazione dell'individuo nel mondo della rete induce altresì a riconoscere la più completa evoluzione e il più spiccato dinamismo del concetto di identità personale, che si arricchisce di una nuova dimensione della personalità, di matrice digitale e dei diritti ad essa connessi»¹⁹.

Dunque, per comprendere il concetto di identità digitale in questo scenario evolutivo è necessario considerare preliminarmente quello di identità personale.

Al concetto di identità personale è possibile attribuire differenti significati, tutti legati alla necessità di definire ciò che una persona è all'interno di un processo di costruzione e di identificazione con uno o più modelli rinvenibili in un dato ambiente sociale²⁰. Possiamo sin da subito affermare che l'identità personale è il risultato – continuamente rivedibile – di un processo di identificazione.

Come accennato l'espressione 'identità personale' assume più valenze semantiche e il dibattito circa la sua definizione e portata è di natura storicamente dottrinale e giurisprudenziale, sviluppatosi in tempi più risalenti.

¹⁵ Cfr. S. Rodotà, *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Bari, 2004; S. Turkle, *Life on the Screen. Identity in the Age of the Internet*, Simon & Schuster, New York, 1995; G. Sciulli, *Il diritto all'oblio e l'identità digitale*, Bologna, 2014.

¹⁶ M. Natri, *Identità digitale e identità personale*, cit., 5.

¹⁷ G. Resta, *Identità personale e identità digitale*, cit., 512 ss. V. S. Rodotà, *Identità e Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari-Roma, 2018, il quale afferma che «[...] La frontiera tra fisicità e digitalità non ha più ragione di esistere».

¹⁸ G. Alpa, *Il diritto di essere sé stessi*, Milano, 2021. Secondo l'Autore «l'identità personale è diventata un'espressione polisensa e con molti margini di ambiguità»; inoltre, secondo l'A., «identità 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». Sul tema v. P. Gleason, *Identifying Identity. A Semantic History*, in *The Journal of American History*, vol. 69, 4/1983.

¹⁹ A. Palladino, «Oblio 4.0» tra identità digitale e cancellazione dati: quale diritto?, in *De Iustitia*, 2/2019, 76.

²⁰ G. Pino, *L'identità personale*, in S. Rodotà, M. Tallacchini (a cura di), *Trattato di biodiritto*, vol. I, *Ambito e fonti del biodiritto*, Milano, 2010, 298.

Segnatamente, il dibattito sul tema ha favorito la creazione di due distinte nozioni di identità personale, una che possiamo definire ‘estrinseca’ e una ‘sostanziale’²¹. La prima e più risalente accezione²² fa riferimento all’esigenza di identificabilità dei soggetti da parte del pubblico potere all’interno di un processo di autenticazione soggettiva²³. In tale prospettiva, la dottrina più recente ha definito tale declinazione di identità personale come ‘anagrafica’²⁴, in quanto riferita al complesso delle risultanze anagrafiche che servono a identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati²⁵.

Oltre a quanto messo in evidenza con riferimento agli strumenti di identificazione dell’individuo, può rintracciarsi – in chiave sostanziale – una seconda nozione di identità personale. Tale accezione è stata oggetto di un’elaborata costruzione giuridica i cui fattori propulsivi sono connessi alla maggiore attenzione dei Paesi occidentali rispetto ai valori stessi della persona, e quindi alla tematica delle sue rappresentazioni sui *mass media*²⁶.

Se in una prima fase questa declinazione dell’identità personale è stata ricostruita come «diritto ad essere correttamente rappresentati»²⁷, a partire dalla storica

²¹ G. Pino, *L’identità personale*, cit., 300.

²² G. Alpa, *L’identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 3/2017, 723-724: «L’identità della persona era conchiusa nella sua consistenza fisica ed affidata ad alcuni riferimenti precisi, tendenzialmente immodificabili, burocraticamente registrabili: il nome, la cittadinanza, il sesso, l’altezza, il colore degli occhi e dei capelli, gli eventuali segni particolari, la città di nascita, il nome dei genitori, lo stato familiare, la professione esercitata, la residenza».

²³ G. Resta, *Identità personale e identità digitale*, cit., 612.

²⁴ G. Pino, *L’identità personale*, cit.: l’Autore afferma come in tal senso il rilievo giuridico dell’identità personale consiste nell’insieme dei segni distintivi esteriori della persona: il nome, determinate caratteristiche somatiche (altezza, sesso), indirizzo di residenza, ovvero in ciò che può rendere quella persona facilmente identificabile; v. anche G. Falco, *Identità personale*, in *Nuovo dig. it.*, VI, Torino, 1938: l’A. aveva considerato l’identità personale come un qualche cosa costituito dall’insieme dei caratteri (connotati e contrasegni personali) e dal nome (generalità), affermando che fissare in un documento identificativo i caratteri e il nome di una persona vuol dire fissarne l’identità.

²⁵ V. Z. Zencovich, *Identità personale*, cit., 294.

²⁶ G. Pino, *L’identità digitale e la tutela della persona*, cit., 723.

²⁷ V. una prima dottrina, A. De Cupis, *Il diritto all’identità personale. Parte prima: il diritto al nome*, Milano, 1949 e la prima giurisprudenza: Pretura di Roma del 6 maggio 1974, ma anche Corte Cass. n. 3769 del 22 giugno 1985. La Corte di Cassazione con sentenza n. 3769/1985 relativa al “caso Veronesi” ha elaborato una definizione specifica del diritto all’identità personale, riconoscendo che: «ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale e particolare, è conosciuta o poteva essere conosciuta con l’applicazione dei criteri della normale diligenza e della buona fede soggettiva; 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 ed univoche, destinato ad estrinsecarsi nell’ambiente sociale».

sentenza della Corte costituzionale del 1994 la stessa si è evoluta verso l'affermazione del «diritto ad essere sé stessi»²⁸.

Nell'abbracciare le attività del soggetto, le sue posizioni professionali, culturali, ideologiche, religiose, sociali, l'identità personale si traduce in una sintesi della "storia" di ciascun soggetto che permette a ogni consociato di essere identificato come una persona ben precisa (la cui vita passata e presente è, ovviamente, caratterizzata da determinate vicende). È in questa prospettiva che, con un'espressione che ha assunto in tempi più recenti dignità normativa, si discute ormai comunemente di diritto all'identità personale²⁹.

Nell'ambito della normativa di rango primario, essa è espressamente impiegata sia all'art. 1 della legge 31 dicembre 1996, n. 675³⁰, sia all'art. 2 del decreto legislativo 30 luglio 2003, n. 196³¹, ora modificato dal decreto legislativo 10 agosto 2018, n. 101, che ha adeguato la normativa nazionale alle disposizioni del Regolamento generale per la protezione dei dati personali n. 2016/679 dell'Unione europea (c.d. GDPR)³².

In questa prospettiva, l'identità digitale assume pertanto la stessa natura bifronte dell'identità personale: da un lato, accogliendo una prospettiva più sostanziale, la stessa può essere intesa come *alter ego* virtuale della persona (e dunque come veicolo di espressione sostanziale della personalità); dall'altro, accogliendo invece una nozione più tecnica, l'identità digitale diviene l'insieme delle informazioni che consentono l'identificazione dell'individuo.

²⁸ Corte Cost., 3 febbraio 1994, n. 13, in *Foro.it*, 1994, I, 1668, che configura il diritto all'identità personale come «[...] 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, e al tempo stesso qualificano, l'individuo».

²⁹ Z. Zencovich, *Identità personale*, cit.,

³⁰ Art. 1, co. 1., L. 31 dicembre 1996, n. 675: «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».

³¹ Art. 2, co. 1, d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali): «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».

³² Il Regolamento (UE) 2016/679 (GDPR), in vigore dal 2018, uniforma nell'Unione europea la tutela dei dati personali fondandosi su principi di trasparenza, minimizzazione e *accountability*.

Sulla base di quanto fin qui rappresentato, può sottolinearsi come l'evoluzione giuridica abbia enucleato ulteriori sfumature dell'identità personale e una 'nuova antropologia'³³.

Da strumento di autenticazione, l'identità digitale diviene vera e propria componente della soggettività, veicolo di rappresentazione e interazione sociale, con effetti diretti sull'immagine, sulla reputazione e, più in generale, sulla dignità dell'individuo³⁴. Dunque, la coesistenza di queste due dimensioni – tecnica e sostanziale – impone di considerare l'identità digitale come area di intersezione tra esigenze di sicurezza, istanze di autodeterminazione informativa e tutela dei diritti della personalità.

1.2. Le 'dimensioni' dell'identità digitale

Le molteplici sfaccettature dell'identità digitale possono essere ricondotte a due piani tra loro intrecciati: uno teorico e uno funzionale.

Sul primo versante è necessario richiamare la ricostruzione elaborata da Stefano Rodotà. Quest'ultimo, come è noto, ha introdotto l'idea di una 'nuova antropologia' al fine di rappresentare la profonda trasformazione dell'identità umana dalla “*natural person*” alla “*digital person*” (ossia un'entità che si presenta sempre più frequentemente come un complesso aggregato di dati)³⁵. È in tale contesto che emerge nel dibattito giuridico italiano una visione più articolata in cui realtà fisica e rappresentazione digitale si uniscono in un intreccio indissolubile³⁶.

Parallelamente, il confronto sul tema – nel dibattito oltreoceano – si era già esteso fino al punto da considerare il concetto di 'persona digitale' come un modello di

³³ S. Rodotà, *Il diritto di avere diritti*, Bari, 2012, 14-15.

³⁴ G. Alpa, *L'identità digitale e la tutela della persona*, cit., 723 ss. L'Autore afferma che la dimensione digitale costituisce un prolungamento della dimensione umana.

³⁵ S. Rodotà, *Il diritto di avere diritti*, cit., 396: l'A. afferma che: «Anche se è eccessivo, e persino pericoloso, dire che “noi siamo i nostri dati”, è tuttavia vero che la nostra rappresentazione sociale è sempre più affidata a informazioni sparse in una molteplicità di banche dati, ed ai “profili” che su questa base vengono costruiti, alle simulazioni che permettono. Siamo sempre più conosciuti da soggetti pubblici e privati attraverso i dati che ci riguardano, in forme che possono incidere sull'eguaglianza, sulla libertà di comunicazione, di espressione o di circolazione, sul diritto alla salute, sulla condizione di lavoratore, sull'accesso al credito e alle assicurazioni, e via elencando. Divenute entità disincarnate, le persone hanno sempre di più bisogno di una tutela del loro “corpo elettronico”».

³⁶ S. Rodotà, *Il diritto di avere diritti*, cit., 395: secondo l'Autore non siamo di fronte a una persona virtuale contrapposta a quella reale, bensì a un inedito e inestricabile intreccio.

personalità individuale pubblica basato su dati e mantenuto da transazioni elettroniche³⁷. In questo senso, sono stati identificati due principali tipologie di persona digitale: da un lato la persona digitale ‘progettata’, risultante dalla scelta consapevole dell’individuo di condividere determinati dati e plasmare attivamente la propria esistenza *online*; dall’altro, la persona digitale ‘imposta’, derivante dall’elaborazione di dati da parte di terzi, spesso in assenza di un’esplicita autorizzazione del soggetto interessato.

A questa bipartizione si è aggiunta, in seguito, una terza dimensione, quella della persona digitale “ibrida”, che scaturisce dalla combinazione di dati volontariamente condivisi con altri raccolti e trattati in maniera automatizzata da piattaforme e soggetti terzi³⁸.

Sul piano funzionale, invece, l’identità assume forme diverse a seconda degli usi e dei contesti – anche nella sua proiezione digitale – dando luogo a ulteriori tassonomie proposte dalla dottrina³⁹.

Si parla di identità funzionale per indicare quella utilizzata ai fini dell’autenticazione in relazione a specifici servizi⁴⁰. Essa consente al soggetto di accedere a contesti determinati e può assumere molteplici forme, anche transnazionali⁴¹.

Diversa è invece l’identità di base, o legale, che rappresenta il riconoscimento giuridico fondamentale della persona. Rilasciata da una fonte affidabile e autorevole, essa consente all’individuo di dimostrare chi è, assicurando un punto di riferimento unitario per la sua identificazione nell’ordinamento di appartenenza.

³⁷ R. Clarke, *The Digital Persona and Its Application to Data Surveillance*, in *The Information Society*, 10/1994, 77-92.

³⁸ A. Roosendaal, *Digital Personae and Profiles as Representations of Individuals*, in *Privacy and Identity: IFIP AICT*, vol. 320, 2010, 226-236.

³⁹ La distinzione tra identità digitali “forti” e “deboli” è ricavabile dall’attività ermeneutica giurisprudenziale. Il Consiglio di Stato ha fornito la differenza tra molteplicità identitarie definendo le prime «quelle direttamente disciplinate dalla legge allo scopo di rafforzare la garanzia dell’uso pubblico della firma digitale» e le seconde «quelle che vengono utilizzate dagli operatori *online* per l’accesso a servizi digitali non pubblici utilizzando sostanzialmente una password eventualmente insieme ad altre credenziali d’accesso» (Cons. Stato, sez. IV, 24 marzo 2016, n. 1214).

⁴⁰ La tripartizione proposta nella trattazione è di V. Graf Narbel, *Digital Identity*, in M. Marelli (ed.), *Handbook on Data Protection in Humanitarian Action*, Cambridge University Press, 2004, 212-229. L’Autore chiarisce come l’identità digitale sia strettamente correlata ad altri concetti quali l’identificazione, l’identità funzionale, l’identità legale e l’identità personale.

⁴¹ Si pensi ad esempio alla tessera universitaria, al certificato elettorale o alle credenziali predisposte per programmi di assistenza sociale, V. Graf Narbel, *Digital Identity*, cit., 215.

Pur essendo unica in un determinato contesto nazionale, non è escluso che una stessa persona possa disporre di più identità legali, ad esempio attraverso passaporti rilasciati da diversi Stati⁴².

Accanto a queste due dimensioni più formali, si colloca l'identità concettuale, o personale, che riguarda la proiezione di sé nel tessuto sociale e relazionale. Essa si esprime tanto nella percezione che ha l'individuo di sé stesso quanto nel modo in cui viene riconosciuto dagli altri e si fonda su attributi immateriali, variabili e culturalmente determinati⁴³. Queste tre dimensioni, elaborate per descrivere le modalità con cui l'identità si manifesta nel mondo fisico e giuridico, trovano un'immediata trasposizione anche nello spazio digitale⁴⁴.

Si delinea, infine, un'ulteriore e inedita declinazione: l'identità 'algoritmica'. Essa concerne il profilo generato senza intervento diretto dell'interessato, bensì in modo automatico e involontario quale esito della mera navigazione *online*⁴⁵.

L'impiego di *cookies* e la raccolta passiva di tracce digitali consentono di elaborare profili estremamente dettagliati degli utenti, aggregando informazioni relative a gusti, preferenze e comportamenti. Tali dati, gestiti principalmente da soggetti terzi e destinati prevalentemente a finalità commerciali, sfuggono in larga misura al controllo diretto degli interessati.

Ne risulta un intreccio complesso di livelli identitari che coesistono e spesso si sovrappongono; è proprio questa stratificazione a determinare una frammentazione del sé digitale.

⁴² V. Graf Narbel, *Digital Identity*, cit., 215.

⁴³ *Ibidem*.

⁴⁴ Sul punto v. anche D. Birch, *Identity is the New Money*, London Publishing Partnership, 2004. L'A., esperto di politiche sull'identità, distingue tre dimensioni fondamentali dell'identità: quella giuridica, connessa alla possibilità di essere individuati in quanto soggetti di diritto; quella sociale, determinata dall'intreccio di relazioni e interazioni con la comunità di appartenenza; e quella personale, legata all'autopercezione. Mentre la prima rimane relativamente stabile, le ultime due risultano sempre più fluide, soprattutto nell'epoca dei *social media* e delle trasformazioni culturali che incidono sulla definizione dell'essere umano in rapporto a genere, orientamento sessuale, appartenenza religiosa o etnica. L'elemento innovativo, secondo Birch, risiede nel fatto che le nuove tecnologie non solo favoriscono tali mutamenti identitari, ma consentono altresì di trasformare questi aspetti dinamici in strumenti di prova e di riconoscimento, in particolare nel dominio dell'identità sociale.

⁴⁵ M. Farina, *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale*, cit., 47.

1.3. L'identità digitale come diritto soggettivo autonomo?

A questo punto della trattazione occorre interrogarsi circa la possibilità che l'identità digitale si configuri come posizione giuridica soggettiva autonoma⁴⁶.

La questione impone di misurare l'istituto in esame alla luce di tre requisiti tradizionalmente indicati e altresì sviluppati dalla giurisprudenza costituzionale: (i) il riconoscimento, o tipizzazione, da parte dell'ordinamento; (ii) l'esistenza di un obbligo giuridico speculare in capo a un soggetto determinato; (iii) il carattere dell'effettività (giustiziabilità) dell'asserita posizione giuridica soggettiva.

Sul primo versante, l'identità digitale ha ricevuto riconoscimento positivo – come si vedrà nel prosieguo – attraverso il Regolamento (UE) n. 910/2014, comunemente noto come Regolamento eIDAS (§ 2.2). Esso ha istituito un quadro comune per l'identificazione elettronica, fissando le condizioni per il reciproco riconoscimento dei mezzi di identità digitale tra gli Stati membri. Il quadro normativo è stato recentemente aggiornato dal Regolamento (UE) 2024/1183 (eIDAS 2) (§ 2.3) con l'intento di garantire un'identità digitale europea a cittadini e imprese, richiedendo agli Stati membri di fornire portafogli di identità digitale interoperabili entro il 2026.

Nella prospettiva nazionale, invece, l'identità digitale beneficia di un riconoscimento legislativo esplicito all'art. 3-*bis* del Codice dell'Amministrazione Digitale (§ 2.1), il quale stabilisce che «ogni individuo ha il diritto di accedere ai servizi *online* offerti [...] tramite la propria identità digitale»⁴⁷. Dunque, tale assetto

⁴⁶ Sul tema dei 'nuovi diritti' si rimanda a F. Modugno, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995; R. Guastini, *Diritti*, in P. Comanducci, R. Guastini (a cura di), *Analisi e diritto*, Torino, 1994; G. Zagrebelsky, *Il diritto mite*, Torino, 1992; R. Bin, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992; E. Denninger, *Diritti all'uomo e Legge fondamentale*, Torino, 1998. Sul tema del costituzionalismo digitale si rinvia a T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 4/2020, 465 ss.; P. Costanzo, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in *Rass. parl.*, 4/2012, spec. 852; V. Cavani, *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in *Dir. pubbl. comp.*, 1/2023, 223 ss.; E. Longo, A. Pin, *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *DPCE*, 1/2023, 103 ss.; O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quad. cost.*, 3/2023, 569 ss.; C. Spiniello, *È (ancora) tempo di costituzionalismo digitale*, in *Rivista italiana di informatica e diritto*, 1/2025, 580 ss.

⁴⁷ La *Carta dei diritti fondamentali dell'Unione Europea* (Carta di Nizza) fornisce un fondamento assiologico. L'articolo 7 stabilisce la tutela della vita privata e familiare, mentre l'articolo 8 sancisce il diritto autonomo alla protezione dei dati personali, evidenziando l'importanza di gestire l'identità, specialmente in contesti digitali, nel rispetto della persona e delle sue informazioni. La *Dichiarazione europea sui diritti digitali*, adottata nel 2022, ha enunciato in modo esplicito il diritto

sembra soddisfare il primo indice del diritto soggettivo, individuando l'identità digitale come posizione giuridica soggettiva protetta. Tuttavia, l'identità digitale resta un "bene strumentale" – vale a dire un *facilitator* per l'esercizio di diritti ulteriori (partecipazione ai procedimenti, *welfare*, istruzione, ecc.) – e non il fine che l'ordinamento intende garantire in sé. Da qui la prima frizione: il diritto viene enunciato in formula ampia («diritto di accedere ai servizi *online* tramite identità digitale»), ma la sua portata pratica è inevitabilmente mediata dal catalogo di servizi effettivamente digitalizzati e dall'architettura dei sistemi nazionali (SPID, CIE, e in futuro EUDI *Wallet*).

Il secondo requisito risulta più complesso; nella concezione classica, ogni diritto soggettivo postula un dovere giuridico speculare (certo e imputabile). Per l'identità digitale tale dovere appare pluristratificato e, in parte, diffuso. Gli attori sono molteplici: lo Stato e le pubbliche amministrazioni⁴⁸; gli *identity/wallet providers*⁴⁹; i *relying parties* (imprese e P.A. che accettano l'identità)⁵⁰. A meno di voler riconoscere l'esistenza di una 'responsabilità a mosaico' di difficile lettura, non può che segnalarsi la difficoltà di individuare un soggetto unico su cui concentrare gli obblighi speculari all'asserito diritto all'identità digitale.

Per quanto concerne invece la verifica della terza condizione circa la giustiziabilità⁵¹, essa risulta un compito di notevole complessità in quanto la stessa conduce a esiti diversi a seconda della dimensione dell'identità digitale presa in considerazione. Se è vero che nella sua accezione di 'identità personale virtuale',

di ogni individuo a possedere un'identità digitale che sia sicura, accessibile e affidabile. Questa affermazione è in linea con il riconoscimento del diritto fondamentale alla protezione dei dati personali, come stabilito dall'articolo 8 della Carta di Nizza.

⁴⁸ Gli Stati e le pubbliche amministrazioni sono chiamati a predisporre soluzioni di identità digitale a livello "elevato" di sicurezza e ad assicurare che i propri servizi siano accessibili tramite tali strumenti, in conformità a quanto previsto dall'art. 64 del Codice dell'amministrazione digitale e dagli artt. 5-*bis* e 6-*octies* del Regolamento (UE) 2024/1183 (c.d. eIDAS 2).

⁴⁹ Gli *identity e wallet providers*, una volta accreditati, sono tenuti al rispetto di obblighi stringenti di correttezza, continuità del servizio e protezione dei dati personali degli utenti, come stabilito dall'art. 6-*septies* del Regolamento eIDAS 2 e dalle Linee guida AgID.

⁵⁰ Le *relying parties*, siano esse imprese o pubbliche amministrazioni, non possono esigere attributi eccedenti il necessario, né rifiutare in modo discriminatorio il mezzo conforme, come previsto dall'art. 6-*novies* del Regolamento eIDAS 2.

⁵¹ A. Barbera, "Nuovi diritti": *attenzione ai confini*, in L. Califano (a cura di), *Corte costituzionale e diritti fondamentali*, Torino, 2004: «Chi prospetta l'esistenza di una posizione giuridica soggettiva dovrebbe avere parimenti l'onere di dimostrare ai sensi dell'art. 24, comma 1, della Costituzione la sua concreta giustiziabilità».

l'identità digitale risulta essere suscettibile di tutela⁵², ci si domanda se nella sua dimensione istituzionale-tecnica la risposta sia altrettanto immediata.

La sottrazione o l'utilizzo abusivo dell'identità digitale attiva un ventaglio di rimedi su più fronti. Se da un lato è attivabile una tutela di tipo amministrativo e paragiurisdizionale, attraverso l'ausilio dell'*identity provider* e dell'AgID⁵³, è altresì possibile attivare una tutela giurisdizionale sia civile sia amministrativa. Segnatamente è infatti possibile attivare un'azione di responsabilità contrattuale verso l'*identity provider* per inadempimento delle obbligazioni di custodia (artt. 1218-1228 c.c.) e aquiliana contro l'autore materiale del furto (art. 2043 c.c.). Inoltre, nel caso di dinieghi o revoche d'ufficio dell'identità digitale da parte della pubblica amministrazione è possibile attivare tutela giurisdizionale dinanzi al TAR ex art. 133 lett. e), n. 1, c.p.a.

Alla luce di questi elementi, la qualificazione dell'identità digitale come diritto soggettivo resta comunque discutibile, così come il suo inquadramento tra i diritti fondamentali di “quarta generazione”⁵⁴.

Essa rappresenta però un mezzo imprescindibile della cittadinanza digitale: l'identità digitale si configura oggi come infrastruttura abilitante della cittadinanza nell'ecosistema amministrativo e di mercato. Tuttavia, si tratta pur sempre di un diritto strumentale al godimento di diritti sostanziali già tipizzati – dall'eguaglianza sostanziale (art. 3 Cost.) al principio di buon andamento (art. 97 Cost.) – piuttosto che di una posizione primaria autonoma.

⁵² La giurisprudenza di legittimità ha riconosciuto all'identità personale dignità di diritto fondamentale, distinto da nome, immagine e onore, e riconducibile ai diritti della personalità (Cass. civ., n. 8827/2010). L'identità digitale può essere considerata, in questa prospettiva, come proiezione in ambiente telematico del medesimo diritto (§1.1).

⁵³ L'Agenzia per l'Italia Digitale (AgID), istituita dal d.l. 83/2012, è l'ente nazionale competente per l'attuazione delle politiche di digitalizzazione e, in particolare, per la vigilanza e l'accreditamento degli *identity provider* e dei gestori di servizi fiduciari qualificati, ai sensi del Codice dell'amministrazione digitale e del Regolamento (UE) n. 910/2014 (eIDAS).

⁵⁴ Per un approfondimento sulla suddivisione elaborata tra diritti di prima generazione (diritti civili e politici), di seconda generazione (diritti sociali) e di terza generazione (categoria residuale che comprende i c.d. diritti verdi) si rimanda a K. Vasak, *A 30 years struggle. the sustained efforts to give force of law to the Universal Declaration of Human Rights*, in *The UNESCO Courier*, 1977, 29-32. Per l'emergere di una eventuale ‘quarta generazione’ di diritti, riconducibile alla sfera digitale, biotecnologica e algoritmica, si rimanda a S. Rodotà, *Tecnologie e diritti*, Bologna, 2021. In termini critici sulle ricostruzioni volte a rappresentare i diritti attraverso una prospettiva generazionale v. G. Pino, *Diritti sociali. Per una critica di alcuni luoghi comuni*, in *Ragion Pratica*, 2/2016, 498.

Per tali ragioni, il dibattito non può esaurirsi nella sola qualificazione dogmatica: la natura ancora ‘in transizione’ dell’istituto rinvia al tema della *governance* e delle architetture istituzionali che ne regolano l’attuazione. Ne discende la necessità di esaminare il contesto multilivello all’interno del quale l’identità digitale si manifesta, si consolida e trova le proprie regole di funzionamento.

2. L'organizzazione multilivello dell'identità digitale

Il paragrafo precedente ha mostrato come l'identità digitale, nata al tempo stesso come strumento funzionale e costruzione sociale, abbia progressivamente assunto una fisionomia giuridica complessa.

In questa parte dell'indagine si analizzerà il tessuto normativo riferito all'istituto nella sua accezione tecnico-giuridica, quale mezzo abilitante per l'erogazione di servizi pubblici e come strumento regolato da un complesso di norme di matrice europea e nazionale. Ciò attraverso l'analisi di quelli che possono essere considerati i 'pilastri' regolatori dell'istituto.

Fino a pochi anni fa, il termine 'identità digitale' pur essendo diffusamente utilizzato nella prassi amministrativa e nelle scienze informatiche, era sfornito di una definizione formale univoca (sia a livello interno sia sovranazionale).

Attraverso l'evoluzione delle politiche di digitalizzazione il concetto ha acquisito dignità giuridica, in particolare nel contesto della trasformazione digitale della pubblica amministrazione e della realizzazione del mercato unico digitale europeo. Tuttavia, ancora oggi non si può affermare che la nozione di identità digitale dettata dalla legge sia perfettamente coincidente con l'espressione impiegata nella prassi forense e giudiziaria. Sarà dunque utile indagare su cosa la legge intenda per identità digitale.

A livello nazionale, una prima definizione è stata introdotta nel 2014⁵⁵ con un decreto attuativo del Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82), in riferimento al Sistema Pubblico di Identità Digitale (SPID)⁵⁶. La disposizione in questione stabilisce che l'accesso all'identità digitale federata⁵⁷ di

⁵⁵ Il primo riferimento di carattere non definitorio nell'ordinamento nazionale di identità digitale è risalente all'anno precedente (2013), contenuto nel comma terzo dell'art. 640-ter del Codice penale che punisce il reato di frode informatica. Commette tale reato «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» con l'aggravante prevista al comma terzo e la conseguente procedibilità d'ufficio per fatti commessi «con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti». In questo caso l'identità digitale oggetto di furto è riferita alle credenziali di accesso ad un sistema informatico.

⁵⁶ D.P.C.M. 24 ottobre 2014, 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. In particolare, la definizione di identità digitale è contenuta nell'art. 1, lett. o).

⁵⁷ Il concetto di 'identità federata' è legato all'*identity management*; essa assimila ed estende alla cooperazione applicativa i concetti tipici del modello RBAC (*Role Based Access Control*), in cui i

cittadini e imprese avvenga previa identificazione personale e attraverso il rilascio di credenziali sicure, sottolineando implicitamente lo stretto collegamento tra identità fisica e digitale.

La disciplina è stata adottata a seguito del recepimento in ambito unionale del Regolamento (UE) 23 luglio 2014 n. 910 (eIDAS) che ha introdotto un quadro normativo volto a garantire il riconoscimento transfrontaliero dei mezzi di identificazione elettronica e a disciplinare i servizi fiduciari per le transazioni elettroniche⁵⁸. Il Regolamento riconosce all'identità digitale la funzione di elemento chiave per assicurare la riconoscibilità dell'individuo nei diversi sistemi informatici, in modo analogo a quanto avviene per l'identità fisica nei rapporti *offline*. Nasce, pertanto, il concetto di identità digitale federata a spendita generalizzata, intesa come corrispondenza tra una specifica persona fisica e le sue credenziali di accesso a un dato sistema informatico, così da permetterne la riconoscibilità nei molteplici sistemi di identificazione del cyberspazio come avviene per l'identità fisica. Tale intervento europeo nell'ambito dell'identificazione digitale si fonda sull'obiettivo politico ed economico di realizzare un "mercato unico digitale" efficiente, interoperabile e sicuro.

Allo stesso tempo, l'ordinamento italiano si è mosso per promuovere la digitalizzazione della pubblica amministrazione, al fine di migliorarne l'efficienza, razionalizzare l'allocazione delle risorse e rafforzare la fruibilità dei diritti da parte dei cittadini⁵⁹.

diritti di accesso a una data risorsa sono basati sul ruolo posseduto dall'utente. Una gestione dell'identità federata prevede in pratica la creazione di relazioni di fiducia tra realtà diverse per l'identificazione e l'autorizzazione degli utenti di una di esse ad accedere alle risorse governate da un'altra.

⁵⁸ Il Regolamento eIDAS distingue i concetti di 'identificazione elettronica' inteso come processo che collega un'identità fisica a un insieme di dati di identità, da quelli di 'identità digitale' inteso come *output* stabile di quel processo e 'autenticazione' inteso, invece, come verifica in tempo reale di tale collegamento.

⁵⁹ Sull'argomento si rinvia a L. Torchia, *Lo Stato digitale*, Bologna, 2023; R. Cavallo Perin-D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020; V. Bontempi (a cura di), *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, 2022; S. Palumbo, *La transizione digitale della pubblica amministrazione italiana nella prospettiva europea. Considerazioni alla luce del Piano nazionale ripresa e resilienza*, in *Dir. econ.*, 1/2023, 163 ss.; F. Luciani, *Brevi note sull'innovazione tecnologica come strumento di buona amministrazione*, in *La Cittadinanza europea*, 2/2022, 199 ss.; F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il Dir. inf.*, 2/2015, 227; G. Duni, *L'amministrazione digitale. Il diritto amministrativo nella evoluzione della telematica*, Milano, 2008; F. Faini, *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in *Dir. inf.*, 4/2019, 1099 ss.; A.G. Orofino, *La semplificazione digitale*, in *Dir. econ.*, 3/2019, 87 ss.; M.

In tale prospettiva, la transizione digitale è divenuta una priorità strategica, come dimostrato dagli investimenti realizzati sia sul piano delle infrastrutture sia sul fronte delle competenze digitali e dell'alfabetizzazione amministrativa.

In continuità con gli indirizzi europei, anche il Governo italiano ha promosso una serie di interventi normativi, finanziari e organizzativi volti a favorire l'adozione di nuove tecnologie, l'interoperabilità dei sistemi pubblici e il rafforzamento dell'identità digitale come strumento di accesso sicuro, uniforme e universalistico ai servizi pubblici.

2.1. Il d.lgs. 82/2005 (CAD)

Il Codice dell'Amministrazione Digitale (CAD)⁶⁰, introdotto con il d.lgs. 7 marzo 2005, n. 82 ed entrato in vigore il 1° gennaio 2006, rappresenta il pilastro normativo italiano in materia di digitalizzazione della pubblica amministrazione⁶¹.

Esso definisce un sistema organico di norme volte a garantire l'efficacia giuridica degli atti e dei documenti informatici, nonché a regolare strumenti quali la firma elettronica, la posta elettronica certificata e, in posizione sempre più centrale, l'identità digitale⁶². Attraverso tale disciplina nazionale si è assistito a una

Pietrangelo, *Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione: luci ed ombre*, in *ID*, 1-2/2005, 73 ss.; F. Merloni (a cura di), *Introduzione all'e-Government. Pubbliche amministrazioni e società dell'informazione*, Torino, 2005; D. Marongiu, *Il governo dell'informatica pubblica*, Napoli, 2007; F. Costantino, *Autonomia dell'amministrazione e innovazione digitale*, Napoli, 2012; Id., *L'uso della telematica nella pubblica amministrazione*, in A. Romano (a cura di), *L'azione amministrativa. Saggi sul procedimento amministrativo*, Torino, 2016, 246 ss.; G. Pesce, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018; F. Martinez, *La digitalizzazione della pubblica amministrazione*, in *MediaLaws*, 2/2018, 146 ss.

⁶⁰ Cfr. E. De Giovanni, *Il codice dell'Amministrazione digitale: genesi, evoluzione, principi costituzionali e linee generali*, in *Rassegna Avvocatura dello Stato*, 3/2018, 155; B. Carotti, *Il correttivo al Codice dell'amministrazione digitale: una meta-riforma*, in *Giorn. dir. amm.*, 2/2018, 131 ss.; Id., *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giorn. dir. amm.*, 1/2017, 7 ss.; E. Carloni (a cura di), *Codice dell'amministrazione digitale*, Rimini, 2005; Id., *La riforma del Codice dell'amministrazione digitale*, in *Giorn. dir. amm.*, 2011, 469 ss.

⁶¹ Dagli anni Novanta sino all'adozione del Codice dell'amministrazione digitale, diversi interventi normativi hanno progressivamente disciplinato l'amministrazione digitale: legge 23 ottobre 1992, n. 421; d.lgs. 12 febbraio 1993, n. 39; legge 15 marzo 1997, n. 59; d.P.R. 10 novembre 1997, n. 513; d.P.R. 20 ottobre 1998, n. 428; d.P.R. 28 dicembre 2000, n. 445; d.lgs. 23 gennaio 2002, n. 10 e d.P.R. 7 aprile 2003, n. 137.

⁶² L'ordinamento italiano aveva regolato nel 1997 il valore legale del documento informatico e delle firme elettroniche, in particolare la firma digitale (v. legge 59/1997 e D.p.r. 513/1997). Successivamente con la legge 191/1998, art. 2, aveva altresì normato in tema di carta di identità elettronica e di lavoro digitale (art. 4 l. 191/1998). Tali temi ritorneranno con maggiore incisività all'attenzione delle istituzioni, della politica, del sistema sociale ed economico dapprima con il

trasposizione dei principi classici dell'azione amministrativa – di economicità, imparzialità, pubblicità e trasparenza – nell'ambiente digitale, secondo una logica di equivalenza tra procedimento tradizionale e procedimento informatizzato⁶³.

Ma soprattutto, la promozione dell'impiego di suddetti strumenti via via più sofisticati e armonizzati con i principi del procedimento ha ormai trasformato lo sviluppo digitale in una caratteristica intrinseca del potere pubblico⁶⁴: la dimensione tecnologica diventa così elemento strutturale della legittimità dell'azione amministrativa e della garanzia dei diritti del cittadino.

In tale contesto, l'identità digitale assume una funzione essenziale, configurandosi quale strumento tecnico-giuridico per l'identificazione univoca e verificata dell'utente nei rapporti digitali con la pubblica amministrazione, intesa come declinazione della soggettività indispensabile per conferire l'accesso ai canali di comunicazione e di informazione degli apparati burocratici⁶⁵.

Essa è definita formalmente dall'art. 1, comma 1, lett. *u-quater* come «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'articolo 64». Tale disposizione stabilisce, in sostanza, un legame certificato e strutturato tra l'identità fisica del cittadino e il suo profilo digitale, funzionale all'accesso ai servizi pubblici *online* e all'imputazione personale di atti giuridicamente rilevanti compiuti in rete⁶⁶. Le modalità operative per il rilascio e la gestione dell'identità digitale sono disciplinate dall'art. 64 del CAD, che ha istituito il “Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese” (SPID)⁶⁷ e dai relativi decreti attuativi di competenza dell'AgID.

Regolamento eIDAS 910/2014 e successivamente sia con la legge 124/2015 (Carta della cittadinanza digitale), sia a seguito della crisi pandemica che ha riproposto per necessità i temi dell'identità digitale, del valore legale dei dati/documenti, delle transazioni elettroniche nel settore pubblico e privato.

⁶³ N. Bardino, *Rapporti con la pubblica amministrazione e identità e domicilio digitali*, in A. Ciriello, M. Maugeri (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 26.

⁶⁴ L. Torchia, *Lo Stato digitale*, cit., 17.

⁶⁵ N. Bardino, *Rapporti con la pubblica amministrazione e identità e domicilio digitali*, cit., 29.

⁶⁶ G. Corasaniti, *Identità digitale tra dati personali e relazioni funzionali*, in A. Ciriello, M. Maugeri (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 246.

⁶⁷ Il Codice dell'Amministrazione Digitale è stato modificato e integrato prima con il d.lgs. 179/2016 e poi con il d.lgs. 217/2017 per promuovere e rendere effettivi i diritti di cittadinanza digitale.

Tali modalità nella loro interazione e nel loro effetto abilitativo corrispondono a un nucleo centrale di diritti definito dall'art. 3 nella sua dimensione essenziale di "cittadinanza digitale"⁶⁸, funzionale all'uso generalizzato ed effettivo delle tecnologie informatiche⁶⁹. Questa dimensione si accompagna a obblighi per le amministrazioni, le quali devono garantire la piena accessibilità, l'interoperabilità e la sicurezza dei propri sistemi digitali. In tale prospettiva, l'identità digitale non rappresenta soltanto uno strumento operativo, ma si configura come presupposto necessario per l'esercizio dei "diritti digitali"⁷⁰ e come proiezione della soggettività giuridica nel cyberspazio.

Il Codice è stato oggetto, nel corso degli anni, di numerose modifiche e aggiornamenti⁷¹ finalizzati a recepire l'evoluzione tecnologica e normativa soprattutto in ambito sovranazionale. Tra gli interventi più significativi, si segnala il d.lgs. 26 agosto 2016, n. 179, che ha aggiornato il testo del CAD per adeguarlo al Regolamento (UE) n. 910/2014 (eIDAS) in materia di identificazione elettronica e servizi fiduciari (§ 2.2). Tale riforma ha introdotto un'ampia revisione del già menzionato art. 64 CAD, prevedendo l'accesso ai servizi digitali attraverso strumenti di identificazione certificata, in particolare il Sistema Pubblico di Identità Digitale (SPID) e la Carta d'Identità Elettronica (CIE).

La modifica più incisiva è riscontrabile al comma 2-*duodecies* dell'art. 64⁷², in quanto per la prima volta la verifica dell'identità digitale (o meglio dell'identificazione elettronica se si intende rispettare la terminologia del Regolamento UE) è equiparata all'accertamento dell'identità tramite controllo del

⁶⁸ Art. 3, co 1, CAD: «Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute».

⁶⁹ G. Corasaniti, *Identità digitale tra dati personali e relazioni funzionali*, cit., 246.

⁷⁰ Sul tema v. F. Ricciulli, *I diritti digitali: verso un'identità unica europea*, in *Diritto pubblico europeo - Rassegna online*, spec. 1/2024, 190 ss.; P. Costanzo, *Avete detto "diritti digitali?"*, in *Diritto, Mercato, Tecnologia*, 2/2016, 145 ss.; F. Oliveri, *Per una teoria generale dei diritti digitali*, in *Dem. dir. soc.*, 1/2025, 203 ss.; G. Ziccardi, *Diritti digitali*, Milano, 2022.

⁷¹ Il Codice è stato oggetto di modifiche e integrazioni nel corso degli anni (oltre venticinque), anche piuttosto recenti, alcune delle quali particolarmente incisive: è il caso del d.lgs. 4 aprile 2006, n. 159, del d.lgs. 30 dicembre 2010, n. 235 e del d.lgs. 26 agosto 2016, n. 179, seguito dal cosiddetto "decreto correttivo", il d.lgs. 13 dicembre 2017, n. 217.

⁷² A. Mazzeo, M. Nastri, *Identificazione in rete: identità digitale e identità personale*, in A. Ciriello, M. Maugeri (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 41.

documento di riconoscimento⁷³. Questo principio di equivalenza contraddistingue una svolta concettuale e normativa: per la prima volta l'identità digitale non è esclusivamente mezzo di accesso ai servizi⁷⁴, ma strumento di piena identificazione legale in grado di produrre effetti equivalenti alla presentazione fisica di un documento⁷⁵.

In precedenza, infatti, l'utilizzo dell'identità digitale era riconosciuto solo per finalità volta per volta determinate. Ne discende un'immediata riconducibilità giuridica dell'attività giuridica al soggetto identificato, con implicazioni rilevanti anche sotto il profilo penale: il furto di identità digitale assume oggi la configurazione di una vera e propria sostituzione di persona⁷⁶.

L'identità digitale, quindi, rappresenta sempre più l'estensione originaria della soggettività giuridica e centro di imputazione personale degli effetti giuridici derivanti da attività svolte in rete. La generalizzazione dell'uso obbligatorio di SPID e CIE per l'accesso ai servizi pubblici digitali conferma la progressiva assimilazione tra identità digitale e identità personale, non solo sul piano tecnico, ma anche su quello sostanziale.

L'esperienza normativa italiana trova però la sua piena coerenza solo se letta alla luce del contesto multilivello in cui è inserita. Il CAD, infatti, si confronta costantemente con le fonti del diritto dell'Unione europea; la disciplina nazionale è stata dunque chiamata ad armonizzarsi con il Regolamento (UE) n. 910/2014 e, oggi, con il nuovo Regolamento (UE) n. 1183/2024, noto come eIDAS 2 (§2.3), che prevede l'introduzione del Portafoglio europeo di identità digitale (EUDI *Wallet*) e nuovi *standard* di interoperabilità e sicurezza.

Il risultato è un sistema stratificato e in costante evoluzione, in cui coesistono le disposizioni del CAD, i decreti attuativi e le Linee guida AgID da un lato, e le fonti sovranazionali direttamente applicabili dall'altro.

⁷³ Ai sensi dell'art. 35 del d.p.r. 28 dicembre 2000, n. 445.

⁷⁴ N. Bardino, *Rapporti con la pubblica amministrazione e identità e domicilio digitali*, cit. 29.

⁷⁵ A. Mazzeo, M. Nastri, *Identificazione in rete*, cit., 41: «Il risultato di questo primo rinvio normativo consiste nell'equiparazione dell'utilizzo di "identità digitale con livello di garanzia almeno significativo" (*rectius* "regimi di garanzia dell'identificazione elettronica" secondo l'art. 8 del Regolamento eIDAS) alla identificazione mediante documento cartaceo di identità o di riconoscimento».

⁷⁶ S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. industr.*, 4-5/2017, 180 ss.

Questa architettura multilivello, se da un lato garantisce uniformità di regole e *standard* comuni – in particolare in materia di sicurezza, interoperabilità e riconoscimento reciproco – dall’altro richiede un continuo sforzo di coordinamento tra fonti e tra istituzioni competenti: AgID, Garante per la protezione dei dati personali, Commissione europea, *European Data Protection Board*.

In prospettiva, l’Italia sarà chiamata ad adeguare nuovamente il proprio impianto normativo alle nuove disposizioni del già citato Regolamento eIDAS 2, così da assicurare la piena integrazione del sistema italiano nello spazio europeo dell’identità digitale, rafforzando la cooperazione tra autorità, garantendo la tutela dei diritti fondamentali e promuovendo un accesso universale, sicuro e affidabile ai servizi pubblici digitali.

2.2. Il regolamento 910/2014 (eIDAS)

Il 23 luglio 2014, il Parlamento europeo e il Consiglio hanno approvato il Regolamento (UE) n. 910/2014, conosciuto come Regolamento eIDAS – *electronic IDentification, Authentication and trust Services* – che disciplina l’identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno⁷⁷. Tale strumento rappresenta oggi il pilastro normativo europeo in materia di gestione delle identità digitali⁷⁸: esso, infatti, se da un lato ha riformato la materia dei servizi

⁷⁷ A livello europeo, la tutela dell’identità digitale si dipana essenzialmente su due assi normativi principali: da un lato il Regolamento eIDAS, dall’altro il Regolamento (UE) n. 679/2016, ossia il *General Data Protection Regulation* (GDPR), cardine della protezione dei dati personali in Europa.

⁷⁸ Per un’analisi della disciplina si rinvia a I. Macrì, *L’identità digitale, nuovo documento di riconoscimento*, in *Azienditalia*, 3/2021, 475 ss.; A. Ortalda, S. Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Riv. it. inf. e dir.*, 1/2022, 145 ss.; G.D. Finocchiaro, *Una prima lettura del reg. UE n.910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, in *Nuove leggi civili commentate*, 3/2015, 419 ss.; M. Farina, *Le tecnologie informatiche e l’effetto moltiplicatore sull’identità personale: riflessioni (meta)giuridiche tra crisi di identità e necessità di tutela dei diritti fondamentali dell’individuo*, in *Rivista elettronica di Diritto, Economia e Management*, 1/2020, 41 ss.; D. Baldini, *The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet*, in *Italian Journal of Public Law*, 1/2024, 297 ss.; J.F.Rodríguez Ayuso, *Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014*, in *federalismi.it*, 24/2017, 2 ss.; N. Tsakalakis, S. Stalla-Bourdillon, K. O’Hara, *Data Protection by Design for Cross-Border Electronic Identification: Does the EIDAS Interoperability Framework Need To Be Modernised?*, in E. Kosta et al. (eds.), *Privacy and Identity Management. Fairness, Accountability and Trasparency in the Age of Big Data*, Springer, 2019.

fiduciari (firma elettronica e altri), dall'altro ha istituito un quadro europeo di interoperabilità dei servizi di identità elettronica⁷⁹.

Dunque, il principale intento della disciplina⁸⁰ è quello di stabilire un 'ecosistema normativo' uniforme per garantire la suddetta interoperabilità transfrontaliera dei sistemi nazionali di identificazione elettronica⁸¹: ciò, attraverso il rafforzamento della fiducia nelle transazioni elettroniche nel mercato interno⁸². Tale interesse coincide sia con una maggiore attenzione a livello globale nei confronti del tema dell'identificazione elettronica transfrontaliera, sia con la strategia di *governance* digitale adottata dall'Unione europea⁸³. Segnatamente, il Regolamento stabilisce un quadro normativo finalizzato ad agevolare la creazione e il governo di strumenti e processi comuni tra gli Stati membri dell'Unione europea per il riconoscimento delle identità elettroniche per l'accesso ai servizi digitali⁸⁴, introducendo modalità di notifica e riconoscimento reciproco dei mezzi e dei regimi di identificazione elettronica⁸⁵.

⁷⁹ E. Prosperetti, *Identità digitale ed elettronica nazionale e transfrontaliera nell'accesso ai servizi pubblici e privati e prospettive di utilizzo nei contratti online e nei servizi bancari*, in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, 434.

⁸⁰ L'Unione europea aveva già dal 2008 avviato un progetto sperimentale, denominato STORK (*Secure Identity Across Borders Linked*) studiando la possibilità di rendere identità elettroniche nazionali interoperabili per l'uso transfrontaliero di servizi in ambito pubblico, privato e sanitario e i risultati positivi ottenuti facevano propendere per una declinazione normativa europea del sistema. Sul punto E. Prosperetti, *Identità digitale ed elettronica nazionale e transfrontaliera nell'accesso ai servizi pubblici e privati*, cit., 434.

⁸¹ M. Farina, *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale*, cit., 50-51.

⁸² Sul punto Considerando 2 del Regolamento eIDAS: «Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea» e Considerando 9: «In molti casi i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri. Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica riconosciuti reciprocamente permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche».

⁸³ A. Ortalda, S. Leucci, *Identità digitale e protezione dei dati personali*, cit., 145.

⁸⁴ *Ibidem*, 146.

⁸⁵ Per "mezzi di identificazione elettronica" il Regolamento eIDAS intende «un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio *online*» (art. 3, co. 2); invece, con "regimi di identificazione elettronica" il Regolamento intende «un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche» (art. 3 co. 3).

È importante sottolineare che il Regolamento eIDAS non entra nel merito delle finalità e delle specifiche modalità operative dei singoli regimi nazionali di identificazione, che restano prerogativa esclusiva dei singoli Stati membri.

Esso, piuttosto, ha previsto i requisiti minimi necessari affinché i sistemi nazionali possano ‘dialogare’ tra loro, garantendo un’interoperabilità con i regimi istituiti da altri Stati membri per un’efficace fruizione dei servizi digitali a livello europeo⁸⁶. È corretto, pertanto, indicarla come disciplina di coordinamento: più nello specifico, il Regolamento ha disposto le condizioni affinché i mezzi adottati dai diversi Stati membri possano venire reciprocamente riconosciuti⁸⁷, disponendo le modalità attraverso cui gli stessi notificano alla Commissione europea l’esistenza e le peculiarità dei loro regimi di identificazione elettronica⁸⁸.

Tuttavia, l’applicazione del Regolamento eIDAS è circoscritta ai mezzi di identificazione elettronica che consentano l’accesso a servizi erogati da “organismi del settore pubblico”⁸⁹; di conseguenza, rimangono esclusi dal suo ambito applicativo i mezzi di identificazione impiegati esclusivamente nell’ambito di servizi offerti da operatori privati.

Inoltre, la disciplina non ha previsto alcun obbligo per gli Stati membri di notificare un proprio sistema di identificazione elettronica: tale scelta è stata lasciata alla discrezione delle autorità nazionali, purché siano rispettati i requisiti di sicurezza e affidabilità stabiliti dal Regolamento. Come è noto, l’Italia ha notificato sia il

⁸⁶ Considerando 12 Regolamento eIDAS: «Un obiettivo del presente regolamento è l’eliminazione delle barriere esistenti all’impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l’autenticazione nei servizi pubblici. Il presente regolamento non intende intervenire riguardo ai sistemi di gestione dell’identità elettronica e relative infrastrutture istituiti negli Stati membri. Lo scopo del presente regolamento è garantire che per accedere ai servizi *online* transfrontalieri offerti dagli Stati membri si possa disporre di un’identificazione e un’autenticazione elettronica sicura».

⁸⁷ Art. 6 Regolamento eIDAS. L’articolo detta un preciso perimetro di obblighi applicabile a tutti gli Stati in tutti i casi in cui le normative o prassi nazionali richiedano l’impiego di mezzi di identificazione elettronica per accedere ai servizi *online* erogati da organismi del settore pubblico.

⁸⁸ Art. 9 Regolamento eIDAS. Dopo un anno di perfezionamento della notifica, sarebbe divenuto operativo il sistema (e l’obbligo) di riconoscimento transfrontaliero, dell’identità nazionale notificata per l’accesso ai servizi *online* delle pubbliche amministrazioni degli Stati membri.

⁸⁹ Art. 3.7, Regolamento eIDAS secondo cui per «organismo del settore pubblico» si intende: «un’autorità statale, regionale o locale, un organismo di diritto pubblico o un’associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un’autorità, un organismo o un’associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato». La definizione è diversa e non coincidente con quella di ente pubblico generalmente accolta nell’ordinamento italiano (sul punto v. *ex multis* R. Ursi, *Diritto amministrativo generale*, Milano, 2024, 93-104), ma è simile al disposto dell’art. 2, co. 2, del CAD che individua i soggetti obbligati a rispettarne le disposizioni.

sistema SPID sia la CIE come mezzi di identificazione elettronica nazionale ai sensi di eIDAS: ciò significa che un cittadino italiano può usare SPID non soltanto per servizi *online* delle amministrazioni italiane, ma altresì per accedere ai servizi *online* dei paesi dell'Unione europea che hanno aderito al nodo⁹⁰ eIDAS italiano⁹¹. Dal punto di vista sostanziale, dunque, è stato previsto un sistema di gestione dell'identità di tipo “federato”: il Regolamento delinea un ecosistema in cui la gestione operativa delle identità digitali resta prerogativa nazionale, mentre l'Unione europea si è limitata a garantire il ‘riconoscimento reciproco’ attraverso la predisposizione di *standard* minimi.

L'impostazione su base volontaria prevista dalla normativa ha comportato una partecipazione disomogenea: alcuni Stati (tra cui l'Italia) si sono dotati di sistemi notificati, mentre altri sono rimasti indietro e di conseguenza la visione di uno spazio europeo delle identità digitali pienamente funzionante è rimasta in parte incompiuta⁹².

Negli anni successivi all'entrata in vigore del Regolamento eIDAS, il contesto europeo e internazionale ha subito significativi mutamenti, amplificati dall'emergenza sanitaria. La crisi pandemica ha contribuito a modificare radicalmente le aspettative degli utenti e dei fornitori di servizi digitali, evidenziando le limitazioni derivanti dai bassi tassi di adozione degli strumenti transfrontalieri di identificazione. Tale scenario ha così indotto la Commissione europea, già nel 2020, ad avviare una revisione profonda del quadro normativo originario, con l'intento di promuovere una maggiore adozione di tali strumenti e di adeguare la normativa al mutato scenario⁹³.

A seguito di questo processo, nel 2021 la Commissione ha presentato una serie di proposte di modifica al Regolamento eIDAS, tra le quali spicca un emendamento

⁹⁰ Il Regolamento istituisce all'art. 5 un sistema di “nodi” nazionali per il riconoscimento reciproco che devono essere in grado di connettersi ai nodi di altri Stati membri” e non avere requisiti tecnici o costi sproporzionati per poter interoperare. Ciascuno Stato membro, sia che abbia notificato regimi di identità elettronica, sia che non intenda notificarne alcuno, deve istituire un nodo, cioè un *server*, che consenta a chi richiede di accedere a un servizio *online* nazionale, di poter essere riconosciuto alla stregua di quanto avviene per i cittadini che accedono a tale servizio con identità elettroniche nazionali (Prosperetti, 44-445).

⁹¹ Ad oggi sono undici gli Stati dell'Unione europea che hanno completato la loro adesione al Nodo italiano eIDAS che garantisce l'interoperabilità transfrontaliera delle identità digitali: Lussemburgo, Norvegia, Lettonia, Slovenia, Olanda, Malta, Spagna, Estonia, Svezia, Grecia e Belgio.

⁹² Nel 2021 soltanto 14 Paesi UE avevano almeno un eID notificato.

⁹³ European Commission, *Shaping Europe's Digital Future*, febbraio 2020.

particolarmente rilevante a fini della disamina. La modifica concerne l'istituzione del cosiddetto "Portafoglio europeo di identità digitale" (*European Digital Identity Wallet*) (§ 2.4). Tale elemento di novità rifletterebbe la volontà della Commissione europea di garantire agli utenti un maggior controllo sui propri dati personali, con l'intenzione di abbandonare progressivamente il modello centralizzato-federato di gestione delle identità elettroniche.

2.3. Il regolamento 1183/2024 (eIDAS 2)

Il Regolamento (UE) 2024/1183⁹⁴ – comunemente denominato eIDAS 2 – segna un punto di svolta nell'evoluzione dell'infrastruttura giuridica europea dell'identità digitale⁹⁵. Dalla logica di coordinamento "leggero" che caratterizzava il quadro del 2014, si è passati a un disegno di vera e propria integrazione normativa e tecnologica, imperniato sul Portafoglio europeo di identità digitale⁹⁶ (*European Digital Identity Wallet*) quale mezzo di identificazione elettronica a spendibilità generalizzata e di deposito di attestati qualificati di attributi.

La revisione segue infatti una prima edizione caratterizzata da significativi progressi per la trasformazione digitale, ma accompagnati allo stesso tempo da risultati non soddisfacenti dalla prospettiva delle transazioni transfrontaliere⁹⁷. Muovendo da una valutazione di impatto che ha messo in luce l'insufficienza di un sistema volontario di notifica⁹⁸ – cui hanno aderito in misura disomogenea appena

⁹⁴ Regolamento (UE) 2024/183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

⁹⁵ Considerando 1 Regolamento eIDAS 2: «Nella comunicazione della Commissione del 19 febbraio 2020 intitolata «Plasmare il futuro digitale dell'Europa» si annunciava la revisione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio (4) al fine di migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere identità digitali affidabili per tutti gli europei».

⁹⁶ L'art. 1 del Regolamento eIDAS 2 definisce il "Portafoglio europeo di identità digitale" quale «mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati». Vedi anche l'art. 5-bis Regolamento eIDAS 2 (Portafogli europei di identità digitale).

⁹⁷ G. Manca, *Introduzione*, in *Il regolamento eIDAS n. 2024/1183, n. spec. Rivista elettronica di Diritto, Economia, Management*, 4/2024, 9-10.

⁹⁸ La riforma è stata proposta inizialmente dalla Commissione europea il 3 giugno 2021 e nasce da un'attenta analisi delle criticità riscontrate nella prima fase di applicazione del Regolamento eIDAS, tra le quali spiccano in particolare la disomogeneità dei sistemi nazionali di identificazione elettronica, alla limitata interoperabilità degli stessi e alla scarsa diffusione dell'utilizzo transfrontaliero delle identità digitali.

quindici Stati membri⁹⁹ – il Legislatore unionale ha normato la predisposizione o il riconoscimento di almeno un *wallet* (portafoglio di identità digitale)¹⁰⁰ conforme, gratuito per l'utente e tecnicamente in grado di garantire un livello di garanzia "elevato" ai sensi dell'art. 8 eIDAS.

Ne deriva un mutamento paradigmatico: l'identità digitale non si configurerebbe più come mera opzione tecnico-amministrativa, bensì come infrastruttura abilitante di cittadinanza europea, il cui controllo rimane in capo alle autorità pubbliche ma la cui gestione operativa può essere affidata a soggetti privati purché certificati, introducendosi così un nuovo mercato dei "*wallet providers*" sottoposto a vigilanza multilivello.

Al fine di raccogliere tutti gli attributi associati all'identità di un cittadino, il Regolamento propone la realizzazione dei suddetti portafogli, intesi come contenitori di attributi che consentono al cittadino europeo di conservare dati di identificazione, credenziali e attributi collegati sua identità, ma soprattutto sotto il suo pieno controllo¹⁰¹, ciò allo scopo di esibirli alle parti richiedenti come strumento di autenticazione.

⁹⁹ Gli Stati membri che, alla data del 24 ottobre 2023 (ultimo aggiornamento ufficiale del portale *eID User Community* della Commissione), avevano completato la procedura di notifica di almeno uno schema di identificazione elettronica ai sensi dell'art. 9 del Regolamento eIDAS sono: Germania, Estonia, Spagna, Croazia, Lussemburgo, Belgio, Slovacchia, Repubblica Ceca, Lettonia, Portogallo, Italia, Paesi Bassi, Lituania, Svezia, Francia.

¹⁰⁰ Considerando 7 Regolamento eIDAS 2: «Un approccio maggiormente armonizzato all'identificazione elettronica dovrebbe ridurre i rischi e i costi dell'attuale frammentazione dovuta all'uso di soluzioni nazionali divergenti oppure, in alcuni Stati membri, all'assenza di tali soluzioni di identificazione elettronica. Un tale approccio dovrebbe rafforzare il mercato interno consentendo ai cittadini e ai residenti dell'Unione, quali definiti dalle legislazioni nazionali, e alle imprese di identificarsi e di fornire un'autenticazione della propria identità *online* e *offline* in modo sicuro, affidabile, di facile utilizzo, pratico, accessibile e armonizzato in tutta l'Unione. Il portafoglio europeo di identità digitale dovrebbe fornire alle persone fisiche e giuridiche di tutta l'Unione un mezzo di identificazione elettronica armonizzato che consenta l'autenticazione e la condivisione dei dati collegati alla loro identità. Tutti dovrebbero poter accedere a servizi pubblici e privati in modo sicuro, sulla base di un ecosistema migliorato per i servizi fiduciari e su prove dell'identità e attestati elettronici di attributi verificati, come qualifiche accademiche, compresi diplomi universitari o altri titoli di studio o qualifiche professionali. Il quadro europeo relativo a un'identità digitale è inteso consentire il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi e legalmente riconosciuti in tutta l'Unione. I fornitori di attestati elettronici di attributi dovrebbero beneficiare di un insieme di norme chiaro e uniforme, mentre le amministrazioni pubbliche dovrebbero potersi avvalere di documenti elettronici in un formato prestabilito».

¹⁰¹ Art. 5-*bis*, co. 4, Regolamento eIDAS 2: «I portafogli europei di identità digitale consentono all'utente, in modo intuitivo, trasparente e tracciabile da quest'ultimo, di:

- 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

Lo schema che propone il Regolamento è differente dagli schemi di identità digitale federata in cui i dati di identità sono forniti dall'*identity provider*¹⁰² a cui il *service provider*¹⁰³ si collega. Nel caso di eIDAS 2 i dati di identità vengono caricati direttamente nel *wallet* al momento della sua attivazione e vengono forniti direttamente dal cittadino al *service provider*, senza che quest'ultimo debba contatto l'*identity provider*.

Dunque, il Regolamento accoglie le suggestioni della *Self-Sovereign Identity*¹⁰⁴, attribuendo all'utente un potere di autodeterminazione rafforzato sui dati, sancendo il divieto per i fornitori di raccogliere metadati sull'uso del *wallet* e di richiedere attributi eccedenti il minimo necessario. Al tempo stesso, investe le pubbliche amministrazioni dell'obbligo di rendere disponibili, tramite interfacce standardizzate, servizi di verifica degli attributi qualificati, con implicazioni organizzative notevoli in termini di interoperabilità semantica e di sicurezza delle basi di dati.

Sotto il profilo tecnico-giuridico, la disciplina degli “attestati elettronici di attributi”¹⁰⁵ – qualificati o meno – rappresenta l'innovazione forse più significativa:

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 [...];
- 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».

¹⁰² Gli *identity provider* (IdP) sono i soggetti accreditati incaricati del rilascio e della gestione delle credenziali digitali degli utenti. Essi assicurano che l'identità dichiarata corrisponda a una persona fisica o giuridica realmente esistente, in conformità ai requisiti di sicurezza e affidabilità stabiliti dalla normativa.

¹⁰³ I *service provider* (SP) sono gli enti, pubblici o privati, che erogano servizi digitali accessibili mediante l'identità digitale dell'utente. Essi si avvalgono delle credenziali rilasciate da un IdP per autenticare l'utente e consentirgli di usufruire delle prestazioni *online*.

¹⁰⁴ Sul paradigma della *Self-Sovereign Identity* (SSI), fondato su modelli decentralizzati di gestione delle credenziali digitali che attribuiscono all'utente il controllo diretto dei propri dati, si rinvia per un'analisi ampia al capitolo III.

¹⁰⁵ Considerando 7 Regolamento eIDAS 2: «[...] Tutti dovrebbero poter accedere a servizi pubblici e privati in modo sicuro, sulla base di un ecosistema migliorato per i servizi fiduciari e su prove dell'identità e attestati elettronici di attributi verificati, come qualifiche accademiche, compresi

essa codifica, con effetti di pieno riconoscimento giuridico, le *verifiable credentials*¹⁰⁶, prevedendo un modello triadico (emittente, titolare, verificatore) che, se correttamente implementato, potrebbe ridurre drasticamente la dipendenza da intermediari di fiducia e abilitare scenari di interoperabilità settoriale (es. mobilità, istruzione, sanità).

Tuttavia, la dottrina ha già rilevato la mancanza di una valutazione d'impatto unitaria sulle tecniche di anonimizzazione e di offuscamento dei metadati¹⁰⁷, evidenziando il rischio di profilazioni indirette da parte dei *service provider*, specie nei settori ad alto valore economico.

Non meno complesso risulta il tema della *governance*: l'istituzione di un quadro di certificazione comune, la definizione di profili di responsabilità per danni derivanti da errori nell'emissione o nella verifica degli attestati e la necessità di prevenire concentrazioni oligopolistiche fra *wallet providers* richiederanno un rafforzamento significativo dei poteri di supervisione sia a livello della Commissione sia delle autorità nazionali competenti.

Nel contesto italiano, ciò implicherebbe necessariamente il potenziamento dell'AgID, che dovrà raccordare il proprio perimetro ispettivo con quello del Garante *privacy* e dell'AGCM, nonché armonizzare l'ecosistema SPID-CIE ai requisiti EUDI *Wallet*.

Attualmente, il Regolamento è pienamente in vigore, ma la sua efficacia operativa dipende dall'adozione del *corpus* di atti di esecuzione e di *standard* di riferimento che devono dettagliare il profilo tecnico-organizzativo dell'*European Digital Identity Wallet*.

diplomi universitari o altri titoli di studio o qualifiche professionali. Il quadro europeo relativo a un'identità digitale è inteso consentire il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi e legalmente riconosciuti in tutta l'Unione. I fornitori di attestati elettronici di attributi dovrebbero beneficiare di un insieme di norme chiaro e uniforme, mentre le amministrazioni pubbliche dovrebbero potersi avvalere di documenti elettronici in un formato prestabilito».

Agli "attestati elettronici di attributi" è dedicata la sezione 9 del Regolamento eIDAS 2.

¹⁰⁶ Le *verifiable credentials* sono attestazioni digitali che collegano, mediante firma crittografica, un attributo personale all'identità di un titolare.

¹⁰⁷ Sul tema dei metadati si rimanda a G. Olivi, "Big Data", *metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Dir. ind.*, 2/2020, 181 ss.; G. Thuermer, L. Koesten, E. Simperl, *Talking Metadata. Understanding Privacy Implications of Volunteer Contributions in Citizen Science Projects*, in *Etica & politica - Ethics & politics*, 2/2023, 197 ss.

Sul piano delle scadenze giuridiche, l'art. 5-*bis* del Regolamento stabilisce che ogni Stato membro dovrà rendere disponibile almeno un *wallet* certificato entro 24 mesi dall'adozione dei principali atti di esecuzione; ove questi fossero approvati entro il quarto trimestre 2025, la distribuzione generalizzata ai cittadini dovrà avvenire non oltre la fine del 2027.

Diverse amministrazioni hanno già avviato iniziative nazionali pilota: Germania (*BundesWallet* integrato in BundID), Francia (*France Identité +*), Italia (fase sperimentale *IT Wallet* su IO), Spagna (*DNIe Wallet*) e Paesi Bassi (*NL Wallet*). Tali progetti serviranno da banco di prova per la futura certificazione conformemente allo schema di sicurezza che ENISA sta predisponendo ai sensi del *Cybersecurity Act*¹⁰⁸.

In ultima analisi, l'effettiva riuscita di eIDAS 2 dipenderà dalla capacità degli Stati membri di garantire un'implementazione rapida, ma soprattutto inclusiva: soltanto in questo modo il portafoglio digitale europeo potrà divenire un'infrastruttura di fiducia, capace di coniugare innovazione, sicurezza e accessibilità per i cittadini.

¹⁰⁸ Il Regolamento (UE) 2019/881, noto come *Cybersecurity Act*, ha significativamente rafforzato il mandato dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), attribuendole un ruolo permanente di supporto agli Stati membri e alle istituzioni europee. Inoltre, ha istituito un quadro europeo di certificazione della cybersicurezza per prodotti, servizi e processi ICT, con l'obiettivo di garantire un livello uniforme di sicurezza e fiducia nel mercato digitale europeo.

3. Il sistema pubblico di identità digitale italiano (SPID)

L'Italia è riconosciuta tra i 'pionieri' dell'identità digitale pubblica¹⁰⁹, avendo normato il sistema SPID, tra le prime e più avanzate identità digitali rilasciate, e provveduto alla notifica alla Commissione UE ai sensi del Regolamento eIDAS come secondo Paese¹¹⁰.

Se da un lato rappresenta la risposta del Legislatore alla duplice esigenza di assicurare l'effettività della "Carta della cittadinanza digitale" introdotta con la legge 124/2015¹¹¹, dall'altro, la coerenza dell'ordinamento interno con il paradigma di trasformazione digitale delineato nella Strategia per la crescita digitale 2014-2020¹¹² ma soprattutto dal Regolamento eIDAS.

Il Sistema Pubblico di Identità Digitale (SPID) è stato introdotto a livello primario dal già citato articolo 64 del Codice dell'Amministrazione Digitale e ha ricevuto una prima disciplina organica attraverso il Decreto del Presidente del Consiglio dei ministri del 24 ottobre 2014¹¹³, che ha stabilito la sua architettura tecnica e le prime scadenze per la sua adozione.

¹⁰⁹ E. Prosperetti, *Identità digitale ed elettronica nazionale e transfrontaliera nell'accesso ai servizi pubblici e privati*, cit., 443.

¹¹⁰ Il primo Stato membro dell'Unione europea ad aver formalmente notificato un sistema di identificazione elettronica ai sensi del Regolamento eIDAS è stato la Germania, con la carta d'identità elettronica nazionale, notificata nel settembre 2017. L'Italia, pur avendo avviato il processo già nel 2017 con SPID, è stato il secondo Paese ad avviare la procedura europea, ma il primo a farlo insieme a operatori privati. La notifica formale è avvenuta a fine luglio 2018.

¹¹¹ La Legge 7 agosto 2015, n. 124 ("Riforma Madia") ha conferito al Governo un'ampia delega per la riorganizzazione della Pubblica Amministrazione, per un approfondimento sull'argomento si rinvia a E. D'Alterio, B.G. Mattarella (a cura di) *La riforma della pubblica amministrazione. Commento alla legge 124/2015 (Madia) e ai decreti attuativi*, Milano, 2017.

L'art. 1, co. 1, lett. o), ha previsto la "Carta della cittadinanza digitale", consentendo poi l'adozione dei decreti già esaminati del 2016 e 2017 che hanno riformato il CAD, potenziato l'AgID e consacrato SPID e CIE quali strumenti primari di identificazione elettronica.

¹¹² Elaborata da Presidenza del Consiglio dei ministri e AgID (marzo 2015) come attuazione nazionale dell'Agenda digitale europea, la Strategia per la Crescita Digitale 2014-2020 ha fissato gli obiettivi di infrastrutturazione a banda ultra-larga, diffusione dei servizi di *e-government* (SPID, pagoPA, Anpr), promozione delle competenze digitali e *open data*. Il documento – aggiornato con i successivi Piani triennali per l'informatica nella P.A. – ha costituito il quadro di programmazione strategica e finanziaria per i progetti digitali cofinanziati da fondi strutturali UE e Fondo nazionale di sviluppo e coesione.

¹¹³ D.P.C.M. 24 ottobre 2014: «Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)», in G.U. 9 dicembre 2014, n. 285, costituisce l'atto regolamentare fondativo di SPID. Stabilisce l'architettura federata del sistema, i requisiti patrimoniali e di sicurezza per l'accreditamento degli *identity provider*, le funzioni di vigilanza dell'AgID, i tre livelli di garanzia dell'autenticazione e le scadenze di adozione per P.A. e imprese, prevedendo la revoca dell'accreditamento in caso di inadempienza.

Ulteriori perfezionamenti sono stati successivamente apportati dai decreti legislativi n. 179/2016¹¹⁴ e n. 217/2017¹¹⁵ – emanati in attuazione dell’articolo 1 della legge 7 agosto 2015, n. 124 (c.d. Legge Madia) – i quali hanno definitivamente affermato il concetto di ‘identità digitale’ come prerequisito per la fruizione telematica di procedimenti e servizi amministrativi.

Attraverso tali modifiche normative, il Legislatore italiano ha perseguito l’obiettivo di uniformare il quadro nazionale al Regolamento eIDAS, favorendo un reciproco riconoscimento delle identità elettroniche a livello europeo e modificando le definizioni e le norme precedentemente incompatibili con il già menzionato regolamento comunitario.

Il modello selezionato, definito come un sistema aperto e federato, riflette la volontà del Legislatore di armonizzare la protezione dell’interesse collettivo, concepita come garanzia di affidabilità, sicurezza e accessibilità universale, con la capacità innovativa degli organismi privati. Tali entità sono incaricate della gestione operativa del rilascio e della gestione delle credenziali, nel rispetto di requisiti patrimoniali, organizzativi e di sicurezza certificati durante la fase di accreditamento (§ 3.1).

SPID si distingue dalle esperienze centralizzate basate su un’unica autorità di emissione, come il *BankID* norvegese¹¹⁶ o il modello a carta *chip* vigente in Germania¹¹⁷, e si inserisce fra le sperimentazioni più avanzate a livello europeo.

¹¹⁴ D.lgs. 26 agosto 2016, n. 179: «Modifiche e integrazioni al Codice dell’Amministrazione Digitale». Il decreto ha adeguato il CAD al Reg. (UE) 910/2014 (eIDAS), riconoscendo SPID e CIE come strumenti di identificazione elettronica, ha potenziato i poteri regolatori e sanzionatori dell’AgID (artt. 14-17) e ha introdotto la nozione di “cittadinanza digitale” quale diritto all’uso delle tecnologie per l’accesso ai servizi pubblici.

¹¹⁵ D.lgs. 13 dicembre 2017, n. 217: «Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179». Il decreto ha completato la riforma del Codice dell’Amministrazione Digitale avviata col D.lgs. 179/2016, precisando la disciplina del domicilio digitale, istituendo l’Indice nazionale degli indirizzi PEC (INAD), rafforzando le sanzioni irrogabili da AgID (art. 17-*bis*) e allineando le definizioni di firma elettronica qualificata e sigillo elettronico ai requisiti del Reg. (UE) 910/2014.

¹¹⁶ Il sistema *BankID* è stato sviluppato nel contesto bancario norvegese e progressivamente divenuto l’identità digitale di uso quotidiano per la quasi totalità della popolazione (oltre 4 milioni di utenti su circa 5,4 milioni di abitanti). Modelli analoghi sono stati sperimentati anche in Danimarca (*NemID*) e in Finlandia (*TUPAS*), confermando la diffusione nell’area nordica di schemi di identità digitale di matrice finanziaria, caratterizzati dalla cooperazione fra istituti bancari e autorità pubbliche.

¹¹⁷ La carta d’identità tedesca è dotata di *chip contactless* e funzione di identificazione *online* introdotta dal 2010. L’autenticazione avviene tramite lettore/NFC e *software* pubblico *AusweisApp*. Lo schema eID tedesco è stato notificato ai sensi di eIDAS con livello di garanzia “high”; accanto

Fin dalla fase di avvio, il sistema è stato concepito come leva di riforma amministrativa: la circolare AgID n. 3/2018 ha sancito l'obbligo per le amministrazioni centrali di migrare i propri servizi verso l'autenticazione mediante SPID, imponendo la progressiva dismissione delle credenziali rilasciate in autonomia; contemporaneamente, il Legislatore ha ampliato il perimetro funzionale dell'identità digitale, attribuendole il valore di piena equipollenza giuridica al documento di riconoscimento ai fini dell'accesso in rete, ma escludendone l'impiego in contesti fisici.

In ambito applicativo, i dati di monitoraggio divulgati da AgID evidenziano che, a marzo 2025, oltre trentaquattro milioni di cittadini – rappresentativi del 65% della popolazione residente maggiorenne – possiedono almeno un'identità SPID attiva, mentre i *service provider* integrati superano le trentaduemila unità, con una quota superiore al venti percento appartenente al settore privato.

L'ampia diffusione di questo meccanismo ne dimostra l'efficacia, in quanto unisce la gratuità per l'utente, procedure di riconoscimento semplificate e un modello di *governance* che stimola la concorrenza tra *identity provider*. Questi ultimi possono differenziare le proprie offerte accessorie, a condizione che rispettino l'interoperabilità dei livelli di garanzia.

Sul fronte della *policy*, SPID ha svolto un ruolo di catalizzatore per i percorsi di inclusione digitale: la convenzione del 2021 tra AgID, Poste Italiane e ANCI ha consentito l'attivazione di sportelli di registrazione assistita nei Comuni con popolazione inferiore a cinquemila abitanti, nel tentativo di ridurre il divario territoriale. Parallelamente, le campagne di formazione finanziate dal PNRR hanno promosso la competenza digitale di base, associando l'adozione dell'identità digitale all'accrescimento del capitale umano.

3.1. *Gli operatori e i livelli di sicurezza*

L'identità SPID si ottiene attraverso la richiesta a uno degli *identity provider* (gestori di identità digitale) accreditati dall'Agenzia per l'Italia digitale (AgID)¹¹⁸.

¹¹⁸ Ai sensi dell'art. 64 CAD e del D.P.C.M. 24 ottobre 2014, l'accreditamento degli *identity provider* è affidato ad AgID, che ne definisce i requisiti patrimoniali, organizzativi e di sicurezza.

Il sistema è concepito come un modello aperto e federato¹¹⁹ che coinvolge soggetti pubblici e privati: previa autorizzazione, essi curano le procedure di registrazione, il rilascio delle credenziali e la gestione dei meccanismi di autenticazione¹²⁰.

All'interno dell'ecosistema SPID è possibile distinguere tre tipologie di operatori. L'*identity provider* (gestore di identità digitale) è il soggetto privato che, una volta accreditato, rilascia le credenziali di accesso al sistema (identità digitali) e gestisce i processi di autenticazione degli utenti.

Il *service provider* (fornitore di servizi) è rappresentato da enti pubblici o privati che mettono a disposizione servizi digitali accessibili tramite SPID.

Infine, l'*attribute provider* (gestore di attributi qualificati) svolge la funzione di certificare attributi specifici dell'utente (quali *status*, ruoli, titoli o cariche), al fine di consentire un accesso differenziato ai servizi digitali.

L'*account* SPID è costituito da credenziali con caratteristiche differenti, corrispondenti al livello di sicurezza richiesto per la fruizione dei servizi.

Attualmente sono previsti tre livelli di sicurezza, ognuno dei quali corrisponde a un diverso livello di SPID. Il primo livello permette di accedere ai servizi *online* semplicemente attraverso la combinazione di un nome utente e una *password* scelti dall'utente. A tale livello è associato un rischio moderato, sufficiente per servizi nei quali un uso indebito dell'identità digitale avrebbe conseguenze limitate per le attività dei cittadini, delle imprese o dell'amministrazione.

Il secondo livello prevede, oltre a nome utente e *password*, la generazione di un codice temporaneo (*One Time Password* - OTP) generato da un dispositivo fisico o virtuale. Si tratta di un'autenticazione a due fattori non necessariamente basata su certificati digitali, idonea per servizi il cui abuso può comportare danni significativi. Il terzo livello, infine, richiede oltre alle credenziali di base, un supporto crittografico (*smart card* o dispositivo di firma digitale remota) che custodisca chiavi private conformi ai requisiti dell'Allegato II del Regolamento eIDAS.

¹¹⁹ Il modello federato di SPID si inserisce nel solco della dottrina che distingue le architetture centralizzate dai sistemi federati, caratterizzati da pluralità di gestori sotto la supervisione pubblica. Sul punto si rimanda a H. Rittenberg, *Who Are You: A Primer on Digital Identity*, in *Journal of Technology and Intellectual Property*, 3 maggio 2022.

¹²⁰ G. Levante, *Il sistema pubblico di identità digitale*, in <https://www.notartel.it/notartel/pdf-studi/sistema-pubblico-id-digitale-1-2020-DI.pdf>, 1/2020, 2 ss.

Questo livello, classificato a rischio elevato, è destinato ai servizi per i quali un uso improprio dell'identità digitale potrebbe causare conseguenze gravi e irreversibili. In tal modo, SPID si configura come un sistema capace di modulare le proprie garanzie di sicurezza in relazione alla delicatezza del servizio richiesto, allineandosi alla logica di proporzionalità e ai criteri di classificazione dei livelli di garanzia previsti dalla normativa europea in materia di identificazione elettronica.

3.2. Il ruolo dell'Agenzia per l'Italia Digitale

L'Agenzia per l'Italia Digitale (AgID) riveste un ruolo centrale nella regolazione e nello sviluppo dell'identità digitale nazionale. Essa definisce gli *standard* e i requisiti di sicurezza necessari a garantire la corretta operatività del sistema e la sua evoluzione, esercitando funzioni di indirizzo tecnico, regolazione e vigilanza¹²¹.

Il CAD, in particolare agli articoli 14 e 17, le attribuisce compiti di coordinamento, accreditamento e controllo, nonché poteri sanzionatori nei confronti degli operatori del Sistema Pubblico di Identità Digitale, così da assicurare uniformità di regole e conformità agli *standard* europei di sicurezza e interoperabilità¹²².

In tale contesto, AgID elabora linee guida e determinazioni tecniche che disciplinano l'emissione e la gestione delle identità digitali, sia per uso personale sia professionale¹²³.

Le sue funzioni regolatorie si collocano in una posizione intermedia tra strumenti giuridici cogenti e atti di *soft law*: da un lato, norme vincolanti che garantiscono certezza giuridica; dall'altro, strumenti flessibili che permettono di adeguarsi con rapidità all'evoluzione tecnologica e alle dinamiche del quadro europeo¹²⁴. Questa oscillazione, se da un lato genera talvolta incertezze applicative, dall'altro consente un migliore allineamento alle politiche digitali dell'Unione.

A livello europeo, AgID funge da nodo di raccordo per l'Italia nell'ambito del Regolamento eIDAS e, più recentemente, di eIDAS 2. L'Agenzia partecipa ai progetti pilota sul futuro *European Digital Identity Wallet* (EUDI Wallet), contribuendo a validarne l'interoperabilità tecnica e giuridica.

Le attività finora esaminate non si limitano a un profilo strettamente tecnico, ma assumono rilievo politico-istituzionale: l'AgID diviene garante dell'accessibilità universale e della tutela della *privacy*, assicurando che i benefici della

¹²¹ L'AgID è istituita quale agenzia sottoposta alla vigilanza della Presidenza del Consiglio dei ministri: assetto e funzioni sono definiti dal d.l. 22 giugno 2012, n. 83, dal regolamento di organizzazione adottato con D.P.C.M. 8 gennaio 2014 e dagli artt. 14 e 17 del CAD.

¹²² Agenzia per l'Italia Digitale (2018), *Determinazione n. 160 del 4 maggio 2018*, disponibile su <https://www.agid.gov.it>.

¹²³ Agenzia per l'Italia Digitale (2019), *Determinazione n. 318 del 9 maggio 2019*, disponibile su <https://www.agid.gov.it>.

¹²⁴ Sul duplice livello della regolazione in materia di identità digitale, tra vincoli di diritto positivo (*hard law*) e strumenti flessibili (*soft law*) si veda l'art. 71 CAD che attribuisce ad AgID il potere di adottare Linee guida vincolanti, in sostituzione delle regole tecniche.

digitalizzazione siano distribuiti in maniera equa, promuovendo una concezione inclusiva della cittadinanza digitale¹²⁵.

Sul versante istituzionale, l'Agenzia collabora con il Garante per la protezione dei dati personali in relazione alle implicazioni sulla *privacy* derivante dall'utilizzo di SPID. Inoltre, collabora altresì con il Ministero dell'Interno per l'integrazione con la Carta d'Identità Elettronica (CIE), e con i *Qualified Trust Service Providers* (QTSP)¹²⁶, al fine di garantire adeguati livelli di certezza giuridica nelle transazioni elettroniche.

Tuttavia, emergono criticità legate alla *governance* di AgID, in particolare per quanto concerne la capacità di *enforcement*, le risorse limitate e la gestione evolutiva di infrastrutture identitarie critiche.

In prospettiva, diventa dunque essenziale rafforzarne le capacità operative: l'integrazione europea dell'identità digitale richiede competenze tecniche avanzate, risorse finanziarie adeguate e un più efficace coordinamento multilivello tra attori pubblici e privati. Solo attraverso tale potenziamento AgID potrà affrontare con successo le sfide poste dal nuovo portafoglio europeo di identità digitale e dalla sovranità tecnologica.

3.3. *La cittadinanza digitale*

L'analisi svolta consente di affermare come l'identità digitale non possa essere ridotta a mero strumento tecnico di autenticazione ma, piuttosto, debba essere intesa come infrastruttura abilitante per l'esercizio effettivo di diritti e per la partecipazione ai circuiti decisionali, informativi ed economico-sociali della società in rete.

¹²⁵ Si rinvia a § 3.3.

¹²⁶ I *Qualified Trust Service Providers* (QTSP) sono i prestatori qualificati di servizi fiduciari riconosciuti dal Regolamento eIDAS. Essi offrono servizi di identificazione e autenticazione digitale – quali firme elettroniche, sigilli, validazioni temporali, certificati per l'autenticazione di siti *web* – conformi agli *standard* tecnici e giuridici fissati dall'Unione europea. L'accreditamento come “*qualified*” garantisce la presunzione legale di validità e integrità dei servizi prestati, attribuendo loro efficacia probatoria rafforzata in tutti gli Stati membri.

È da questa constatazione che prende forma il concetto di “cittadinanza digitale”¹²⁷, non semplice esito della trasformazione amministrativa, bensì nuovo *status* giuridico che traduce nello spazio virtuale le prerogative del cittadino¹²⁸.

Prima di proseguire circa l’analisi di tale nozione – destinata a occupare posizione centrale nel dibattito sui diritti digitali – si ritiene opportuno formulare alcune considerazioni preliminari che ne chiariscono presupposti e coordinate teoriche.

La cittadinanza¹²⁹ viene tradizionalmente intesa come *status* personale derivante dall’appartenenza del soggetto a un determinato ordine politico¹³⁰. Tale concetto è connesso all’ordinamento giuridico statale, in quanto il conseguimento di detto *status* si rileva nella possibilità per il cittadino di concorrere, attraverso l’espressione del voto, al funzionamento del sistema politico, nonché di divenire

¹²⁷ Sull’argomento si rinvia a G. Pascuzzi, *La cittadinanza digitale*, Bologna, 2021; P. Marsocci, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *AIC*, 1/2015, 1-16; S. Rodotà, *Il diritto di avere diritti*, cit.; A. Simoncini, *Sovranità e potere nell’era digitale*, in T.E. Frosini et al. (a cura di), *Diritti e libertà in Internet*, Firenze, 2017; F. Amoretti, E. Gargiulo, *Dall’appartenenza materiale all’appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, in *Pol. dir.*, 3/2010, 353-389; E.N. Fragale, *La cittadinanza amministrativa al tempo della digitalizzazione*, in *Dir. amm.*, 2/2022, 471-512; T.E. Frosini, *Il diritto costituzionale di accesso a internet*, in *Rivista AIC*, 1/2015, 2 ss.; P. Costanzo, *Avete detto “diritti digitali”*, cit., 145 ss.; F. Di Donato, *Lo stato trasparente. Linked open data e cittadinanza attiva*, Pisa, 2010; F. Costantino, *La c.d. cittadinanza digitale*, in *Dir. pubbl.*, 1/2023, 143 ss.; M. Caporale, *Dalle smart cities alla cittadinanza digitale*, in *federalismi.it*, 2/2020, 30 ss.; E. Di Maria, S. Miceli, *Le frontiere dell’e-government: cittadinanza elettronica e riorganizzazione dei servizi in rete*, Milano, 2004.

¹²⁸ Il concetto di ‘cittadinanza digitale’ non è definito in modo univoco: le discipline nazionali e sovranazionali ne offrono letture differenti, oscillanti tra un’accezione ristretta, ancorata al rapporto tra individuo e pubblica amministrazione, e una più ampia, che investe il catalogo dei diritti fondamentali e le dinamiche dell’appartenenza sovranazionale; v. J.F. Metzl, *Information Technology and Human Rights*, in *Human Rights Quarterly*, 4/1996, 705 ss.

¹²⁹ Per un approfondimento sul tema della cittadinanza, *ex multis*, si rinvia a R. Quadri, voce *Cittadinanza*, in *Novissimo Dig. It.*, vol. III, Torino, 1959, 307 ss.; G. Biscottini, voce *Cittadinanza*, in *Enc. dir.*, vol. VII, Roma, 1960, 140 ss.; C. Romanelli Grimaldi, voce *Cittadinanza*, in *Enc. giur.*, vol. III, Roma, 1988, 1 ss.; R. Clerici, voce *Cittadinanza*, in *Digesto disc. pubbl.*, vol. III, Torino, 1989, 112 ss.; G. Zincone, *Da sudditi a cittadini*, Bologna, 1992; L. Ferrajoli, *Cittadinanza, proprietà, diritti della persona*, in *Pol. econ.*, 1993, 49 ss.; E. Grosso, *Le vie della cittadinanza. Le grandi radici. I modelli storici di riferimento*, Padova, 1997; G. Cordini, *Elementi per una teoria giuridica della cittadinanza*, Padova, 1998; C. Amirante, voce *Cittadinanza (teoria generale)*, in *Enc. dir.*, aggiornamento XI, vol. VI, Roma, 2003, 1 ss.; G. Azzariti, *La cittadinanza. Appartenenza, partecipazione, diritti delle persone*, in *Dir. pubbl.*, 1/2011, 425 ss.; D. Porena, *Il problema della cittadinanza. Diritti, sovranità e democrazia*, Torino, 2011; P. Gargiulo, *Le forme della cittadinanza*, Roma, 2012; T. De Pasquale, *Problemi interpretativi della nozione giuridica di cittadinanza: un concetto «europeizzato» di diritto pubblico interno? La controversa relazione tra cittadinanza dell’Unione europea e cittadinanze nazionali degli Stati membri*, in *Riv. it. dir. pubb. comunit.*, 2012, 445 ss.; P. Mindus, *Cittadini e no. Forme e funzioni dell’inclusione e dell’esclusione*, Firenze, 2014; A. Morrone, *Le forme della cittadinanza nel Terzo Millennio*, in *Quad. cost.*, 2015, 303 ss.; R. Caridà, *I diritti di cittadinanza inclusiva tra esigenze di sicurezza e doveri di solidarietà*, in *federalismi.it*, 14/2017; P. Costa, *Cittadinanza*, Roma-Bari, 2017.

¹³⁰ E.N. Fragale, *La cittadinanza amministrativa al tempo della digitalizzazione*, cit., 475.

titolare di situazioni giuridiche attive e passive nei confronti della comunità di appartenenza¹³¹.

Tuttavia, l'affermarsi dell'«intangibilità dei diritti»¹³² dell'uomo nel nuovo paradigma tecnologico ha condotto al graduale abbandono dell'idea per cui la cittadinanza sia «unica, esclusiva e totalizzante»¹³³ espressione di appartenenza allo Stato-nazione¹³⁴.

Pertanto, alla tradizionale idea di cittadinanza 'sovrana'¹³⁵, si sono affiancate altre forme di cittadinanza con una differente matrice di inclusione giuridica¹³⁶ e risultanti da una pluralità di piani di appartenenza.

Si è così affermata l'idea di una cittadinanza europea¹³⁷, ma anche di una cittadinanza amministrativa¹³⁸ e, da ultimo, – almeno secondo una determinata dottrina – anche quella di cittadinanza digitale. Quest'ultima non introduce soltanto prerogative inedite nate dalle tecnologie dell'informazione, ma riflette nell'ambiente virtuale anche diritti già riconosciuti (basti pensare alla libertà di espressione, alla partecipazione democratica o alla tutela dei dati personali)

¹³¹ Cfr. P. Costa, *Cittadinanza*, cit.; P. Lombardi, *Giudice amministrativo e cittadinanza: quale contributo per un concetto giuridicamente sostenibile?*, in *federalismi.it*, 20/2018; T.H. Marshall, *Citizenship and Social Class*, in *Inequality and Society*, J. Manza, M. Sauder (eds.), New York, 2009; G. Moro, *Cittadinanza*, Milano, 2020.

¹³² G. Berti, *Cittadinanza, cittadinanze e diritti fondamentali*, in *Riv. dir. cost.*, 1997, 3 ss.

¹³³ D. Kochenov, *Cittadinanza. La promessa di un alchimista*, Bologna, 2020, 204.

¹³⁴ Espressione utilizzata da E.N. Fragale, *La cittadinanza amministrativa ai tempi della digitalizzazione*, cit., 476. V. anche F. Cortese, *Cittadinanza e liberalizzazioni*, in F. Cortese et al. (a cura di), *Dallo status di cittadino ai diritti di cittadinanza. Quaderni della facoltà di giurisprudenza*, 2, 2014, 17 ss.

¹³⁵ E.N. Fragale, *La cittadinanza amministrativa ai tempi della digitalizzazione*, cit., 476.

¹³⁶ G. Arena, *Il principio della sussidiarietà orizzontale nell'art. 118, u.c., della Costituzione*, in *Studi in onore di Giorgio Berti*, Napoli, 2005, 217.

¹³⁷ Sul tema M. Cartabia, *Cittadinanza europea*, in *Enc. giur. Treccani*, vol. VI, Roma, 1995; V. Lippolis, *La cittadinanza europea*, Bologna, 1994; F. Menegazzi Munari, *Cittadinanza europea: una promessa da mantenere*, Torino, 1996; B. Nascimbene, *Diritti di cittadinanza e libertà di circolazione nell'Unione europea*, Padova, 2012; S. O'Leary, *The Evolving Concept of Community Citizenship*, London, Kluwer, 1996.

¹³⁸ Con riferimento alla cittadinanza amministrativa, essa è stata intesa come appartenenza alla comunità locale, propria del residente o come capacità di diritto pubblico, sintesi delle facoltà, interessi e diritti riconosciuti in capo all'amministrato nel rapporto amministrativo. Si tratta di un complesso di situazioni giuridiche tra loro diversificate, comprensive non solo di diritti sociali ma altresì di situazioni giuridiche legate alla dinamica procedimentale. Sul tema *ex multis* R. Cavallo Perin, *La configurazione della cittadinanza amministrativa*, in *Dir. amm.*, 1/2004, 201 ss.; F. Manganaro, *Vecchi problemi e nuove prospettive della cittadinanza*, in F. Manganaro, A. Romano Tassone (a cura di), *Persona ed amministrazione. Privato, cittadino, utente e pubbliche amministrazioni*, Torino, 2004; S. Cassese, *Il cittadino e l'amministrazione pubblica*, in *Riv. trim. dir. pubbl.*, 1998, 1015 ss.; S. Pellizzari, *La cittadinanza amministrativa tra diritto europeo e diritto nazionale*, in F. Cortese et al. (a cura di), *Dallo status di cittadino ai diritti di cittadinanza*, Napoli, 2014.

conferendo loro forme d'esercizio più ampie, modalità di fruizione innovative e, talvolta, contenuti ulteriormente arricchiti. Secondo questa prospettiva, dunque, l'universo digitale non sostituisce il catalogo classico dei diritti, bensì lo estende e lo riqualifica permettendo di trasformare le tradizionali garanzie in strumenti adeguati alle dinamiche di uno spazio relazionale ormai inscindibilmente connesso. Nel descritto contesto, l'espressione 'cittadinanza digitale' ha ormai da tempo trovato spazio nell'ordinamento giuridico, ove tuttavia non è sempre adoperata con accezione univoca. Ad essa – sul piano delle fonti – fa esplicito richiamo la rubrica della sezione II del già esaminato CAD¹³⁹ nella parte in cui individua una 'Carta della cittadinanza digitale'. Il riferimento ai diritti di 'cittadinanza digitale' figura anche all'art. 17, co. 1-*quinquies*, della stessa normativa che prevede l'obbligo dell'AgID di pubblicare sul suo sito istituzionale una guida sui diritti di cittadinanza digitale previsti dallo stesso Codice *de qua*.

Inoltre – sul versante europeo – alla cittadinanza digitale è dedicato anche un capitolo della Comunicazione della Commissione europea del 9 marzo 2021¹⁴⁰, in cui è prevista l'adozione di una 'Dichiarazione europea sui diritti e i principi digitali'¹⁴¹.

Nella dimensione nazionale, il fenomeno della cittadinanza digitale si ritrova più ancorato a un nuovo modo di intendere le relazioni tra utente e amministrazione.

Il CAD prende infatti in considerazione solo una parte del più ampio catalogo dei diritti digitali, concentrandosi in particolare sulle pretese digitali esercitabili nei confronti dell'amministrazione. Restano in secondo piano i diritti sorti per evoluzione e adattamento delle libertà fondamentali della persona (quali la

¹³⁹ Si rinvia al § 2.1.

¹⁴⁰ Comunicazione della Commissione europea del 9 marzo 2021, 2030 *Digital Compass: the European way for the Digital Decade*, COM(2021) 118 final, in cui viene delineata la strategia europea per la trasformazione digitale del prossimo decennio e prospettata l'adozione di una Dichiarazione europea sui diritti e i principi digitali, destinata a costituire un quadro di riferimento politico per gli Stati membri e le istituzioni dell'Unione.

¹⁴¹ La 'Dichiarazione europea sui diritti e i principi digitali' per il decennio digitale è stata proclamata congiuntamente dal Parlamento europeo, dal Consiglio e dalla Commissione il 26 gennaio 2022 (GUUE C 23 del 23.1.2023, p. 1 ss.). Essa individua sei aree prioritarie – centralità della persona, solidarietà e inclusione, libertà di scelta, partecipazione democratica, sicurezza e sostenibilità – costituendo un quadro politico di riferimento per orientare le politiche digitali dell'Unione e degli Stati membri.

protezione dei dati personali o il diritto all'oblio). In questo senso, sembrerebbe più opportuno fare riferimento a una 'cittadinanza amministrativa digitale'¹⁴².

Nella dimensione euro-unionale, invece, la cittadinanza digitale viene trattata in una prospettiva indubbiamente più ampia, superando quello 'statuto' circoscritto al rapporto tra amministrato e amministrazione pubblica. Si tratta di un approccio che intende offrire effettiva tutela nei riguardi della persona, senza tralasciare ad esempio le minacce che sempre più di frequente tendono a presentarsi nelle relazioni con i poteri privati.

Alla luce delle considerazioni sinora espresse, si evince la ragione per cui la cittadinanza digitale sia destinata a configurarsi come un nuovo *status* del cittadino¹⁴³.

La proiezione della cittadinanza nel mondo virtuale non comporta una duplicazione della cittadinanza dell'individuo, bensì l'emergere di una nuova forma di cittadinanza, per l'appunto 'digitale'.

Nello spazio virtuale, diritti 'classici' e prerogative di nuova generazione (interoperabilità, controllo sui propri dati, sicurezza cibernetica) si intrecciano in un unico fascio di situazioni giuridiche. In tale contesto, l'effettiva titolarità di una identità digitale diviene condizione di tale cittadinanza. Senza un'identità digitale spendibile l'individuo è posto ai margini del circuito decisionale, informativo e sociale che oggi si svolge principalmente *online*.

La sfida non è sovrapporre un riflesso digitale alla tradizionale idea di cittadinanza, ma di ridisegnarla come spazio aperto e inclusivo capace di evitare che il divario tecnologico si traduca in un divario di diritti.

¹⁴² E.N. Fragale, *La cittadinanza amministrativa al tempo della digitalizzazione*, cit., 481.

¹⁴³ Sul fenomeno della c.d. "proliferazione" delle cittadinanze, inteso come riflesso del progressivo indebolimento della sovranità statale a seguito di processi quali la globalizzazione, l'integrazione europea, il rafforzamento delle entità politiche sub-statali e la digitalizzazione dell'economia e della società, cfr. V. De Santis, *Cittadinanza digitale e diseguaglianze*, in *Italian Papers on Federalism*, 1/2025, 3; F. Manganaro, *Dalla cittadinanza alle cittadinanze. Questioni su un concetto polimorfico*, in *AmbienteDiritto.it*, 4/2022, 4; E.N. Fragale, *La cittadinanza amministrativa al tempo della digitalizzazione*, cit., 476.

CAPITOLO II

Tecnologie emergenti e ridefinizione dell'identità

1. Le nuove frontiere tecnologiche dell'identità digitale

L'incessante evoluzione delle tecnologie dell'informazione¹⁴⁴ sta riconfigurando in profondità il paradigma dell'identificazione elettronica.

Alle soluzioni basate su credenziali tradizionali (*username/password*) o su dispositivi crittografici, si affiancano oggi tre 'motori di innovazione' – intelligenza artificiale, sistemi biometrici, tecnologie a registro distribuito (DLT) – destinati a ridefinire tanto l'architettura tecnica quanto il quadro giuridico dell'identità digitale.

I sistemi biometrici riducono l'asimmetria tra identità fisica e digitale, trasformando tratti corporei (impronta digitale, volto, voce, iride) in *template* numerici qualificati come «categorie particolari di dati personali» ai sensi dell'art. 9 GDPR. Tuttavia, l'immutabilità di tali dati rende di fatto impossibile revocare il fattore di autenticazione in caso di violazione, esponendo l'individuo a rischi di profilazione irreversibili. Ne consegue l'esigenza di un rafforzato presidio regolatorio: un ruolo più incisivo sia del Garante della *privacy*, sia dell'AgID che dovrà definire *standard* di sicurezza omogenei, specie in relazione all'imminente ecosistema EUDI *Wallet*. L'affidabilità dei sistemi biometrici dipende, a propria volta, dai modelli di

¹⁴⁴ Le intersezioni tra diritto e informatica sono da tempo oggetto di approfondimento nella letteratura giuridica. Senza pretese di esaustività si richiamano V. Frosini, *Cibernetica, diritto e società*, Milano, 1968 e *Informatica, diritto e società*, Milano, 1988. Sul piano internazionale si richiamano D.R. Johnson, D. Post, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 5/1996, 1367 ss. circa il dibattito del cyberspazio come ambito che, per le sue caratteristiche intrinseche, necessita di un sistema di regole distinto rispetto a quello applicabile ai territori geograficamente delimitati e L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999. In tempi più recenti si segnalano F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019; Id., *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, 16/2020, 79 ss.; Id., *Società tecnologica, amministrazione pubblica e diritti digitali*, in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Padova, 2021, 17 ss.; Id., *Regolazione della società e protezione dei diritti nell'era tecnologica*, in G. Cassano, S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 17 ss.; Id., *Diritto all'esistenza digitale*, in *BioLaw Journal - Rivista di BioDiritto*, n. 3/2019, 91 ss.

intelligenza artificiale addestrati su immagini o segnali biometrici rappresentativi delle diversità etniche e di genere.

Il regolamento sull'Intelligenza Artificiale, entrato in vigore nel 2025, classifica i sistemi di identificazione biometrica remota in spazi pubblici “ad alto rischio”, assoggettandoli a valutazioni di conformità *ex ante*, a obblighi di trasparenza algoritmica e all'iscrizione in una banca-dati europea per agevolare il controllo diffuso.

Prendendo in considerazione l'intelligenza artificiale come frontiera tecnologica autonoma è possibile rintracciare una duplice veste. In prospettiva difensiva, essa consente di individuare anomalie nell'uso delle credenziali e di rafforzare i meccanismi di autenticazione.

Sul versante offensivo, le stesse tecniche possono essere impiegate per generare *deep fake* capaci di eludere i controlli biometrici. Per tali ragioni, la disciplina europea insiste su strumenti di gestione del rischio e su verifiche periodiche dei sistemi, così da prevenire abusi e ridurre i rischi di manipolazione algoritmica.

La terza frontiera è rappresentata dalla *blockchain* e, più in generale, dalle tecnologie a registro distribuito (*Distributed Ledger Technologies*).

L'architettura decentralizzata di tali registri offre un'alternativa radicale ai modelli centralizzati o federati di gestione identitaria. Questo paradigma – alla base delle sperimentazioni di *Self-Sovereign Identity* (SSI) che verranno approfondite nel capitolo successivo – attribuisce all'utente il controllo esclusivo delle proprie chiavi crittografiche necessarie per dimostrare selettivamente attributi diversi a contesti diversi (*selective disclosure*). L'immutabilità dei blocchi, la marcatura temporale e la decentralizzazione del consenso consentono di superare la necessità di un'autorità di registrazione centralizzata, rafforzando la fiducia intersoggettiva e semplificando l'onere probatorio in sede amministrativa o giudiziaria. Tuttavia, la persistenza dei dati entra in tensione con il diritto alla cancellazione ai sensi dell'art. 17 GDPR, imponendo soluzioni innovative di ‘reversibilità’ della registrazione.

L'interazione sinergica fra queste tre classi di tecnologie innesca dinamiche di reciproco potenziamento, tuttavia, ogni avanzamento tecnico costituisce un'arma a doppio taglio amplificando il rischio di sorveglianza pervasiva e di esclusione algoritmica.

Il capitolo che segue si articola in tre sezioni dedicate, rispettivamente, al cuore tecnologico di ciascuna frontiera (§1.1-1.3), ai riflessi socio-giuridici in termini di profilazione e sorveglianza, con particolare attenzione al dibattito sull'*Internet governance* e alla cosiddetta 'terza via' europea (§ 2.1-2.3) e, infine, ai modelli architetturali di gestione dell'identità (§ 3.1-3.3).

L'obiettivo è duplice: da un lato, mettere in luce le potenzialità di innovazione e semplificazione insite nelle nuove tecnologie; dall'altro, evidenziare le aree di fragilità normativa che richiedono una regolazione tempestiva e proporzionata affinché l'identità digitale resti, nell'ecosistema iperconnesso, uno strumento di emancipazione e non piattaforma di disuguaglianza.

1.1. Intelligenza artificiale e machine learning

L'intelligenza artificiale¹⁴⁵ (d'ora in avanti, IA) ha rivoluzionato numerose dimensioni dell'agire umano¹⁴⁶, ridefinendo le modalità con cui l'individuo interagisce, lavora e si identifica nell'ambiente *online* e *offline*¹⁴⁷.

¹⁴⁵ La produzione scientifica sul tema è ormai vastissima; senza alcuna pretesa di esaustività si possono richiamare, tra gli altri, L. Floridi, *Etica dell'intelligenza artificiale*, Milano, Cortina, 2022; A. D'Aloia, *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021; Id., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, 1/2019, 4 ss.; G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996; M.A. Boden, *L'Intelligenza Artificiale*, Bologna, 2019, 119 ss.; A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020; G. Finocchiaro, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 4/2022, 1085 ss.; A.C. Mangiameli Amato, *Intelligenza artificiale, "big data" e nuovi diritti*, in *Riv. inf. dir.*, 1/2022, 93 ss.; S.J. Russel, P. Norvig, *Artificial intelligence. A modern approach*, New Jersey, 2010; J.C. Heudin, *Intelligence Artificielle. Manuel de survie*, Science-eBook, 2017. Quanto al rapporto tra intelligenza artificiale e pubblica amministrazione si vedano, tra gli altri, D. Marongiu, *L'attività amministrativa automatizzata*, Santarcangelo di Romagna, 2005; A. Masucci, *Procedimento amministrativo e nuove tecnologie*, Torino, 2011; D.U. Galetta, J.G. Corvalán, *Intelligenza artificiale per una Pubblica Amministrazione 4.0?*, in *federalismi.it*, 3/2019, 7 ss.; E. Picozza, *Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence*, in *Giur. it.*, 7/2019, 1657 ss.; S. Vaccari, *Note minime in tema di Intelligenza Artificiale e decisioni amministrative*, in *Giustamm.it*, 10/2019, 1 ss.; P. Forte, *Diritto amministrativo e Data Science. Appunti di intelligenza amministrativa artificiale (AAI)*, in *P.A. Persona e Amministrazione*, 1/2020, 247 ss.; G. Pesce, *Funzione amministrativa, intelligenza artificiale e Blockchain*, Napoli, 2021; A.G. Orofino, *Pubblici servizi, digitalizzazione e intelligenza artificiale*, in R. Giordano et al. (a cura di), *Il diritto nell'era digitale*, Milano, 2022, 541 ss.; L. Previti, *La decisione amministrativa robotica*, Napoli, 2022; M. Macchia, A. Mascolo, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in *Giorn. dir. amm.*, 4/2022, 556 ss.; V. Fanti, *Intelligenza artificiale e diritto amministrativo: prospettive, limiti e pericoli*, in *Dir. e proc. amm.*, 4/2022, 1001 ss.; G. Gallone, *Riserva di umanità e funzioni amministrative*, cit.; Id., *Digitalizzazione, amministrazione e persona: per una "riserva di umanità" tra spunti codicistici di teoria giuridica dell'automazione*, in *PA Persona e Amministrazione*, 1/2023, 329 ss.; B. Marchetti, *Intelligenza artificiale, poteri pubblici e "rule of law"*, in *Riv. it. dir. pubbl.*, 1/2024, 49 ss.; M.C. Cavallaro, *Intelligenza artificiale, interesse pubblico e complessità della scelta amministrativa*, in *Amministrativamente*, 3/2024, 936 ss.

¹⁴⁶ Cfr. A. Longo, G. Scorza, *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Milano, 2020; T. Scantamburlo, A. Charlesworth, N. Cristianini, *Machine Decisions and Human Consequences*, in K. Yeung, M. Lodge (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, 69 ss.

¹⁴⁷ Sull'opportunità di superare la distinzione tra dimensione *online* e *offline*, si veda l'*Onlife Manifesto* promosso dalla Direzione Generale CONNECT della Commissione europea (2013) e coordinato da Luciano Floridi. Il documento introduce il concetto di '*onlife*' per descrivere la nuova esperienza ibrida dell'esistenza contemporanea, in cui l'individuo agisce e si identifica in un ambiente informazionale integrato, l'"infosfera". Il Manifesto ha influenzato profondamente la riflessione etica e giuridica sull'impatto delle tecnologie emergenti, v. L. Floridi (ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Berlino, 2014.

Nel rivoluzionare le stesse interazioni sociali, l'IA ha progressivamente inciso in settori giuridicamente rilevanti, tra cui la sanità, la finanza, i trasporti, l'istruzione e, per ciò che ci interessa, l'identificazione elettronica.

Al giorno d'oggi, infatti, l'intelligenza artificiale rappresenta la frontiera evolutiva dei sistemi di identità digitale attraverso l'elaborazione di documenti di riconoscimento, attributi biometrici e segnali contestuali.

È opportuno evidenziare che tale tecnologia non ha ricadute soltanto sul piano strettamente tecnico-operativo, ma può incidere altresì sul piano esistenziale della persona con riferimento alla sua 'proiezione digitale'. In questa prospettiva, la pervasività dei sistemi di intelligenza artificiale ha imposto un'esigenza regolatoria stringente culminata, da ultimo, nell'elaborazione del Regolamento (UE) 2024/1689 (IA *Act*)¹⁴⁸. Prima di procedere con l'analisi di tale cornice normativa, si ritiene necessario soffermarsi brevemente sui profili definitori dell'IA.

Così come non esiste una nozione univoca di "intelligenza" nella riflessione filosofica e scientifica¹⁴⁹, altrettanto complesso risulta circoscrivere il significato di

¹⁴⁸ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) approvato il 13 giugno 2024 (e pubblicato nella Gazzetta ufficiale dell'Unione europea in data 12 luglio 2024).

¹⁴⁹ L'*Oxford Companion to the Mind* (opera di riferimento enciclopedica sulla mente umana) nel definire l'intelligenza ha affermato: «sono disponibili innumerevoli test per misurare l'intelligenza, ma nessuno sa con sicurezza che cosa sia l'intelligenza, e addirittura nessuno sa con sicurezza che cosa misurino i test disponibili», R.L. Gregory, *«Innumerable tests are available for measuring intelligence, yet no one is quite sure of what intelligence is, or even of just what is that the available tests are measuring»*, voce "Intelligence", in *The Oxford Companion to the Mind*, Oxford, 1987, 375. Sulla definizione di intelligenza e di intelligenza artificiale si rinvia a G. Pasceri, *Intelligenza artificiale, algoritmo e machine learning. La responsabilità del medico e dell'amministrazione sanitaria*, Milano, 2021, 15-18.

“intelligenza artificiale”¹⁵⁰. Si tratta di un concetto dinamico che abbraccia diversi metodi e campi di applicazione in continuo sviluppo¹⁵¹.

In una fase precedente, l’ordinamento sovranazionale si era limitato a definire l’intelligenza artificiale in specifici atti di *soft law*. In particolare, la “Carta etica europea sull’utilizzo dell’intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi”¹⁵² (approvata dalla Commissione europea nel 2018) ha descritto l’intelligenza artificiale come «insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine, le capacità cognitive degli esseri umani».

Ancora, un ulteriore richiamo definitorio si riscontra nella “Comunicazione della Commissione europea del 25 aprile 2018”¹⁵³, ove il termine ‘intelligenza artificiale’ viene utilizzato per indicare «sistemi che mostrano un comportamento intelligente analizzando l’ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi».

Da ultimo, il Legislatore europeo ha proposto una definizione di natura descrittiva stabilendo che un ‘sistema di intelligenza artificiale’ è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e 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,

¹⁵⁰ L’espressione “intelligenza artificiale” è stata coniata nel 1955 dal matematico e informatico statunitense John McCarthy nell’ambito di un progetto di ricerca che presentò per un seminario estivo al Dartmouth College. Nella traduzione italiana, lo studioso la definiva come: «un processo consistente nel far sì che una macchina si comporti in modi che sarebbero definiti intelligenti se fosse un essere umano a comportarsi allo stesso modo», in J. McCarthy, M. Minsky, N. Rochester, C. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Stanford, 31 agosto 1955.

Tra i primi studi scientifici in tema di intelligenza artificiale non possono che essere richiamati i lavori di A. Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, in *Proceedings of the London Mathematical Society*, 1936, 230 ss.; Id, *Computing Machinery and Intelligence*, in *Mind*, 59/1950, 433 ss.; A.L. Samuel, *Some Studies in Machine Learning Using the Game of Checkers*, in *Journal of Research and Development*, 3/1959, 210 ss.; M.L. Minsky, *Semantic Information Processing*, Cambridge (MA), 1968. Sul funzionamento della c.d. macchina di Turing, si vedano, tra gli altri, E. Rich, K. Knight, *Artificial Intelligence*, New York, 1991; K. Warwick, H. Shah, *Turing’s Imitation Game*, Cambridge (UK), 2016.

¹⁵¹ Si rimanda ad A. Santosuosso, *Intelligenza artificiale e diritti. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, 6 ss.

¹⁵² *Carta etica europea sull’utilizzo dell’intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, CEPEJ(2018)14, appendice III, 47.

¹⁵³ Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L’intelligenza artificiale per l’Europa*, COM(2018) 237, 25 aprile 2018.

raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»¹⁵⁴. Accanto l'esigenza di chiarire il concetto di intelligenza artificiale, l'IA Act¹⁵⁵ – affermando l'antropocentrismo dell'ambiente digitale¹⁵⁶ – ha predisposto un complesso uniforme di regole¹⁵⁷ al fine di affrontare i rischi¹⁵⁸ connessi agli impieghi più delicati della tecnologia¹⁵⁹, modulando la regolazione in relazione alla

¹⁵⁴ Art. 3, par. 1, IA Act.

¹⁵⁵ L'IA Act rappresenta una tappa di svolta sostituendo l'impostazione programmatica dei precedenti interventi a una disciplina organica e giuridicamente vincolante. Tra i diversi contributi in dottrina sul tema si vedano, *ex multis*, B. Carotti, *Le finzioni dell'intelligenza senza corpo, o dell'“AI Act”*, in *Giorn. dir. amm.*, 1/2025, 31 ss.; G. Finocchiaro, *Intelligenza Artificiale. Quali regole?*, Bologna, 2024; G. Lo Sapio, *L'“Artificial Intelligence Act” e la prova di resistenza per la legalità algoritmica*, in *federalismi.it*, 16/2024, 265 ss.; C. Novelli, *L'“Artificial Intelligence Act” (AIA) Europeo: alcune questioni di implementazione*, in *federalismi.it*, 2/2024, 95 ss.; A. Malaschini, *Il regolamento europeo sull'intelligenza artificiale (IA), l'orientamento italiano e i diversi indirizzi di Stati Uniti e Regno Unito*, in *Rass. Parl.*, 1/2024, 35 ss.; A.M. Alaimo, *Il Regolamento sull'Intelligenza Artificiale. Un treno al traguardo con alcuni vagoni rimasti fermi*, in *federalismi.it*, 25/2024, 231 ss.; J. Ponce Solé, *Il regolamento dell'unione europea sull'intelligenza artificiale, la discrezionalità amministrativa e la riserva di umanità*, in *Riv. trim. dir. pubbl.*, 3/2024, 825 ss.; N. Zorzi Galgano, *Il Regolamento UE 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contr. impr.*, 1/2025, 45 ss.; S. Pagliantini, *La base giuridica dell'AI Act ex art. 114 Tfu: l'intelligenza artificiale tra mercato e persona*, in *Foro it.*, 1/2025, 19 ss.; L. Previti, *La proposta di regolamento europeo in materia di intelligenza artificiale tra incertezze applicative ed esigenze di semplificazione*, in *Rassegna trimestrale dell'Osservatorio AIR*, 1/2023, 19 ss.; G. Contissa, F. Galli, *AI Act e diritti fondamentali: presupposti tecnologici e ricadute normative*, in *Quad. cost.*, 3/2024, 738 ss.; R. Ruoppo, *Il regolamento UE in materia di Intelligenza Artificiale (c.d. AI Act): un quadro normativo uniforme per la tutela dei diritti fondamentali*, in *Rass. dir. civ.*, 3/2024, 996 ss.; R. Petruso, G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *La Nuova Giurisprudenza Civile Commentata*, 4/2024, 989 ss.

¹⁵⁶ Art. 1 IA Act in cui viene chiarito l'oggetto e lo scopo del Regolamento (par. 1) si afferma: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione». Cfr. anche considerando 1 e considerando 176.

¹⁵⁷ Il fondamento giuridico dell'IA Act è rinvenibile negli articoli 114 TFUE e 16 TFUE. Il bilanciamento tra 'benessere' e 'mercato' rievoca quella che è stata definita «doppia anima» (suggerimento di N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati*, Milano, 2019, 35) già con riguardo al GDPR e in cui resta latente la dialettica tra persona e mercato, che ha nel tempo segnato il passaggio «dall'Europa dei mercati all'Europa dei diritti». Su quest'ultimo punto v. G. Alpa, M. Andenas, *L'Europa dei diritti e i diritti fondamentali*, in G. Alpa, M. Andenas, *Fondamenti del diritto privato europeo*, Milano, 2005, 53 ss.

¹⁵⁸ La regolazione dell'IA Act è incentrata sull'applicazione del principio di precauzione che ha l'obiettivo di assicurare un livello elevato di protezione dei diritti fondamentali, attraverso un approccio basato «sul rischio chiaramente definito».

¹⁵⁹ Affrontare il problema dei rischi associati all'impiego dell'IA era uno degli obiettivi indicati nel Libro bianco sull'IA pubblicato dalla Commissione il 19 febbraio 2020 (Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM(2020)65).

pericolosità¹⁶⁰. L'utilizzo e la commercializzazione dei sistemi di intelligenza artificiale sono infatti diversamente calibrati tenendo in considerazione le caratteristiche oggettive degli stessi sistemi, le loro funzioni e i compiti che sono chiamati a svolgere¹⁶¹.

Se da un lato il Regolamento inquadra gli usi legittimi dell'intelligenza artificiale secondo una scala di rischio crescente, dall'altro individua un nucleo di pratiche – tra le quali la manipolazione subliminale¹⁶², il *social scoring* generalizzato¹⁶³ e il riconoscimento biometrico in tempo reale ai fini di sorveglianza di massa¹⁶⁴ – intrinsecamente inaccettabili in quanto lesivi dei diritti fondamentali, dell'identità personale e pericolosi per lo sviluppo della personalità individuale.

Per quanto concerne le tecniche di manipolazione, il riferimento è ai sistemi di IA che impiegano componenti subliminali – come stimoli sonori, visivi o audiovisivi – capaci di agire al di sotto della percezione umana¹⁶⁵. Questi sistemi, insieme ad altre tecniche manipolative o ingannevoli, sono idonei a pregiudicare la capacità decisionale, la libertà di autodeterminazione dei singoli, arrecando (anche potenzialmente) un «danno significativo»¹⁶⁶ agli stessi.

Per tali ragioni, le pratiche appena descritte sono vietate: il presidio normativo integra e rafforza le tutele previste dalla direttiva sulle pratiche commerciali sleali, salvaguardando la dignità della persona e la libera formazione della volontà nell'ecosistema digitale.

Ulteriore tecnica di IA vietata dalla normativa in questione concerne il *social scoring*, ovvero l'attribuzione di un punteggio sociale sulla base del comportamento sociale o di caratteristiche personali o della personalità note, dedotte o previste¹⁶⁷.

¹⁶⁰ V. De Santis, *Identità e persona all'epoca dell'intelligenza artificiale: riflessioni a partire dall'IA Act*, in *federalismi.it*, 19/2024, 151.

¹⁶¹ U. Ruffolo, A. Amidei, *La regolazione ex ante dell'intelligenza artificiale tra gestione del rischio by design, strumenti di certificazione preventiva e «autodisciplina» di settore*, in A. Pajno, F. Donati, A. Perrucci, *Intelligenza artificiale e diritto*, cit., 494.

¹⁶² Considerando 29 e art. 5, par. 1, lett. a).

¹⁶³ Considerando 31 e art. 5, par. 1, lett. c).

¹⁶⁴ Considerando 32 e art. 5, par. 1, lett. h); 2, 3, 4, 5, 6, 7.

¹⁶⁵ Considerando 29.

¹⁶⁶ Il divieto opera a prescindere dalla prova di un intento doloso: è sufficiente che la distorsione comportamentale e il «danno significativo» siano conseguenze ragionevolmente prevedibili dell'adozione di tali tecniche. Sono escluse, invece, le pratiche lecite in ambito medico, come la riabilitazione cognitiva o il trattamento psicoterapeutico, purché svolte nel rispetto delle norme di settore e previa acquisizione di un consenso informato effettivo (Considerando 29).

¹⁶⁷ Art. 5, par. 1, lett. c).

L'attribuzione del punteggio sociale è vietata quando da quest'ultima derivi un trattamento pregiudizievole o sfavorevole in contesti sociali non collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, oppure se tale trattamento pregiudizievole risulti ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità.

La disciplina intende dunque vietare quei sistemi impiegati in modo massiccio¹⁶⁸ – come, ad esempio, in Cina¹⁶⁹ – che divengono strumento di gestione sociale al fine di orientare il comportamento di imprese, individui e organizzazioni sociali, trasformandosi in una vera e propria «infrastruttura digitale di sorveglianza»¹⁷⁰. Dunque, nel contesto europeo si è consolidata la consapevolezza che i sistemi di credito sociale rispetto al singolo possono costituire una forma di manipolazione inconsapevole capace di plasmare l'identità e orientare il comportamento mentre, sul piano collettivo rischiano di diventare uno strumento di controllo sociale diffuso¹⁷¹.

Infine, anticipando il principale oggetto di studio del successivo paragrafo, un ulteriore fattore di rischio per la tutela dell'identità è rappresentato dall'impiego dell'intelligenza artificiale per il riconoscimento biometrico.

Ciò, come è noto, in ragione della capacità della tecnologia in questione di identificare una persona attraverso le sue caratteristiche fisiologiche o

¹⁶⁸ Il Regolamento vieta espressamente quei sistemi di IA che attribuiscono un punteggio alla persona sulla base di una raccolta pervasiva di comportamenti, per poi condizionare l'accesso a diritti o opportunità. In tali modelli di *social scoring* un credito sociale basso si traduce, ad esempio, nell'esclusione da sussidi economici, nel divieto di espatrio o nell'impossibilità di accedere a scuole e università selezionate. L'effetto complessivo è una forma di sorveglianza di massa che, attraverso un sistema di premi e penalità, orienta il comportamento individuale violando il diritto alla dignità e alla non discriminazione (Considerando 31). Per un approfondimento si rimanda ad A. Vigorito, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *MediaLaws*, 1/2023, 104 ss.; G. Sciascia, *Reputazione e potere: il "social scoring" tra distopia e realtà*, in *Giorn. dir. amm.*, 3/2021, 317 ss.; Y. Citino, *Cittadinanza "a punti" e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, in *Dir. comp.*, 22 giugno 2022; T. Lam, *The People's Algorithms: Social Credits and the Rise of China's Big (Br)other*, in A. Mennicken, R. Salais (eds.), *The New Politics of Numbers. Utopia, Evidence and Democracy*, Palgrave Macmillan, Cham, 2022, 71 ss.

¹⁶⁹ A.S.Y. Cheung, Y. Chen, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, in *Law & Social Inquiry*, vol. 47, 4, 1137 e ss.

¹⁷⁰ Così V. De Santis, *Identità e persona all'epoca dell'intelligenza artificiale*, cit., 153. Sul tema si rinvia a G. Kostka, *China's social credit systems and public opinion: Explaining high levels of approval*, in *New media & Society*, 21/2019, 1565 ss.; F. Liang, V. Das, N. Kostyuk, M.M. Hussain, *Costructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy & Internet*, 10/2018, 415 ss.

¹⁷¹ V. De Santis, *Identità e persona all'epoca dell'intelligenza artificiale*, cit., 154.

comportamentali, agevolando processi di «categorizzazione»¹⁷² di individui e interi gruppi su larga scala.

In assenza di un'interazione fisica con l'interessato, i sistemi di riconoscimento biometrico basati su intelligenza artificiale sono in grado di accertare l'identità di una persona confrontando i tratti biometrici rilevati (ad esempio tramite videocamera o microfono) con i dati biometrici già archiviati in uno o più *database*. Le immagini o le tracce audio acquisite vengono elaborate dall'algoritmo, che raffronta le caratteristiche estratte con quelle memorizzate, restituendo in tempo reale la corrispondenza positiva o negativa e consentendo, di fatto, l'identificazione a distanza della persona.

I rischi derivanti dall'impiego di sistemi di riconoscimento biometrico diventano particolarmente critici quando l'autorità pubblica li utilizza «in tempo reale in spazi accessibili al pubblico»¹⁷³, per identificare istantaneamente soggetti all'interno di flussi indeterminati di passanti. Tale scenario prefigura un controllo pervasivo che si tradurrebbe in una vera e propria sorveglianza di massa¹⁷⁴, in evidente tensione con i principi di una democrazia pluralista.

L'approfondimento degli aspetti giuridici e tecnici di tale frontiera tecnologica costituirà oggetto del prossimo paragrafo¹⁷⁵.

Dunque, l'intelligenza artificiale del futuro dovrà essere necessariamente sicura e, soprattutto, in grado di suscitare fiducia nei cittadini¹⁷⁶. Ciò assume particolare rilievo con riferimento ai concetti di identificazione e identità personale, da un lato particolarmente permeabili al decorso del tempo, all'evoluzione tecnologica e al mutare della sensibilità collettiva, dall'altro indissolubilmente legati alle garanzie costituzionali della persona.

¹⁷² Considerando 16.

¹⁷³ Art. 5, par. 1, lett. h); 2, 3, 4, 5, 6, 7.

¹⁷⁴ F. Mollo, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, in *federalismi.it*, 19/2023, 267 ss. Più ampiamente sul tema è fondamentale la riflessione di S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

¹⁷⁵ *Infra* § 1.2.

¹⁷⁶ E.C. Raffiotta, M. Baroni, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal - Rivista di BioDiritto*, 1/2022, 179.

1.2. I sistemi di riconoscimento biometrico

L'identificazione elettronica fonda, in misura crescente, la propria affidabilità sull'elaborazione di dati biometrici, ossia dati personali tratti da caratteristiche fisiche o comportamentali uniche e identificative di ciascuna persona fisica¹⁷⁷.

Il Regolamento GDPR qualifica tali dati come «categorie particolari» di dati personali¹⁷⁸ e li definisce come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»¹⁷⁹. Costituiscono esempi di dati biometrici le impronte digitali, la conformazione fisica della mano, del volto, dell'iride o della retina, il timbro e la tonalità della voce.

La raccolta delle informazioni biometriche avviene mediante componenti *hardware* e *software* che acquisiscono le informazioni e le analizzano confrontandole con dati precedentemente acquisiti e custoditi in appositi *database*. Tali dati, in linea di massima, garantiscono un'autenticazione sicura e univoca, semplificando allo stesso tempo la gestione delle credenziali¹⁸⁰. La biometria, in tal senso, rappresenta certamente una delle più significative evoluzioni tecnologiche nel campo dell'identificazione digitale. Non possono tuttavia essere trascurate le opacità connesse a tale tecnologia. Segnatamente, la fase di verifica dell'autenticità solleva

¹⁷⁷ Per una panoramica sul tema v. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; E. Cadamuro, *Le nuove sfide per la tutela dei dati biometrici nella costruzione dell'identità digitale: tra istanze europee e sistema nazionale*, in *Riv. trim. dir. pen. econ.*, 3-4/2024, 364 ss.; R. Das, *The science of Biometrics: Security technology for identity Verification*, Routledge, 2019; A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2/2019; G. Singh, G. Bhardwaj, S.V. Singh, V. Garg, *Biometric Identification System: Security and Privacy Concern*, in S. Awasthi et al. (eds.), *Artificial Intelligence for a Sustainable Industry 4.0.*, Springer, 2021; N.K. Ratha, J.H. Connell, R.M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems*, in *IBM Systems Journal*, 40.3/2001, 614 ss.; R. Ducato, *I dati biometrici*, in V. Cuffaro et al. (a cura di), *I dati personali del diritto europeo*, Torino, 2019; L. Cuomo, *Profili giuridici del trattamento biometrico dei dati*, in *Riv. it. med. leg.*, 1/2014, 43 ss.; S. Del Gatto, *Il riconoscimento facciale. A che punto siamo?*, in *Giorn. dir. amm.*, 5/2022, 692 ss.

¹⁷⁸ L'art. 9 GDPR prevede un divieto generale di trattamento, salvo alcune deroghe tassativamente previste. Rientrano nelle «categorie particolari» di dati personali, oltre i dati biometrici, i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

¹⁷⁹ Art. 4, par. 1, n. 14 GDPR.

¹⁸⁰ A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, cit., 2.

non poche criticità sul piano della tutela dei diritti fondamentali. Il rischio è già stato evidenziato nella proposta di revisione del Regolamento eIDAS¹⁸¹ e, in tempi meno recenti, dal Comitato consultivo della “Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale” (n. 108)¹⁸², unico strumento internazionale giuridicamente vincolante in materia di protezione dei dati.

L’espressione ‘dati biometrici’ è stata introdotta nella Convenzione solo a seguito del più recente protocollo di emendamento (c.d. Convenzione 108+)¹⁸³, volto ad aggiornare il precedente testo sia alle esigenze derivanti dallo sviluppo tecnologico, sia a coordinarlo con quadro europeo delineato dal GDPR¹⁸⁴.

La nozione è dunque approdata nell’ordinamento nazionale soltanto in tempi recenti: prima dell’entrata in vigore del Regolamento europeo sulla *privacy* non si ravvisava, infatti, una definizione puntuale¹⁸⁵.

Tuttavia, già con il Provvedimento del 28 settembre 2001 relativo all’installazione di sistemi di rilevazione cifrata presso istituti di credito, il Garante per la protezione dei dati personali aveva fissato regole di trattamento stringenti per garantire la tutela dei diritti fondamentali. In particolare, si vietava la ‘schedatura’ dei clienti mediante

¹⁸¹ Considerando 11: «I portafogli europei di identità digitale dovrebbero garantire il massimo livello di sicurezza per i dati personali utilizzati per l’autenticazione, indipendentemente dal fatto che tali dati siano conservati localmente o attraverso soluzioni basate sul *cloud*, tenendo conto dei diversi livelli di rischio. L’uso di dati biometrici per l’autenticazione è uno dei metodi di identificazione che offrono un elevato livello di sicurezza, in particolare se utilizzato in combinazione con altri elementi di autenticazione. Poiché i dati biometrici rappresentano una caratteristica unica di una persona, il loro utilizzo richiede misure organizzative e di sicurezza commisurate al rischio che il trattamento di tali dati può comportare per i diritti e le libertà delle persone fisiche, e conformi al regolamento (UE) 2016/679».

¹⁸² Convenzione adottata dal Consiglio d’Europa il 28 gennaio 1981 (c.d. Convenzione 108).

¹⁸³ Convenzione adottata dal Consiglio d’Europa il 18 maggio 2018. L’Italia ha ratificato la c.d. Convenzione 108+ con legge n. 60 del 22 aprile 2021 inerente la “Ratifica ed esecuzione del Protocollo di modifica alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale”.

¹⁸⁴ Art. 6 Convenzione 108+: «1. L’elaborazione di: dati genetici; dati a carattere personale relativi a reati, procedure e condanne penali e alle misure di sicurezza correlate; dati biometrici che identificano una persona in maniera univoca; dati a carattere personale che rivelano informazioni riguardanti l’origine razziale o etnica, le opinioni politiche, l’appartenenza sindacale, le convinzioni religiose o di altro tipo, la salute o la vita sessuale, è autorizzata soltanto a condizione che siano previste per legge garanzie adeguate a complemento di quelle della presente Convenzione. 2. Tali garanzie devono essere atte a prevenire i rischi che l’elaborazione di dati degni di particolare protezione può rappresentare per gli interessi, i diritti e le libertà fondamentali della persona interessata, in particolare il rischio di discriminazione.»

¹⁸⁵ Il dato biometrico rientrava nell’ambito della disciplina generale previsto per il dato personale e successivamente della disciplina a tutela del dato sensibile. Sul punto v. R. Ducato, *I dati biometrici*, cit., 1295.

rilevazione cifrata delle impronte digitali, prevedendo che l'accesso tramite sistemi biometrici fosse subordinato al consenso dell'interessato e accompagnato da modalità alternative di identificazione¹⁸⁶.

Un ulteriore intervento di rilievo è rappresentato dal “Provvedimento generale prescrittivo in tema di biometria” del 12 novembre 2014 e dalle allegate “Linee guida in materia di riconoscimento biometrico e firma grafometrica”, che forniscono congiuntamente un quadro unitario di misure tecniche, organizzative e procedurali per innalzare i livelli di sicurezza dei trattamenti biometrici e per conformarli alla disciplina prevista dal Codice *Privacy*.

Con il d.lgs. n. 101/2018, recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio”¹⁸⁷, il Legislatore nazionale ha introdotto l'art. 2-*septies* nel più risalente d.lgs. n. 196/2003. La disposizione ha previsto che il trattamento di dati biometrici – alla stregua di quelli genetici o di quelli relativi alla salute – è lecito solo se ricorre una delle condizioni di cui all'art. 9, par. 2 del GDPR e nel rispetto delle «misure di garanzia» periodicamente disposte dal Garante.

In ambito penale, invece, il d.lgs. n. 51/2018¹⁸⁸ – che include i dati biometrici tra le categorie di dati personali – impone per tali dati una consultazione preventiva del Garante, prima del relativo trattamento, riconoscendone l'elevato rischio per i diritti e le libertà degli interessati¹⁸⁹.

L'IA *Act*, riprendendo il quadro già delineato dal GDPR¹⁹⁰, qualifica i dati biometrici come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica,

¹⁸⁶ E. Cadamuro, *Le nuove sfide per la tutela dei dati biometrici nella costruzione dell'identità digitale*, cit., 378.

¹⁸⁷ Sul punto si rinvia a D. Provolo, *Il sistema sanzionatorio del novellato codice della privacy e la tutela penale patchwork dei dati genetici e dei dati biometrici*, in *Riv. trim. dir. pen. econ.*, 1-2/2019, 242 ss.

¹⁸⁸ D.lgs. 18 maggio 2018, n. 51, di attuazione della direttiva UE 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti in materia penale.

¹⁸⁹ Art. 24, co. 1, lett. b) d.lgs. 51/2018.

¹⁹⁰ Considerando 14 IA *Act*: «La nozione di «dati biometrici» utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del regolamento (UE) 2016/679, all'articolo 3, punto 18, del regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche».

quali le immagini facciali o i dati dattiloscopici»¹⁹¹. A monte, il Regolamento¹⁹² qualifica molte applicazioni biometriche come «sistemi ad alto rischio», giacché i dati biometrici rappresentano una categoria particolare di dati sensibili e il loro impiego è ammesso entro i limiti previsti dal pertinente diritto dell'Unione europea e dalle legislazioni nazionali¹⁹³.

Rientrano in tale categoria, in particolare, i sistemi di IA impiegati per la «categorizzazione biometrica»¹⁹⁴ basata su caratteristiche sensibili tutelate dall'art. 9, par. 1, GDPR, nonché i sistemi di «riconoscimento delle emozioni»¹⁹⁵. In questi casi, l'IA *Act* impone specifici obblighi di trasparenza, affinché gli

¹⁹¹ Art. 3, par. 34.

¹⁹² L'IA *Act* fornisce altresì la definizione di «identificazione biometrica» come «il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati» (art. 3, par. 35).

¹⁹³ F. Mollo, *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *federalismi.it*, 28/2024, 108.

¹⁹⁴ Considerando 16: «La nozione di «categorizzazione biometrica» di cui al presente regolamento dovrebbe essere definita come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale, il che significa che l'elemento non può, per ragioni tecniche oggettive, essere utilizzato senza il servizio principale e che l'integrazione di tale caratteristica o funzionalità non rappresenta un mezzo per eludere l'applicabilità delle norme del presente regolamento. Ad esempio, i filtri che classificano le caratteristiche facciali o del corpo utilizzate sui mercati *online* potrebbero costituire una tale caratteristica accessoria, in quanto possono essere utilizzati solo in relazione al servizio principale che consiste nel vendere un prodotto consentendo al consumatore di visualizzare in anteprima il prodotto su sé stesso e aiutarlo a prendere una decisione di acquisto. Anche i filtri utilizzati nei servizi di *social network online* che classificano le caratteristiche facciali o del corpo per consentire agli utenti di aggiungere o modificare immagini o video potrebbero essere considerati una caratteristica accessoria, in quanto tale filtro non può essere utilizzato senza il servizio principale dei servizi di social network consistente nella condivisione di contenuti *online*».

¹⁹⁵ Considerando 18: «La nozione di «sistema di riconoscimento delle emozioni» di cui al presente regolamento dovrebbe essere definita come un sistema di IA finalizzato a identificare o inferire emozioni o intenzioni di persone fisiche, sulla base dei loro dati biometrici. La nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. Non comprende stati fisici, quali dolore o affaticamento, compresi, ad esempio, ai sistemi utilizzati per rilevare lo stato di affaticamento dei piloti o dei conducenti professionisti al fine di prevenire gli incidenti. Non comprende neppure la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni. Tali espressioni possono essere espressioni facciali di base quali un aggrottamento delle sopracciglia o un sorriso, gesti quali il movimento di mani, braccia o testa, o caratteristiche della voce di una persona, ad esempio una voce alta o un sussurro».

interessati siano informati circa le modalità di funzionamento dei sistemi impiegati¹⁹⁶.

Il Regolamento vieta espressamente i sistemi di categorizzazione biometrica volta a dedurre caratteristiche sensibili quali origine razziale o etnica, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale od orientamento sessuale¹⁹⁷.

Un filtraggio di *dataset* fondato su dati biometrici resta consentito unicamente nell'ambito delle «attività di contrasto»¹⁹⁸ – riferite alle attività svolte da autorità competenti in materia di prevenzione, indagine, accertamento e perseguimento di reati, nonché esecuzione di sanzioni penali. Analogo divieto opera nei contesti lavorativi e scolastici per i sistemi di riconoscimento delle emozioni destinati a rilevare stati d'animo o intenzioni sulla base di dati biometrici. Restano escluse solo le applicazioni mediche o di sicurezza, ad esempio per il monitoraggio dell'affaticamento alla guida o nell'impiego di macchinari.

Sono inoltre vietate le attività di c.d. *scraping*¹⁹⁹, cioè l'estrazione massiva e non mirata di volti da *Internet* o da circuiti di videosorveglianza, al fine di creare o ampliare *database* di riconoscimento facciale²⁰⁰.

Tra le tecniche di identificazione biometrica passate in rassegna, la più intrusiva sotto il profilo dei diritti e delle libertà consiste nel riconoscimento biometrico remoto in tempo reale in spazi accessibili al pubblico²⁰¹, ossia, in luogo pubblico o

¹⁹⁶ Naturalmente resta escluso l'obbligo di trasparenza qualora tali tecniche siano autorizzate dalla legge per attività di accertamento e prevenzione di reati, nonché per realizzare attività di indagine.

¹⁹⁷ Art. 5, par. 1, lett. g).

¹⁹⁸ Art. 1, par. 45 nel definire «attività di contrasto» chiarisce che si tratta delle «attività svolte dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse».

¹⁹⁹ Art. 5, par. 1, lett. e).

²⁰⁰ Il Garante per la *privacy* italiano ha multato la società statunitense *Clearview AI* per aver realizzato un'estrazione massiva di immagini pubblicamente accessibili da *social network*, *blog* e siti *web* al fine di trasformarle in dati biometrici. Il Garante ha precisato che l'attività di *web scraping* svolta dalla società non è sovrapponibile a quella di un motore di ricerca generalista: il servizio fornisce, infatti, un vero e proprio strumento di identificazione biometrica operando un processo di datificazione dell'identità. Sul punto si veda l'ordinanza di ingiunzione nei confronti di *Clearview AI*, 10 febbraio 2022, n. 9751362; Corte di Giustizia, sent. 6 novembre 2003, causa C-101/01, par. 47; Garante europeo per la protezione dei dati, *EDPS Opinion on the possibility to use Clearview AI and similar services at Europol*, Case 2020-0372.

²⁰¹ Garante per la protezione dei dati personali, Sistema automatico di ricerca dell'identità di un volto, 26 luglio 2018, n. 9040256, sottolinea la differenza tra l'impiego di sistemi di IA da remoto – utilizzati dagli operatori di polizia per agevolare l'identificazione di un soggetto mediante ricerca automatizzata sotto costante supervisione umana – e l'impiego di sistemi di IA destinati

aperto al pubblico²⁰². Tale tecnologia, capace di identificare istantaneamente individui all'interno di flussi indeterminati di persone, incide marcatamente sulle prerogative democratiche²⁰³. Per tale ragione, l'*IA Act* ne ammette l'impiego soltanto in circostanze eccezionali e tassative²⁰⁴. Si fa riferimento ad attività di contrasto relative a determinate ipotesi di reato²⁰⁵, alla ricerca mirata di specifiche vittime di sottrazione, tratta o sfruttamento sessuale di esseri umani; alla localizzazione di persone scomparse e alla prevenzione di minacce terroristiche. In questi casi è richiesta un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o amministrativa indipendente, preceduta da una valutazione d'impatto sui diritti fondamentali e notificata all'autorità di vigilanza e a quella per la protezione dei dati²⁰⁶.

all'identificazione in tempo reale. Sul punto, v. E.C. Raffiotta, M. Baroni, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 382.

²⁰² Considerando 19.

²⁰³ Nel 2018 il Garante per la protezione dei dati personali ha espresso parere favorevole circa l'impiego del sistema SARI (Sistema Automatico di Riconoscimento Immagini) per la ricerca di un volto all'interno di una banca dati, qualificando tale riconoscimento biometrico come «mero ausilio all'agire umano». Ben diverso è stato l'orientamento assunto con riferimento a SARI *Real Time*: secondo l'Autorità, il monitoraggio in tempo reale dei volti non dispone di una base giuridica idonea a giustificare la «forte interferenza con la vita privata» che un simile trattamento comporterebbe. Il sistema, infatti, realizzerebbe un trattamento automatizzato su larga scala in grado di riguardare «anche coloro che siano presenti a manifestazioni politiche e sociali», dunque potenzialmente rivelatore di dati, quali convinzioni politico-sindacali e religiose, sensibili (v. Garante per la protezione dei dati personali, Parere sul sistema SARI *Real Time*, 25 marzo 2021, n. 9575877).

²⁰⁴ La Corte EDU ha precisato che in una società democratica il riconoscimento facciale a distanza in tempo reale per essere considerato «necessario» richiede un alto livello di giustificazione (Corte EDU, 4 luglio 2023, *Glukhin c. Russia*), deve essere fondato su un'idonea base giuridica, deve essere motivato e proporzionato. Sul punto v. C. Nardocci, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU "Glukhin c. Russia"*, in *BioLaw Journal - Rivista di BioDiritto*, 1/2024, 279 ss. e G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso "Glukhin c. Russia"*, in *DPCE online*, 1/2024, 695 ss.

²⁰⁵ L'art. 5 rinvia all'allegato II, che elenca sedici ipotesi di reato: terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e pornografia minorile; traffico illecito di stupefacenti o sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario; lesioni gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive; sequestro, detenzione illegale e presa di ostaggi; reati che rientrano nella competenza giurisdizionale della Corte penale internazionale; illecita cattura di aeromobile o nave; violenza sessuale; reati ambientali; rapina organizzata o a mano armata; sabotaggio; partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

²⁰⁶ Nei casi di urgenza, debitamente giustificati, l'impiego dell'identificazione biometrica da remoto in tempo reale è consentito a condizione che entro 24 ore venga richiesta l'autorizzazione. Se l'autorizzazione viene rifiutata, l'uso dei sistemi di identificazione biometrica in tempo reale collegati a tale autorizzazione deve essere interrotto immediatamente e tutti i dati e gli output raccolti vanno cancellati (art. 5, par. 3).

Il medesimo equilibrio tra innovazione e tutela si scorgerebbe nel nuovo Regolamento eIDAS 2 che, come già approfondito, testimonia l'intenzione di un cambiamento di paradigma per l'identità digitale in Europa. Le nuove norme saranno operative dal 2026 e, potenzialmente, assicureranno ad ogni cittadino e impresa in possesso di un portafoglio europeo di identità digitale, un'identificazione e un'autenticazione sicure e affidabili per l'accesso ai servizi pubblici e privati in tutta l'Unione.

Nei lavori preliminari al progetto è emersa – al fine di garantire *standard* elevati di sicurezza e affidabilità – la necessità di rendere obbligatoria per gli Stati membri la previsione di un meccanismo di autenticazione biometrica nella realizzazione di questi sistemi. Sebbene il testo definitivo non contenga un obbligo espresso, la progettazione del *wallet* europeo contempla moduli biometrici per elevare il livello di garanzia. Ciò rende imprescindibili adeguati presidi di cybersicurezza, soprattutto alla luce delle minacce segnalate da ENISA ed Europol, che evidenziano l'uso di *deepfake* sempre più sofisticati, capaci di falsificare tratti biometrici e favorire furti d'identità o frodi patrimoniali²⁰⁷.

In conclusione, i dati biometrici costituiscono il presente e il futuro dei sistemi di identità digitale. Tuttavia, la loro estrinseca natura sensibile richiede un quadro normativo e tecnico rigoroso, idoneo a mitigare i rischi di discriminazioni, sorveglianza e abusi.

1.3. La blockchain e le Distributed Ledger Technologies

Se l'intelligenza artificiale e la biometria rappresentano oggi le tecnologie più avanzate nel campo dell'identificazione digitale, la *blockchain* e, più in generale, le *Distributed Ledger Technologies* (DLT) mirano a ridefinire in modo stesso in cui l'identità e i dati personali vengono gestiti e garantiti.

²⁰⁷ Un esempio significativo di tale minaccia è rappresentato dal *trojan* “*GoldPickaxe*”, un *malware* progettato per colpire i sistemi operativi dei dispositivi mobili. Esso utilizza i dati biometrici delle vittime, insieme ad altri dati identificativi, per generare video *deepfake* successivamente impiegati dagli operatori del *malware* per autenticare transazioni finanziarie fraudolente. L'attacco avviene mediante messaggi di *phishing* che simulano comunicazioni ufficiali provenienti da enti governativi, richiedendo la creazione di un profilo biometrico facciale completo e la scansione del documento di identità.

La tecnologia *blockchain*²⁰⁸, descritta da alcuni studiosi come “macchina della verità”²⁰⁹, affonda le proprie radici nel *white paper* “*Bitcoin: A Peer-to-Peer Electronic Cash System*”²¹⁰, pubblicato nel 2008 sotto lo pseudonimo di Satoshi Nakamoto. Tale progetto si sviluppa sulla base di un’ideologia maturata già negli anni Ottanta dello scorso secolo: attivisti matematici auspicavano un’infrastruttura capace di raggiungere un consenso comune senza un’autorità deputata alla raccolta delle informazioni.

L’obiettivo era dunque quello di individuare un meccanismo capace di coordinare azioni individuali, in assenza di un corpo centrale, garantendo al contempo l’integrità dei dati contro tentativi di manipolazione²¹¹.

Si riteneva che solo una moneta elettronica anonima, basata su robuste tecniche crittografiche, avrebbe potuto garantire scambi sicuri (sistemi di messaggistica sicuri, contratti digitali ecc.). Dunque, in tale solco, Nakamoto combinò tecnologie già esistenti in campo informatico e realizzò un registro digitale distribuito²¹² al fine di eliminare l’intermediario nella convalida delle transazioni di “moneta elettronica”²¹³.

²⁰⁸ Per una panoramica generale sull’argomento si rinvia a M.J. Casey, P. Vigna, *La macchina della verità. La blockchain e il futuro di ogni cosa*, Milano 2018; A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 12 marzo 2015; A. Borg, *Prefazione*, A. Basile (a cura di), *Blockchain la nuova rivoluzione industriale*, Palermo, 2019; K. Law, E. Mik, *Pause the blockchain legal revolution*, in *International and Comparative Law Quarterly*, 69/2020, 135 ss.; F. Sarzana di S. Ippolito, M. Nicotra, *Diritto alla blockchain, intelligenza artificiale e IoT*, Milano, 2018; A. Fiorelli, A.R. Cassano, *La rivoluzione tecnologica della blockchain*, in G. Cassano, S. Previti (a cura di), *Il diritto di Internet nell’era digitale*, cit., 253 ss.; M. Chierici, *La “blockchain”: una lettura giuridica per uno sguardo verso il futuro*, in *Cyberspazio e diritto*, 3/2018, 385 ss.

²⁰⁹ L’espressione è di M.J. Casey, P. Vigna, *La macchina della verità*, cit.

²¹⁰ S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, reperibile su <https://bitcoin.org/bitcoin.pdf>.

²¹¹ Il movimento di attivisti è noto come movimento “*Cypherpunk*”. Le ideologie alla base del movimento sono state racchiuse da Eric Hughes nel *Cypherpunk Manifesto* (E. Hughes, *A Cypherpunk’s Manifesto*, 9 marzo 1993). Tali ideologie presero vita nel 1994 con DigiCash, un sistema di pagamento virtuale creato dal matematico David Chaum per scambiare denaro in modo affidabile su *Internet* in assenza di intermediari. Anni dopo Nick Szabo, collaboratore di Chaum, pubblicò uno scritto dal titolo “*The God Protocols*” nel quale sviluppava alcuni concetti poi ripresi da Nakamoto. Quest’ultimo riuscì a superare gli ostacoli che avevano impedito il corretto funzionamento di un sistema di pagamento decentralizzato.

²¹² La *blockchain* può definirsi come la forma più avanzata di registro distribuito (*Distributed Ledger Technology* o DLT), ponendosi come *species* all’interno del *genus* di questi ultimi. Per uno studio specifico sulla tecnologia DLT si rimanda a R. Maull *et al.*, *Distributed ledger technology: Applications and implications*, in *Strategic Changes*, 26/2017, 481.

²¹³ Ci si riferisce al *Bitcoin*, la prima e più nota criptovaluta. Sull’argomento si rinvia a S. Copaccioli, *Criptovalute e Bitcoin: un’analisi giuridica*, Milano, 2015; D. Capoti, E. Colacchi, M. Maggioni, *Bitcoin Revolution: la moneta digitale alla conquista del mondo*, Milano, 2015; N. Vardi,

Dal punto di vista tecnico, la *blockchain* può essere descritta come un registro visibile a tutti e imm modificabile in cui la fiducia nell'intermediario è sostituita da prove matematiche, delineando un ecosistema nato in ambito finanziario ma estendibile a svariate applicazioni, dal diritto pubblico²¹⁴ alla gestione dell'identità digitale.

La cifratura a doppia chiave asimmetrica²¹⁵ e le 'impronte' di *hash*²¹⁶ garantiscono l'integrità e la paternità delle operazioni compiute all'interno del sistema²¹⁷. La

"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin, in *Dir. inform.*, 3/2015, 443; G. Gasparri, *Timidi tentativi giuridici di una messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*, in *Dir. inform.*, 3/2015, 415.

²¹⁴ Sui possibili utilizzi della tecnologia *blockchain* nell'ambito della pubblica amministrazione si vedano, tra gli altri, P. Rubecchini, *Tecnologia blockchain e fiducia amministrativa*, Napoli, 2023; Id., *Blockchain e pubblica amministrazione italiana: i primi passi di un cammino ancora lungo*, in *Giorn. dir. amm.*, 3/2021, 298 ss.; G. Gallone, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Dir. ec.*, 3/2019, 187 ss.; M. Macchia, *Blockchain e pubblica amministrazione*, in *federalismi.it*, 2/2021, 117 ss.; Id., *Blockchain and Public Authorities: a Field Yet to Be Explored*, in *Erdal*, 2/2021, 19 ss.; F. Votta, *L'amministrazione pubblica e la tecnologia "blockchain"*, in *Giorn. dir. amm.*, 4/2022, 450 ss.; S. Caldarelli, *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, in *Dir. inform.*, 4/2020, 857 ss.; M. Ippolito, *La disintermediazione dei processi nella pubblica amministrazione: l'impatto della tecnologia "blockchain"*, in *ambientediritto.it*, 2/2021, 36 ss.; M. Matassa, *Blockchain e pubblica amministrazione: stato dell'arte e prospettive*, in *IdF*, 3/2021, 803 ss. Tra i contributi che hanno affrontato l'argomento con un taglio più specifico rimanda invece a G. D'Acquisto, *Blockchain e GDPR: verso un approccio basato sul rischio*, in *federalismi.it*, 2/2021, 53 ss.; M. Farina, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?*, in *federalismi.it*, 21/2020, 170 ss.; M. Verzaro, *La blockchain e il fabbisogno di personale nella pubblica amministrazione*, in *federalismi.it*, 2/2021, 195 ss.; F. Faini, *Il diritto nella tecnica*, cit., 79 ss.; G. Gallone, *"Blockchain" e "Big data" nel settore pubblico: spunti in tema di G.D.P.R. "compliance"*, in *federalismi.it*, 14/2022, 66 ss.; G. Lo Sapio, *Il tormentato rapporto tra "blockchain" e pubblica amministrazione nel prisma dei contratti pubblici*, in *federalismi.it*, 26/2023, 112 ss.; G. Gometz, M. Tawa Folarin, *Voto elettronico presidiato e blockchain*, in *Ragion pratica*, 2/2018, 317 ss.; M. Marchesi, *Blockchain pubbliche e permissioned: una questione di fiducia*, in *federalismi.it*, 2/2021, 140 ss.; I. Francucci, *Trasparenza, blockchain e gestione dei rifiuti*, in *Dir. amm.*, 1/2024, 273 ss.; L. Manfredi, *Progetto Pilota per la realizzazione, su Blockchain, del Fascicolo Sanitario Elettronico con il coinvolgimento dei Fondi Sanitari Integrativi nel flusso di dati*, in *federalismi.it*, 21/2023, 226 ss.; F. Faini, *Blockchain e diritto. La «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e previdenza*, 1/2020, 297 ss.

²¹⁵ La cifratura a doppia chiave asimmetrica è stata individuata dal Legislatore italiano quale tecnologia alla base della firma digitale già nel D.P.R. 10 novembre 1997, n. 513. Per una puntuale analisi sulla tecnologia si rinvia a A.G. Orofino, *Firme elettroniche e procedimenti amministrativi*, Bari, 2008, 83 ss.

²¹⁶ «La funzione di hash consente di ridurre in maniera univoca in insieme di bit in una stringa alfanumerica, univocamente riconducibile al contenuto originario, fornendo una sorta di "impronta digitale". Mentre non è possibile risalire al contenuto originario della stringa al risultato della funzione, eventuali modifiche di tale contenuto possono essere rilevate in quanto l'applicazione della funzione sul nuovo contenuto porterà la creazione di una stringa diversa», così F. Sarzana Di S. Ippolito, M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, cit., 13.

²¹⁷ Così M. Matassa, *Blockchain e pubblica amministrazione*, cit., 808.

prima tecnologia consente all'utente di impiegare una coppia di chiavi (pubblica/privata) per provare origine, paternità e immodificabilità dell'operazione. La transazione, unitamente a tutte quelle generate in un dato intervallo di tempo, confluisce in un "blocco": quest'ultimo, prima di essere aggiunto alla catena, è sintetizzato in un'impronta di *hash*. Poiché ciascun blocco contiene l'*hash* del precedente, l'intera sequenza diventa cronologicamente ricostruibile e virtualmente incorruttibile.

Un ulteriore tratto distintivo risiede nell'architettura *peer-to-peer* della *blockchain* in cui gli utenti operano come nodi del sistema fungendo simultaneamente da *client* (fruitore) e *server* (distributore). In tal modo ciascun partecipante può leggere e scaricare i dati custoditi dagli altri nodi, rendendo irrilevante l'attacco a un singolo punto della rete, in quanto nessuna copia isolata è essenziale per la continuità del sistema.

Il consenso si forma attraverso il principio della *proof of work*²¹⁸ che richiede la risoluzione di un problema computazionale: l'impegno di risorse *hardware* rende antieconomica la frode e incentiva i partecipanti a comportamenti onesti.

Il risultato è un *database* aggiornato, gestito e coordinato in assenza di un centro, dove ogni blocco validato diventa definitivo e la sua eventuale modifica richiede, di fatto, un nuovo consenso collettivo.

Da qui si ravvisa la peculiarità evidenziata dal Ministero dello Sviluppo Economico come principale valore della *blockchain*: la drastica riduzione del 'costo della fiducia', ossia dei presidi organizzativi tradizionalmente necessari a garantire l'esecuzione certa di uno scambio informativo o di valore²¹⁹.

L'affidabilità dell'operazione, infatti, deriva dalle regole crittografiche del protocollo e non da un'autorità centrale. Pertanto, la regolazione della *blockchain*

²¹⁸ Il principio della *proof of work* è stato teorizzato da Hal Finney nel 2004 come meccanismo di creazione del consenso; tale tecnologia richiede che determinati *computer* del *network* (generalmente identificati come "miners") utilizzino la loro potenza computazionale per risolvere quesiti matematici e che gli altri, una volta risolto il quesito, verifichino che la soluzione non corrisponda a una transazione precedente. Per incentivare i *miners* a utilizzare la loro potenza computazionale a beneficio della rete è previsto un premio in criptovalute a beneficio dei nodi che hanno risolto il problema matematico. Per un maggiore approfondimento della questione si rinvia a J. Bonneau, A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten, *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, in *IEEE Symposium on Security and Privacy*, 2015, 104.

²¹⁹ MISE, *Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain. Sintesi per la consultazione pubblica*, 2019, 3.

richiede senz'altro un approccio differente dagli schemi tradizionali: la natura distribuita del registro ridisegna la concezione di fiducia e la responsabilità giuridica.

La tecnologia in questione costituirebbe un'evidente rivoluzione nel campo dell'identità digitale. I tratti distintivi della *blockchain*, quali la decentralizzazione dell'autorità e l'immutabilità provabile dei dati, ridefinirebbero i tradizionali presidi giuridici di autenticità, integrità e prova documentale. Verrebbe meno la custodia unilaterale da parte dell'ente pubblico delle informazioni personali, che lascerebbe il passo ad una co gestione del cittadino, con verifica istantanea dell'attributo.

Non a caso il Regolamento eIDAS 2 punta in questa direzione, prefigurando un portafoglio europeo d'identità digitale in cui lo Stato resta garante della veridicità dell'attributo, ma non più esclusivo detentore del dato²²⁰.

Tuttavia, la potenziale redistribuzione della fiducia solleva delicate questioni regolatorie. Alcuni aspetti della tecnologia entrano in tensione con i principi enucleati dal GDPR, come il principio di minimizzazione dei dati²²¹, il principio di limitazione della conservazione dei dati²²² e il diritto alla cancellazione degli stessi²²³.

Inoltre, restituire il controllo delle credenziali al cittadino è virtuoso solo se accompagnato da robuste politiche di alfabetizzazione digitale e da servizi di

²²⁰ L'Unione europea è stata tra le prime istituzioni a investire sugli sviluppi della *blockchain*, affrontando il fenomeno attraverso la *Risoluzione del Parlamento europeo* del 26 maggio 2016. Inoltre, è stato creato altresì un Osservatorio (*UE Blockchain Observatory & Forum*) e una *partnership* tra Stati con l'obiettivo di creare un'infrastruttura europea di servizi *blockchain* (*European Blockchain Partnership*).

²²¹ Art. 5, par. 1, lett. c) GDPR: «I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati».

²²² Art. 5, par. 1, lett. e) GDPR: «I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato».

²²³ Cfr. art. 17 GDPR, noto come "diritto all'oblio" che riconosce all'interessato la possibilità di ottenere dal titolare del trattamento la rimozione dei propri dati quando essi non siano più necessari rispetto alle finalità per le quali sono stati raccolti, sia stato revocato il consenso o il trattamento risulti illecito. Introdotto per rafforzare il controllo dell'individuo sui propri dati, in linea con l'art. 8 della Carta dei diritti fondamentali dell'Unione europea e con la giurisprudenza della Corte di giustizia, tale diritto è tuttavia soggetto a bilanciamento, potendo essere escluso in presenza di esigenze prevalenti, quali l'esercizio della libertà di espressione e d'informazione, l'adempimento di obblighi legali o motivi di interesse pubblico riconosciuti (art. 17, par. 3, GDPR).

custodia delegata sicura. Diversamente, l'asimmetria informativa rischia di spostarsi dall'amministrazione all'utente.

In definitiva, la *blockchain* – nata nel perimetro finanziario ma presto eletta a «futuro di ogni cosa»²²⁴ – offre l'infrastruttura per un'identità digitale “*Self-Sovereign*”. Purché, però, l'innovazione non si traduca in nuove vulnerabilità, è necessario un paradigma regolatorio che combini sperimentazione guidata, responsabilità multilivello e tutela effettiva dei diritti dell'interessato.

2. Identità digitale, profilazione e sorveglianza

Nell'ecosistema digitale contemporaneo l'identità non si limita più a certificare “chi siamo”, ma si manifesta come flusso continuo di tracce – biometriche, comportamentali, contestuali – che le nuove frontiere tecnologiche catturano, raccolgono e combinano in tempo reale.

Algoritmi di *machine learning* trasformano *click*, spostamenti e interazioni in profili capaci di anticipare preferenze, propensioni al rischio e persino stati emotivi, mentre le infrastrutture biometriche segnano il passaggio dall'autenticazione statica alla riconoscibilità permanente²²⁵.

L'intreccio tra identità digitale, profilazione e sorveglianza costituisce oggi uno dei nodi più critici dell’“infosfera”²²⁶: come visto, alla progressiva smaterializzazione delle credenziali personali, corrisponde un'espansione altrettanto rapida delle pratiche di tracciamento, classificazione ed estrazione di valore dai dati che tali credenziali generano o rendono accessibili.

Muovendo dalla consapevolezza che ogni interazione in rete lasci un'impronta informativa suscettibile di essere riassemblata in profili dettagliati, il mercato ha elaborato modelli di *business* fondati sull'osservazione sistematica dei comportamenti e sull'inferenza in tempo reale di preferenze e propensioni.

²²⁴ L'espressione è tratta da M.J. Casey, P. Vigna, *La macchina della verità*, cit.

²²⁵ Senza pretese di esaustività, sull'impatto degli algoritmi sul modello sociale contemporaneo si vedano, tra gli altri, H. Fry, *Hello World. Essere umani nell'era delle macchine*, nella traduzione di A. Migliori, Torino, 2018; B. Kaiser, *La dittatura dei dati*, Milano, 2019; S. Zuboff, *Il capitalismo della sorveglianza*, cit.; P. Dourish, *Algorithms and their others: Algorithmic culture in context*, in *Big Data & Society*, 2/2016, 3 ss.

²²⁶ Cfr. L. Floridi, *La quarta rivoluzione*, cit.; Id. *The Onlife Manifesto*, cit.

Parallelamente, le autorità pubbliche – spinte da esigenze di sicurezza, controllo dei flussi e razionalizzazione dei servizi – hanno progressivamente integrato strumenti di analisi predittiva e riconoscimento biometrico nei rispettivi apparati.

In questo contesto, l'identità digitale non è più soltanto un dispositivo di autenticazione per l'accesso ai servizi, ma diventa la chiave d'ingresso a un ecosistema di dati relazionali, comportamentali e biometrici che, una volta acquisiti, alimentano cicli costanti di profilazione.

La stessa architettura *Internet*, concepita in origine come spazio neutrale di scambio, si è progressivamente trasformata in un'infrastruttura di sorveglianza diffusa, nella quale sensori, piattaforme e *data broker* cooperano alla raccolta e all'elaborazione di informazioni su scala globale.

Ne discende, per l'ordinamento, non soltanto il compito di garantire i presidi fondamentali delle interazioni digitali, ma anche la necessità di affrontare questioni inedite – opacità algoritmica, asimmetrie informative, pratiche di manipolazione comportamentale – che i modelli regolatori tradizionali faticano a inquadrare²²⁷.

Il quadro normativo europeo – dal GDPR all'*IA Act*, fino al Regolamento eIDAS 2 – nel recepire le istanze di cambiamento, sta tentando di riannodare i fili di questa nuova cittadinanza.

Su queste premesse, il paragrafo approfondisce come le tecnologie emergenti, su tutte il riconoscimento biometrico, abbiano inciso nelle dinamiche di sorveglianza alimentando un 'capitalismo' di dati in cui la profilazione diviene l'infrastruttura economica di base.

Seguirà un confronto circa le principali strategie di *Internet governance* (modello californiano, cinese ed europeo), per mostrare come ciascuna attribuisca all'identità digitale uno statuto giuridico differente e, di conseguenza, prefiguri differenti assetti di responsabilità, tutele e poteri di controllo.

2.1. Tra sorveglianza e 'capitalismo'

²²⁷ Cfr. A. Pirni, A. Carnavale, *The challenge of regulating emerging technologies. A philosophical framework*, in E. Palmerini, E. Stradella (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, 2013.

Il ricorso alle tecnologie emergenti, in particolare ai sistemi di riconoscimento facciale, ha favorito forme di sorveglianza più diffuse e pervasive rispetto a qualunque altra tecnologia finora disponibile²²⁸.

Per ‘sorveglianza’ si intende, in senso ampio, la «raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono»²²⁹. Tale pratica, nei suoi più pericolosi impieghi, può rivelarsi lesiva dei diritti fondamentali, in quanto capace di imporre limiti e controlli.

Le riflessioni sociologiche contemporanee mostrano come non sia più adeguata l’immagine del controllo potenzialmente costante, visibile e inverificabile²³⁰ incarnata dal modello di carcere panottico di Jeremy Bentham²³¹. In tale modello una singola guardia, collocata al centro di una struttura circolare, poteva sorvegliare assiduamente i detenuti passivi e inconsapevoli.

Le tecnologie digitali, tuttavia, attraverso algoritmi, *Internet* e *big data*, consentono di praticare una sorveglianza che va ben oltre le aspirazioni di questo modello²³².

Il superamento dell’idea di un controllo esercitato da un singolo soggetto posto staticamente al centro dell’ipotetica prigione, lascia spazio a una raccolta massiva

²²⁸ Si vedano, *ex multis*, G. Mobilio, *Tecnologie di riconoscimento facciale*, cit.; K.A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York, 2011; E. Learned-Miller *et al.*, *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020; M. Hu, *Biometric surveillance and big data governance*, in D. Gray, S.E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge, 2017.

²²⁹ D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002, 2. Sul tema si rinvia a Z. Bauman, D. Lyon, *La sorveglianza nella modernità liquida*, Roma-Bari, 2015; G. Ziccardi, *Controllo, sorveglianza e segreto: una prospettiva informatico-giuridica*, in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, vol. III, Milano, 2019, 3 ss.; P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020; M. Galič, T. Timan, B.J., Koops, *Bentham, Deleuze and Beyond: an Overview of Surveillance Theories from the Panopticon to Participation*, in *Philosophy & Technology*, 30/1, 2017, 10 ss.

²³⁰ Così G. Mobilio, *Tecnologie di riconoscimento facciale*, Napoli, 2021, 13.

²³¹ J. Bentham, *Panopticon ovvero la casa d’ispezione*, Venezia, 1983, 1997. Quello immaginato da Bentham è un modello architettonico di carcere strutturato in maniera circolare, in cui i detenuti sono disposti alla periferia, tutti visibili da un unico osservatore (ispettore) collocato in una torre di controllo al centro. Da questa posizione, l’osservatore può monitorare i detenuti senza che essi possano sapere se l’ispettore sia davvero presente o li stia osservando, essendo nascosto dietro a persiane che permettono di vedere ma non di essere visto. Come messo in luce da M. Foucault, *Sorvegliare e punire. Nascita della prigione*, Torino, 1993, 218 ss., l’asimmetria cognitiva tra sorvegliante e sorvegliato è cruciale: il primo garantisce la perfetta disciplina e il «funzionamento automatico del potere» anche senza esercitare una sorveglianza continua, mentre il secondo «è visto ma non vede; oggetto di informazioni, mai soggetto di una comunicazione».

²³² G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 13.

di informazioni su larga scala e alla disponibilità di tecniche capaci di analizzare e rielaborare i dati raccolti²³³. Le nuove forme di sorveglianza non sono più esclusiva prerogativa di soggetti pubblici – né si esauriscono nella figura orwelliana del “Grande Fratello che ti osserva”²³⁴ – ma vengono attuate anche, e sempre più spesso, da soggetti e imprese private.

Ne deriva uno scenario caratterizzato da molteplici osservatori e sorvegliati, attraverso una pluralità di attori. In tale contesto, ciò che rende peculiare questa nuova forma di sorveglianza è il ruolo attivo che gli individui stessi assumono nel processo di monitoraggio. Gli utenti, attraverso le piattaforme digitali, partecipano quotidianamente alla propria sorveglianza, spesso consapevolmente ma talvolta anche in modo inconsapevole.

Si instaura così una dinamica dialettica tra sorveglianti e sorvegliati, nella quale gli utenti sono al contempo “oggetti” che forniscono contenuti e “soggetti” che generano nuove forme di sorveglianza²³⁵.

Attraverso le informazioni e i contenuti generati dalle attività quotidiane *online* – *click*, messaggi, condivisioni di foto – i gesti individuali diventano fonte di dati continuamente monitorati da una vasta gamma di attori (governi, aziende private, fino agli utenti stessi dei *social network*). Tali flussi informativi rappresentano oggi una risorsa economica strategica, oggetto di desiderio per fini commerciali e di controllo soprattutto da parte delle c.d. *Big Tech*²³⁶.

Si tratta di colossi del *web* che oggi esercitano un potere effettivo di sorveglianza, ponendosi al centro di un nuovo paradigma economico definito dalla dottrina “capitalismo della sorveglianza”²³⁷.

²³³ P. Tincani, *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 2/2018, 61 ss.

²³⁴ Il richiamo va al noto G. Orwell, 1984, Milano, 1950.

²³⁵ G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 15.

²³⁶ Cfr. R. Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That's Progress*, in *Vox*, 11 giugno 2020; M. Kwet, *The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud*, in *The Intercept*, 14 luglio 2020.

²³⁷ L'espressione richiama la nota elaborazione di S. Zuboff, *Il capitalismo della sorveglianza*, cit. che per primo ha inquadrato e approfondito il tema del ‘capitalismo della sorveglianza’ come nuova risorsa economica. Più in generale, e anche sotto una diversa prospettiva, si rimanda allo studio dei più rilevanti contributi in tema di *big data*. Con riferimento alla letteratura internazionale si vedano, *ex multis*, V. Mayer-Schönberger, K. Cuckier, *Big data: A revolution that will transform how we live, work and think*, Houghton Mifflin Harcourt, Boston-New York, 2013; R. Kitchin, *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, Sage, Los Angeles, 2014. Con riferimento al dibattito italiano, invece, si rimanda tra gli altri a F. Faini, *Data Society*,

Questo contesto è aggravato ulteriormente dalla ‘collaborazione’ tra sorveglianza privata e sorveglianza statale. Le forze dell’ordine, in particolare, si rivolgono sempre più spesso a intermediari privati, o direttamente alle grandi piattaforme del *web*, per ottenere la disponibilità di tecnologie, immagini e dati personali²³⁸. Un caso emblematico è quello del programma PRISM²³⁹, rivelato da Edward Snowden nel 2013²⁴⁰, che ha mostrato la collaborazione talvolta volontaria, talvolta coatta, delle principali piattaforme digitali con i servizi di *intelligence* statunitensi nella raccolta sistematica dei dati degli utenti a livello globale²⁴¹.

Alla luce di tali dinamiche, la questione non riguarda più soltanto la sorveglianza in senso ‘orwelliano’, intesa come controllo sociale costante e inibitoria incarnata dalla figura del ‘Grande Fratello’. Piuttosto, richiamando la metafora kafkiana²⁴², il problema odierno è quello di un potere invisibile e incomprensibile²⁴³, capace di

cit.; A. Mantellero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.*, 1, 2012, 135-144; M. Orefice, *I big data. Regole e concorrenza*, in *Politica del diritto*, 4, 2016, 697-744; D. Cardon, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Milano, 2016 e G. Mazzei, *Big data come beni comuni globali e principi in tema di public utilities*, in *federalismi.it*, 12, 162-184, 2023.

²³⁸ Si rammenta, nuovamente, il caso relativo alla *start-up* americana *Clearview AI* che ha sviluppato un sistema di riconoscimento facciale in grado di identificare una persona attraverso il confronto non limitato alle foto segnaletica disponibili alle forze di polizia o alle foto degli archivi delle motorizzazioni civili, ma altresì attraverso le immagini presenti su *internet*, compresi i *social network*. Per un approfondimento si rinvia a I. Neroni Rezende, *Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective*, in *New Journal of European Criminal Law*, 3/2020, 375 ss.

²³⁹ Il programma PRISM è un sistema di intercettazione gestito dalla *National Security Agency* (NSA) in base alla sezione 702 del *Foreign Intelligence Surveillance Act Amendments Act* del 2008. Attivo dal 2007, il programma consentiva all’*intelligence* statunitense di ottenere, tramite ordini segreti emessi dal tribunale FISC, l’accesso diretto ai *server* di principali *provider* (fra cui Microsoft, Google, Facebook, Apple, Yahoo!) per acquisire in modo pressoché illimitato contenuti di *e-mail*, file archiviati e metadati di utenti non statunitensi. L’esistenza di PRISM è stata rivelata da Edward Snowden nel giugno 2013 attraverso documenti riservati pubblicati dal *Guardian* e dal *Washington Post*. Si rinvia a G. Greenwald, *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Milano, 2014; G. Suffia, *La “società liquida” e il caso Snowden*, in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, cit., 23 ss.

²⁴⁰ V. Bay M., *What is Cybersecurity? In search of an encompassing definition for the post-Snowden era*, in *French journal for media research*, 6/2016, 1-28.

²⁴¹ Lo scandalo *Datagate* nasce dalle rivelazioni Edward Snowden, ex analista della *National Security Agency* degli Stati Uniti, ha svelato come a seguito degli attentati terroristici dell’11 settembre 2001, l’Agenzia abbia praticato un regime di sorveglianza indiscriminato e continuativo, accedendo ai metadati riguardanti il traffico telefonico all’interno degli USA e tra questi e l’estero. Sull’argomento si rinvia a P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, cit., 100 ss.; S. Sica, G. Giannone Codiglione, *La libertà fragile. Pubblico e privato al tempo della rete*, Napoli, 2014, 25 ss.; G. Greenwald, *No place to hide*, cit.

²⁴² F. Kafka, *Il processo*, Milano, 1984.

²⁴³ G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 21.

raccogliere informazioni su ogni individuo, elaborare profili personali e assumere decisioni automatizzate senza fornire spiegazioni o possibilità di partecipazione. Diviene dunque essenziale, anche sul piano giuridico e politico, «definire le condizioni necessarie per evitare che la società della sorveglianza si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca una ulteriore legittimazione proprio nella tecnologia»²⁴⁴.

2.2. Lo stato dell'arte dell'Internet governance e la 'terza via' europea

Le dinamiche di sorveglianza e sfruttamento dei dati descritte, riflettono modelli differenti di governo della rete e dell'informazione. Ogni forma di controllo o libertà digitale cela, infatti, una precisa filosofia di *Internet governance*, che traduce in regole giuridiche e infrastrutturali le scelte politiche di ciascun ordinamento.

È su questo terreno che – nell'ultimo ventennio – sono emerse nel panorama contemporaneo due visioni antitetiche di *governance* della rete.

Il 'modello californiano', nato nell'ecosistema della *Silicon Valley*, si basa su un'impostazione *multi-stakeholder* orizzontale che affida il controllo della rete a governi, organizzazioni internazionali, settore privato, della ricerca e anche a singoli individui²⁴⁵. In questo modello lo Stato si limita a promuovere l'innovazione e a finanziare l'infrastruttura, ma si astiene dall'imporre restrizioni arbitrarie alla libera circolazione delle informazioni²⁴⁶. Non è un caso, infatti, se il sistema è definito da alcuni come "il selvaggio west", in cui il ruolo dello Stato si riduce più a un *non facere* più che in un *facere*.

²⁴⁴ S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, 165.

²⁴⁵ W. Kleinwächter, *The Power of Ideas: Internet Governance in a Global Multi Stakeholder Environment*, Marketing für Deutschland, Berlino, 2007; W. Drake, E. Wilson, *Multistakeholderism, Civil Society and Global Diplomacy: The Case of the World Summit on the Information Society*, in W. Drake, E. Wilson (eds.), *Governing Global Electronic Networks: International Perspectives on Policy and Power*, MIT Press, Cambridge (MA), 2008, 539-582; M. Mueller, *Networks and States. The global Politics of Internet Governance*, MIT Press, Cambridge (MA), 2010.

²⁴⁶ Presidenza degli Stati Uniti d'America, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, 2011, 21, reperibile su https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Sul versante dell'identità digitale, tale impostazione tende a delegarne la definizione e la custodia alle *Big Tech*: credenziali di accesso e profili degli utenti vengono trattati come *asset* aziendali, scambiati per pubblicità comportamentale e analisi predittiva. L'individuo, se pur formalmente sovrano dei propri dati, finisce col percepire l'identità *online* come un *login* da offrire in cambio di servizi gratuiti. All'estremo opposto si colloca il 'modello cinese', sostenuto, seppur con le dovute distinzioni, anche da diversi altri Paesi, tra cui la Russia²⁴⁷. Tale impostazione giustifica un controllo statale intenso e pervasivo sulla rete e sui suoi utenti al fine di perseguire 'politiche di sicurezza', implementato tramite il '*Great Firewall*'²⁴⁸ e un complesso sistema di sorveglianza algoritmica. Questo paradigma richiama l'idea del già menzionato *Panopticon* benthamiano (o, più banalmente, del grande occhio orwelliano): la censura preventiva e la profilazione di massa rendono l'utente costantemente visibile attraverso la sua attività in rete. In tale contesto, l'identità digitale si atteggia a proiezione funzionale al *social scoring*: ogni interazione *online* contribuisce a un *dossier* statale che abilita o limita l'accesso a diritti e servizi. Dunque, il soggetto non controlla i dati che lo rappresentano, ma li subisce come strumento politico-sociale.

Nelle democrazie occidentali, la sorveglianza non assume forme così manifestamente coercitive ma, come visto, si è trasformata in 'capitalismo della sorveglianza'. L'identità dell'utente diviene materia prima per la profilazione commerciale: il potere non è più concentrato nella torre centrale, bensì diffuso in una costellazione di *server*, sensori mobili e piattaforme che accumulano dati biografici, relazionali e biometrici.

²⁴⁷ Segnatamente, negli ultimi anni la Russia ha investito ingenti somme per sviluppare una rete intranet per consentire al Paese di disconnettersi dalla rete globale. In considerazione dei recenti sviluppi politici-internazionali, derivanti dall'invasione dell'Ucraina, l'obiettivo primario del governo russo è oggi quello di raggiungere un'autarchia digitale. Per una ricognizione del dibattito sull'argomento si rinvia, tra gli altri a M. Ristolainen, *Should 'runet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West*, in *Journal of information warfare*, 4, 2017, 112 ss. e S. Davydov (a cura di), *Internet in Russia. A Study of the Runet and Its Impact on Social Life*, Springer, 2020.

²⁴⁸ Per un approfondimento sull'argomento si veda G. Walton, *China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China*, Rights & Democracy, 2001; J. Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, Zed Books, Londra, 2019.

Così, il modello della sorveglianza dell'individuo finisce per sovrapporsi in larga parte con quello della sorveglianza dei dati o di "dataveglianza"²⁴⁹. Tale modello, pertanto, sembra reggersi sulla struttura non tanto di un 'Super-panopticon', come da alcuni sostenuto, ma del modello sinottico fatto proprio da Bauman per descrivere la società postmoderna²⁵⁰.

La sorveglianza non proviene più da un centro, ma assume caratteri sempre più labirintici, capillari, al punto da evocare una dimensione 'kafkiana'.

Così, il 'Grande Fratello' descritto da Orwell evolve in una forma più penetrante, quella teorizzata da Lessig (tra i pionieri del diritto di *Internet*)²⁵¹, in cui il controllo esercitato dal potere governativo si fonde con quello delle grandi multinazionali tecnologiche. Dalla commistione tra *Big Governments* e *Big Tech* emerge così un nuovo tipo di 'occhio', dotato di uno sguardo più acuto e penetrante rispetto al passato.

Consapevole della polarizzazione tra visione mercatista e sovranismo autoritario, l'Unione europea – a partire dal discorso del Presidente Macron, in occasione dell'*Internet Governance Forum* del 2018²⁵² – ha aperto la strada alla creazione di un terzo modello europeo di *Internet governance*. Quest'ultimo, distinto sia dal modello 'californiano', sia da quello 'cinese', rappresenta una 'terza via'²⁵³ fondata sulla tutela dei diritti fondamentali, garanzia della concorrenza e neutralità tecnologica²⁵⁴. Tale strada ha già trovato una dimensione concreta a seguito

²⁴⁹ L'espressione è di R. Clarke, *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, 1988, 498 ss.

²⁵⁰ Z. Bauman, D. Lyon, *La sorveglianza nella modernità liquida*, cit.

²⁵¹ Si rimanda alle note idee di L. Lessig, *Code: And Other Laws of Cyberspace*, cit.; Id., *Code: Version 2.0*, Basic Books, New York, 2006.

²⁵² L'*Internet Governance Forum* (IGF) è una piattaforma *multi-stakeholder* istituita nel 2006 dalle Nazioni Unite con l'obiettivo di garantire con cadenza annuale un dialogo aperto e inclusivo su questioni specifiche riguardanti *Internet*. Cfr. J. Mathiason, *Internet Governance: The New Frontier of Global Institutions*, Routledge, Abingdon, 2009; J. Malcom, *Multi-stakeholder governance and the Internet Governance Forum*, Terminus Press, Perth, 2008; D. Epstein, *The making of information governance: the case of the Internet Governance Forum*, in *journal of Information Technology*, 2, 2013, 137-149.

²⁵³ Sull'argomento si veda, *ex multis*, O. Pollicino, *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online*, in *Riv. trim. dir. pubbl.*, 4, 2022, 1051-1068.

²⁵⁴ Sul tema si rinvia a T. Wu, *Network Neutrality, Broadband Discrimination*, in *Journal on Telecommunications and High Technology Law*, 2, 2003, 141-175; Id., *The Master Switch: The Rise and Fall of Information Empires*, Alfred A. Knopf, New York, 2010; H.K. Cheng, B. Subhaiyoti, G. Hong, *The debate on net neutrality: a policy perspective*, in *Information system research*, 1, 2011, 60-82. Con riferimento alla letteratura italiana, v. D'Acunto L. (a cura di), *Net (or not) Neutrality?*

dell'adozione del pacchetto sulla legge sui servizi digitali, composto dal *Digital Services Act* (DSA)²⁵⁵ e dal *Digital Market Act* (DMA)²⁵⁶.

Nonostante non venga affrontato in maniera diretta, il tema della 'sorveglianza digitale' o 'dataveglianza', sembra affermarsi un nuovo equilibrio tra la tutela dei diritti fondamentali e il mantenimento del già richiamato principio di neutralità della rete.

In questi scenari fin qui descritti, l'identità digitale si atteggia a parametro rivelatore delle differenti filosofie di *governance*.

Nel 'modello californiano' costituisce merce detenuta da privati e scambiata in mercati opachi; nel 'modello cinese' è appendice del passaporto interno, imposta dallo Stato e funzionale alla sorveglianza politica.

Nella prospettiva europea, invece, aspira a configurarsi quale diritto della personalità, ma restano aperte questioni delicate. Fino a che punto l'ecosistema occidentale, pur normato, riuscirà a evitare derive soffocanti? La natura invisibile dell'attività di *profiling* algoritmico rende meno tangibile la minaccia, ma non ne riduce l'impatto. Per questo la 'terza via' europea dovrà occuparsi di promuovere l'alfabetizzazione digitale, *audit* indipendenti e *accountability* computazionale.

3. Tipologie di sistemi di gestione dell'identità digitale

Dopo aver analizzato i diversi modelli di *governance* della rete, sembra opportuno soffermarsi sui sistemi di gestione dell'identità digitale che rappresentano la traduzione operativa di precise scelte politico-istituzionali.

Sebbene vengano descritti in termini puramente tecnici (architetture informatiche, protocolli di autenticazione, *standard* di interoperabilità), tali sistemi riflettono una determinata concezione del potere e fiducia nello spazio digitale.

La loro struttura definisce chi esercita il controllo sui dati, come si distribuiscono le responsabilità tra soggetti pubblici e privati e in quale misura l'individuo conserva la propria autonomia informativa. In questo senso, l'architettura tecnica

Web e regolazione, ESI, Napoli, 2017; P. Otranto, *Net Neutrality e poteri amministrativi*, in *federalismi.it*, 3, 2019, 2-45.

²⁵⁵ Reg. (UE) 5 luglio 2022, n. 2065, sul punto v. S. Tommasi, "*Digital services act*" e "*artificial intelligence act*": tentativi di futuro da armonizzare, in *Persona e Mercato*, 2/2023, 279 ss.

²⁵⁶ Reg. (UE) 5 luglio 2022, n. 1925.

dell'identità non è neutra: traduce sul piano infrastrutturale una visione politica della rete e del rapporto tra cittadino, mercato e istituzioni.

Per 'sistema di gestione dell'identità digitale' si intende, in questa sede, l'insieme di regole, procedure e tecnologie che disciplinano l'intero ciclo di vita dell'identità: dalla verifica iniziale del soggetto, al rilascio e alla conservazione delle credenziali, fino all'autenticazione presso i servizi.

L'assetto della fiducia e la ripartizione delle responsabilità lungo questa catena non costituiscono meri dettagli tecnici, bensì variabili che incidono sull'intensità della profilazione, sulla concentrazione dei dati, sulla resilienza dell'infrastruttura ed anche sulla tutela effettiva dei diritti.

La prassi e la letteratura distinguono tre modelli di riferimento che corrispondono alle soluzioni effettivamente adottate.

Nel modello centralizzato, un unico soggetto istituisce l'identità, custodisce gli attributi e le credenziali. Tale soluzione assicura una *governance* lineare e basata su *standard* maturi, pur concentrando potere decisionale e informativo con rischi connessi al *single point of failure*, alla proliferazione degli *account* e a possibili tensioni con i principi di minimizzazione e di limitazione della finalità.

Il modello federato introduce invece una separazione di ruoli: un *Identity Provider* (IdP) rilascia e gestisce le credenziali, mentre una pluralità di *Service Provider* (SP) le accetta, consentendo all'utente di utilizzare un'unica identità per accedere a servizi diversi (*Single Sign-On*). Ne derivano vantaggi in termini di portabilità e usabilità e riduzione della frammentazione, ma anche ulteriori criticità come la dipendenza dall'intermediario e la concentrazione dei metadati presso l'IdP, con possibili effetti a cascata in caso di disservizi o violazioni.

Con il modello decentralizzato infine, il baricentro si sposta sull'utente: le credenziali vengono custodite in un *wallet* personale e presentate in forma selettiva, mentre soggetti pubblici o privati rilasciano attestati firmati e verificabili.

Cresce così il controllo individuale e si limita la circolazione dei dati, ma emergono sfide rilevanti come la gestione sicura delle chiavi crittografiche, la necessità di meccanismi di recupero affidabili e la compatibilità con alcuni diritti fondamentali. La trattazione che segue si propone di approfondire le caratteristiche distintive di ciascun modello di gestione dell'identità, non con l'intento di individuare un

paradigma superiore agli altri, ma piuttosto di evidenziare le condizioni di funzionamento, i limiti strutturali che ognuno di essi presenta.

L'obiettivo è mostrare come l'evoluzione del sistema tenda verso configurazioni ibride capaci di distribuire poteri e responsabilità, preservando al contempo sicurezza, concorrenza e tutela dei diritti fondamentali in un quadro di fiducia tecnologica.

3.1. Il modello centralizzato

Il modello centralizzato di gestione dell'identità digitale – spesso definito ‘modello silos’ – si fonda sull'accentramento di tutte le fasi del ciclo di vita dell'identità in capo a un unico soggetto – pubblico o privato – che funge da *trust anchor* per l'intero ecosistema di servizi²⁵⁷.

L'organizzazione che istituisce l'identità dell'utente per il proprio servizio rimane il punto centrale del modello. In tale archetipo, l'utente crea il proprio *account*, attraverso credenziali presso la stessa organizzazione erogatrice del servizio (ad esempio un *social network*, una banca o una piattaforma di *e-commerce*).

Il gestore conserva nei propri *database* interni (c.d. ‘silos’), sia gli attributi identificativi (nome, data di nascita, recapiti) sia i fattori di autenticazione, assumendo al contempo le funzioni di verifica, autorizzazione, *audit* e revoca.

Sul versante tecnico-organizzativo il modello offre molteplici vantaggi intuitivi. Innanzitutto, la maturità degli *standard*: i protocolli sono ormai consolidati e supportati da un'ampia base di *best practice* in tema di sicurezza applicativa e infrastrutturale. Altro aspetto da evidenziare è la semplicità di *governance*: esistendo un unico titolare del trattamento, le responsabilità in caso di *data breach*

²⁵⁷ Sull'argomento cfr. H. Rittenberg, *Who Are You: A Primer on Digital Identity*, cit.; P.A. Grassi, M.E. Garcia, J.L. Fenton, *Digital Identity Guidelines*, National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.SP.800-63-3>; A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, the Sovrin Foundation, 29(2016)18, 2016; World Economic Forum, *Inclusive Deployment of Blockchain for Supply Chains (white paper)*, Parte 2, <https://www.weforum.org/publications/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction/>, 2019; U. Glasser, M. Vajihollahi, *Identity management architecture*, in *Security Informatics*, Springer, 2010, 97 ss.; J. Bradley, B. Hill, N. Sakimura, *Identity Management Using a Centralized Authority*. In *Proceedings of the 2014 IEEE International Conference on Identity, in Security and Behavior Analysis (ISBA)*, Hong Kong, 14-18 July 2014, 1-8.

risultano facilmente individuabili e l'adempimento degli obblighi di notifica (art. 33 GDPR) segue una catena gerarchica lineare²⁵⁸.

Infine, la riduzione dei costi di coordinamento: il *service provider* delega l'intero processo di *on-boarding* a sé stesso, evitando di dover stipulare accordi di fiducia con soggetti terzi e garantendosi l'accesso continuativo a un patrimonio informativo strategico per l'analisi di mercato.

Tale assetto, tuttavia, porta con sé alcuni potenziali rischi e debolezze.

Il primo problema si riscontra nella circostanza per cui la compromissione del *database* dell'organizzazione – come dimostrano i casi *Yahoo*, *Equifax* o, più di recente, *EasyJet* – esporrebbe simultaneamente un imponente numero di dati sensibili identitari²⁵⁹.

La concentrazione di tali dati in un unico perimetro si traduce in una superficie di attacco altamente appetibile per attori malevoli, costringendo i gestori a investimenti crescenti in *cyber-defence* senza, tuttavia, poter garantire il rischio zero.

In secondo luogo, l'architettura centralizzata genera il c.d. 'fenomeno delle identità multiple': ogni piattaforma richiede la creazione di un nuovo *account*, costringendo l'utente a gestire insiemi eterogenei di credenziali e aumentando il rischio di riutilizzo di *password* deboli²⁶⁰.

Ne derivano inefficienze, duplicazioni informative e, sul piano dei diritti, una violazione sistemica del principio di minimizzazione dei dati (art. 5, § 1, lett. c) GDPR), poiché lo stesso attributo viene replicato in innumerevoli silos sprovvisti di interoperabilità semantica.

Inoltre, la disponibilità di insiemi di dati comportamentali può alimentare modelli di profilazione a fini di *marketing* predittivo, in molti casi oltre la soglia del legittimo interesse e in potenziale contrasto con il principio di limitazione della finalità (art. 5, § 1, lett. b) GDPR).

²⁵⁸ Cfr. S. Romanosky, *Examining the Impact of Data Breach Disclosure Laws*, in *Journal of Policy Analysis and Management*, 35(3), 2016, 641 ss.; D.K. Citron, D. Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, in *Texas Law Review*, 96(4), 2018, 737 ss.

²⁵⁹ In tal senso v. H.V.A. Le *et al.*, *Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees*, in *Computers*, 14/2025, 2 ss.

²⁶⁰ *Ibidem*.

La pandemia di Covid-19 ha accentuato tali limiti, sottoponendo i registri centrali a carichi senza precedenti: il massiccio ricorso ai servizi *online* di pubbliche amministrazioni e piattaforme sanitarie ha evidenziato problemi di scalabilità e di resilienza operativa.

Sul piano normativo-istituzionale, la direttiva la c.d. *Open Data Directive*²⁶¹ e il regolamento eIDAS inquadrano il gestore centralizzato come *Qualified Trust Service Provider*, attribuendogli titolarità piena e obblighi di sicurezza rafforzata (artt. 24-27 eIDAS).

Tuttavia, l'evoluzione regolatoria più recente (Regolamento eIDAS 2) prefigura un decentramento selettivo: il *wallet* europeo, pur interoperando con i registri nazionali, delega la custodia delle credenziali al dispositivo dell'utente, dimezzando la dipendenza da silos monolitici e introducendo l'obbligo di *selective disclosure by design*²⁶².

In prospettiva comparata, il paradigma centralizzato conserva un rilevante vantaggio di implementazione in settori regolamentati ad alto rischio (servizi bancari, telecomunicazioni, difesa), dove l'esigenza di un *audit* univoco e di requisiti di *compliance* certificabili supera le istanze di portabilità.

Nondimeno, le pressioni regolatorie sulla protezione dei dati e la crescita di applicazioni transfrontaliere – finanza aperta, *e-government*, sanità digitale – rendono plausibile un graduale spostamento verso altre tipologie di modelli, nei quali il potere di certificare e custodire l'identità sia distribuito tra più attori sotto cornici di fiducia comuni²⁶³.

In conclusione, il modello centralizzato rimane una pietra angolare dell'identità digitale contemporanea grazie alla sua chiarezza di *governance* e alla disponibilità di soluzioni pronte all'uso; tuttavia, i rischi di *single point of failure*, la moltiplicazione delle identità e le tensioni con i principi di *privacy* e concorrenza ne evidenziano la natura transitoria.

²⁶¹ Direttiva (UE) 20 giugno 2019, n. 1024.

²⁶² Per *selective disclosure by design* si intende un principio di *privacy by design* applicato ai sistemi di identità: l'utente deve poter rivelare al verificatore solo gli attributi strettamente necessari, senza mostrare l'intera credenziale.

²⁶³ V. D. Wang, J. Zhao, Y. Wang, *A Survey on Privacy Protection of Blockchain: The Technology and Application*, in *IEE Access*, 8/2020.

La traiettoria evolutiva, già tracciata dalle recenti iniziative europee e dall'emergere di architetture *Self-Sovereign*, indica la necessità di ricomporre la dicotomia fra efficienza centralizzata e tutela dei diritti, orientando la progettazione di sistemi identitari verso schemi che distribuiscano responsabilità e poteri in modo più equo e resiliente.

3.2. Il modello federato

Il modello federato nasce come risposta ai problemi propri dell'architettura centralizzata²⁶⁴. In questo schema l'elemento cardine è l'*Identity Provider*, soggetto (pubblico o privato) che detiene gli attributi dell'utente, li autentica e, su richiesta li trasferisce in modo standardizzato ai diversi *Service Provider* con cui l'utente intende interagire. In tal senso l'IdP agisce da ponte di fiducia tra l'utente e la molteplicità di servizi disponibili, consentendo la fruizione attraverso una sola identità per accedere a una pluralità di domini applicativi.

Sul piano tecnico, la federazione si fonda su protocolli interoperabili che permettono di veicolare in maniera sicura asserti di autenticazione e attributi aggiuntivi.

Dunque, ci sarà un reindirizzamento per l'utente all'IdP per il *login*: quest'ultimo verifica le credenziali, genera una conferma firmata digitalmente e lo invia allo SP, il quale, fidandosi della firma dell'IdP, rilascia l'accesso alla risorsa.

Nell'ordinamento nazionale, il Sistema Pubblico di Identità Digitale (SPID) costituisce una federazione di nove *Identity provider* qualificati²⁶⁵ che emettono

²⁶⁴ Sull'argomento si rinvia a C. Satchell *et al.*, *Identity crisis: user perspectives on multiplicity and control in federated identity management*, in *Behaviour & Information Technology*, 1/2011, 51 ss.; D.W. Chadwick, *Federated identity management*, in *Foundations of Security Analysis and Design*, Springer, 96 ss., 2009; H. Rittenberg, *Who Are You*, cit.; P.A. Grassi, M.E. Garcia, J.L. Fenton, *Digital Identity Guidelines*, cit.; A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, cit.; World Economic Forum, *Inclusive Deployment of Blockchain for Supply Chains (white paper)*, cit.; U. Glasser, M. Vajihollahi, *Identity management architecture*, cit., 97 ss.; J. Carretero *et al.*, *Federated identity architecture of the European eID System*, in *IEEE Access*, 6/2018, 75302 ss.; T. Hardjono, A. Pentland, *Open Algorithms for Identity Federation*, in *Advances in Information and Communication Networks*, 2019, 24 ss.

²⁶⁵ Gli *Identity Provider* accreditati nella federazione SPID risultano: Aruba ID, EtnaID, Intesi Group ID, InfoCert ID, ID InfoCamere, Lepida ID, Namirial ID, PosteID, SielteID, SpidItalia, TeamSystem ID, TIM ID (Presidenza del Consiglio dei ministri - Dipartimento per la trasformazione digitale).

credenziali di diverso livello di garanzia riconosciute da oltre 13000 amministrazioni e da un numero crescente di operatori privati.

Il modello – come già osservato – assicura la portabilità transfrontaliera previa notifica eIDAS e limita la creazione di nuovi *account*, pur lasciando all’IdP la custodia dei dati e il *log* degli accessi.

Sul versante privato, l’accesso con *Google* o *Facebook Login* rappresenta, invece, la variante commerciale del paradigma: l’utente riutilizza il proprio *account social* per registrarsi rapidamente su siti terzi.

I vantaggi funzionali del modello federato sono molteplici. Anzitutto l’utente gestisce un’unica coppia di credenziali e riduce la probabilità di *password* deboli o riutilizzate.

Accanto a tali benefici si collocano criticità non trascurabili.

Il principale è dato dal fatto che la federazione introduce un vincolo di interdipendenza reputazionale: una violazione o un disservizio dell’IdP si propaga a cascata su tutti i *service provider*, generando un rischio sistemico. È dunque essenziale che il quadro contrattuale sia solido e che esistano meccanismi che garantiscano la continuità operativa.

Sul piano giuridico-istituzionale, il regolamento eIDAS ha già sperimentato la federazione a livello statale mediante il meccanismo di ‘schema notificato’: uno Stato membro può far riconoscere le proprie identità elettroniche negli altri Stati, purché rispetti i requisiti di sicurezza, interoperabilità e protezione dati fissati dalla Commissione.

La revisione eIDAS 2 introduce ora il concetto di *European Digital Identity Wallet* che, pur basandosi su IdP nazionali, sposta la custodia delle credenziali nel dispositivo dell’utente, delineando un modello federato-decentrato in cui l’IdP certifica ma non conserva necessariamente i dati²⁶⁶.

In conclusione, il modello federato rappresenta un’evoluzione intermedia tra l’accentramento rigido dei silos e la piena autodeterminazione promessa dall’identità *Self-Sovereign*. Per evitare che la concentrazione di potere informativo

²⁶⁶ Cfr. B. Podgorelec, L. Alber, T. Zefferer, *What is a (Digital) Identity Wallet? A Systematic Literature Review*, in *IEEE 46th Annual Computers, Software, and Applications Conference*, 2022, 809 ss.; D. Baldini, *The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet*, cit.

si traduca in nuove forme di sorveglianza o in pratiche anticoncorrenziali, il legislatore e gli organismi di standardizzazione dovranno promuovere pluralismo degli IdP, trasparenza algoritmica e meccanismi di *accountability* robusti, così da assicurare che la federazione, oltre a semplificare l'esperienza dell'utente, rafforzi effettivamente il suo controllo sull'identità digitale.

3.3. Il modello decentralizzato

Il modello decentralizzato, noto come *Self-Sovereign Identity* (SSI), rappresenta la terza – e finora più ambiziosa – tappa dell'evoluzione dei sistemi di gestione dell'identità digitale²⁶⁷.

Al centro della SSI vi è un principio di piena titolarità individuale: l'identità non è emessa né custodita in modo permanente da un'autorità centrale (come nel modello centralizzato), né intermediata da un *identity provider* (come nel modello federato),

²⁶⁷ Sul tema si rinvia a C. Allen, *The Path to Self-Sovereign Identity*, 26 aprile 2016; A. Preukschat, D. Reed, *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credential*, New York, 2021; A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, cit.; A. Mühle et al., *A Survey on Essential Components of a Self-Sovereign Identity*, 17 luglio 2018; F. Schardong, R. Custódio, *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*, in *Sensors*, 22/2022; R. Soltani, U.T. Nguyen, A. An, *A Survey of Self-Sovereign Identity Ecosystem, Security and Communication Network*, in *Security and Communication Networks*, 2021; F. Glaser, *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis*, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 1543 ss.; M. Raskin, D. Yermack, *Digital Currencies, Decentralized Ledgers, and the Future of Central Banking*, in P. Conti-Brown, R.M. Lastra (eds.), *Research Handbook on Central Banking*, 2018, 474 ss.; O.J. Gstrein, D. Kochenov, *Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?*, in *Frontiers in Blockchain*, 3/2020, 1 ss.; P. De Filippi, A. Wright, *Blockchain and the Law*, Cambridge (MA), 2018; S. Pike, F. Dickson, *Identity on the Blockchain Special Report: Forecast and Analysis for Blockchain-Based Identity Solutions*, Jul 2018 - *Special Study*, 2018; K.C. Toth, A. Anderson-Priddy, *Self-Sovereign digital identity - a paradigm shift for identity*, in *IEEE Secur. Priv.*, 17/2019, 17 ss.; U. Der, S. Jähnichen, J. Sürmeli, *Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution*, in *Computers and Society*, 5 dicembre 2017; Š. Čučko, M. Turkanović, *Decentralized and self-sovereign identity: Systematic mapping study*, in *IEEE Access*, 4/2016, 1 ss.; Q. Stokkink et al., *A truly selfsovereign identity system*, in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 1-8, 2021; M. Kubach et al., *Selfsovereign and decentralized identity as the future of identity management?*, in *Open Identity Summit 2020*, 2020; F. Wang, P. De Filippi, *Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion*, in *Frontiers in Blockchain*, 2/2020; M. Alexander, *A survey on essential components of a selfsovereign identity*, in *Computer Science Review*, vol. 30, 80 ss., 2018; A. Othman, J. Callahan, *The Horcrux Protocol: a Method for Decentralized Biometric-based Self-sovereign identity*, in *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN)*, 1-7, luglio 2018; H.V.A. Le et al., *Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees*, cit.

ma è detenuta, controllata e presentata direttamente dall'utente mediante strumenti crittografici che ne garantiscono autenticità, integrità e verificabilità²⁶⁸.

Ispirato alla filosofia “*user-centric*” maturata nell'ambiente *Cypherpunk* e reso tecnicamente praticabile dalle *blockchain permissioned* o *permissionless*, il paradigma ridisegna la catena della fiducia spostandone il baricentro dall'istituzione al soggetto interessato.

I vantaggi sistemici del modello decentralizzato sono notevoli. In primo luogo, esso elimina il rischio di *single point of failure*: non esistendo un archivio centrale, un attacco informatico non può compromettere milioni di identità in un sol colpo²⁶⁹.

In secondo luogo, la portabilità globale: un DID non è vincolato a confini giurisdizionali, cosicché l'identità diventa transfrontaliera. Ciò si rivela cruciale per migranti, rifugiati e soggetti privi di documenti, cui i programmi delle Nazioni Unite guardano con crescente interesse²⁷⁰.

In terzo luogo, la struttura della tecnologia soddisfa intrinsecamente il principio di minimizzazione e consente all'utente di mantenere una visibilità completa sui *logs* di accesso, riducendo la sorveglianza invisibile tipica degli IdP federati.

Non mancano, tuttavia, sfide di prima grandezza.

La più discussa è la custodia delle chiavi: la perdita della *private key* equivale a una dissoluzione dell'identità digitale e impone meccanismi di recupero che non tradiscano la sovranità dell'utente. Un secondo nodo riguarda invece la *governance* dei *ledger*: se la *blockchain* è *permissionless*, i nodi validatori possono risiedere in giurisdizioni con *standard* di tutela dei dati divergenti; se è *permissioned*, la selezione degli operatori può reintrodurre centri di potere che minano la

²⁶⁸ G. Laatikainen, T. Kolehmainen, P. Abrahamsson, *Self-Sovereign Identity Ecosystems: Benefits and Challenges*, in *12th Scandinavian Conference on Information Systems*, Orkanger, Norway, 17 giugno 2021.

²⁶⁹ *Ibidem*.

²⁷⁰ Sull'applicazione della tecnologia *blockchain* nel settore umanitario, si veda A.J. Zwitter, M. Boisse-Despiaux, *Blockchain for humanitarian action and development aid*, in *J. Int. Humanit. Action*, 3/2018, 1 ss., che analizza i principali casi d'uso mettendone in luce opportunità e criticità e B. Kewell, R. Adams, G. Parry, *Blockchain for Good?*, in *Strategic Change*, 26/2017, 429 ss. In relazione all'impiego della *blockchain* per la potenziale creazione di identità basate su dati biometrici destinate a combattere la tratta di minori, cfr. S. Sundararajan, *Moldova Eyes Blockchain IDs to help curb child trafficking*. *Coin Desk*, <https://www.coindesk.com/moldova-eyes-blockchain-ids-to-help-curb-child-trafficking/>, 2017.

decentralizzazione sostanziale. Terzo, l'immutabilità del registro collide con il diritto alla cancellazione (art. 17 GDPR).

Sul piano normativo l'Unione europea sta compiendo passi decisivi.

Il Regolamento eIDAS 2 riconosce il *wallet* europeo di identità digitale come strumento in cui le credenziali sono custodite dall'utente, mentre gli Stati si limitano a emettere attributi qualificati firmati. L'infrastruttura EBSI sperimenta già casi d'uso – diplomi universitari, qualifiche professionali – su un *ledger* gestito congiuntamente dai Paesi membri, dimostrando la fattibilità di un modello *permissioned* a governance pubblica.

Tuttavia, il rischio di *digital divide* è reale: l'onere di gestire chiavi, *backup* e aggiornamenti *software* può escludere le fasce meno alfabetizzate. Programmi di alfabetizzazione digitale, interfacce *human-centric* e servizi di custodia delegata regolamentati (analoghi ai conti correnti) diventano quindi componenti essenziali di una SSI equa e inclusiva.

In prospettiva, il modello decentralizzato non va considerato in ottica sostitutiva rispetto alle soluzioni preesistenti, ma come un *layer* complementare che ridistribuisce poteri e responsabilità. Gli Stati e le imprese conservano la facoltà di emettere attributi veritieri e di alta affidabilità, ma perdono il monopolio della custodia; l'utente acquista autonomia senza rinunciare a garanzie di validità legale. La sfida consisterà nel calibrare *trust framework* ibridi – fatti di *standard* aperti, regole di *governance* e *audit* indipendenti – che sappiano coniugare la resilienza tecnica delle *blockchain* con i requisiti di proporzionalità, protezione dati e sicurezza pubblica. Solo così la *Self-Sovereign Identity* potrà trasformarsi da paradigma visionario a infrastruttura concreta al servizio dei diritti fondamentali e dello sviluppo socio-economico.

CAPITOLO III

Quale futuro per l'identità digitale?

1. I futuri ostacoli della cittadinanza digitale

Nell'attuale scenario di trasformazione tecnologica, la 'cittadinanza digitale' si confronta con sfide che ne condizionano l'effettiva realizzazione.

Tra queste, come già affrontato, un ruolo centrale è assunto dall'intelligenza artificiale, che si configura come fattore ambivalente. Se da un lato, l'IA è in grado di incrementare l'efficienza dei servizi pubblici, favorire l'accesso all'informazione, promuovere l'autonomia di soggetti fragili, ampliando dunque le possibilità di inclusione sociale, dall'altro lato rischia di consolidare disuguaglianze già esistenti.

In assenza di adeguate garanzie di equità, trasparenza e accessibilità, la tecnologia potrebbe riprodurre *bias* algoritmici, escludendo i soggetti meno alfabetizzati digitalmente e rendendo opachi processi decisionali determinanti per l'attribuzione di diritti e per l'accesso a prestazioni essenziali.

In tale prospettiva, garantire un accesso equo e sostanziale alle opportunità offerte dalla società digitale diviene una sfida strettamente connessa all'attuazione del principio di uguaglianza sostanziale sancito dall'art. 3, comma 2, della Costituzione, che impone al legislatore e alle istituzioni di predisporre strategie normative e politiche inclusive orientate a un futuro digitale democratico e rispettoso delle diversità²⁷¹.

L'accesso alle tecnologie digitali e la capacità di utilizzarle consapevolmente costituiscono infatti prerequisiti imprescindibili per la partecipazione alla vita economica, sociale e istituzionale.

In assenza di adeguate misure di inclusione, la digitalizzazione rischia di trasformarsi da strumento di democratizzazione a fattore di esclusione, generando nuove forme di stratificazione sociale²⁷².

²⁷¹ C. Napolitano, *Inclusione sociale e trasformazione digitale: dal digital divide all'esclusione algoritmica*, in *Democrazia e Diritti Sociali*, 1/2025, 179 ss.

²⁷² Sul tema si vedano, *ex multis*, E.J. Helsper, *The digital disconnect. The social causes and consequences of digital inequalities*, Londra, 2021; S. Vantin, *I divari digitali nell'epoca della rete*

Il fenomeno del *digital divide*²⁷³ rappresenta l'espressione più evidente di tali dinamiche. Non più limitato alla mera disponibilità di dispositivi o infrastrutture di rete, esso assume una connotazione multidimensionale.

Al *deficit* infrastrutturale (*access divide*) si affianca infatti un divario culturale (*skills divide*), connesso al possesso delle competenze necessarie per un utilizzo efficace degli strumenti digitali. A ciò si aggiunge una dimensione intergenerazionale: se i cosiddetti 'nativi digitali' possiedono una naturale familiarità con gli strumenti informatici, altre fasce di popolazione (in particolare anziani e adulti privi di percorsi di alfabetizzazione) risultano penalizzate nell'accesso e nell'uso consapevole degli strumenti informatici²⁷⁴.

Questa distribuzione diseguale delle competenze riproduce e amplifica fratture economiche, territoriali, educative e generazionali. Il *deficit* di competenze digitali si configura così come un moltiplicatore delle disuguaglianze, incidendo sull'effettività dei diritti e sull'accesso alle opportunità proprie della società digitale.

Le disuguaglianze socio-digitali emergono in particolar modo dalle intersezioni tra fattori economici, culturali e infrastrutturali, che determinano condizioni di accesso molto differenziate. Chi dispone di maggiori risorse economiche e culturali risulta favorito nell'acquisto di dispositivi aggiornati, nell'accesso a connessioni stabili e nell'acquisizione di competenze.

globale, in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, 2024.

²⁷³ Sul tema si rinvia a K. Mossberger, C.J. Talbert, M. Stansbury, *Virtual Inequality. Beyond the Digital Divide*, Washington, 2003; B.M. Compaine, *The Digital Divide: Facing a Crisis or Creating a Myth?*, Cambridge, 2003; P. Norris, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge, 2001.

²⁷⁴ Cfr. E. Hargittai, *Second Level Digital Divide: Differences in People's Online Skills*, First Monday, in www.firstmonday.org, 7, 4/2002; E. Hargittai, A. Hinnant, *Digital Inequality: Differences in Young Adults' Use of the Internet*, in *Communication Research*, 5/2008, 602 ss.; S. Bentivegna, *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Roma-Bari, 2009; L. Sartori, *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Bologna, 2006; R. Pisa, *Il digital divide e le iniziative per superarlo*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), *La Rete Internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015.

Al contrario, le categorie più vulnerabili – anziani, persone con disabilità, residenti in aree interne o migranti – affrontano barriere multilivello che limitano la funzione emancipatoria delle tecnologie²⁷⁵.

Dunque, un ulteriore profilo riguarda le differenze culturali: l'approccio alle tecnologie varia, infatti, da una piena adesione a forme di resistenza o rifiuto, influenzando in modo significativo le pratiche d'uso.

Da ciò emerge che le strategie di inclusione digitale devono adottare un approccio integrato, capace di tenere insieme le dimensioni infrastrutturali, educative e sociali, così da garantire una reale partecipazione alla cittadinanza digitale.

1.1. Il digital divide

La cittadinanza digitale, nelle sue diverse articolazioni, rappresenta in potenza un fattore egualitario: essa consente infatti di esercitare diritti indipendentemente dalla residenza fisica, dalla cittadinanza politica formale o dall'appartenenza a una specifica comunità territoriale²⁷⁶.

La digitalizzazione, per le sue caratteristiche intrinseche, si propone come strumento capace di rimuovere barriere materiali e sociali, rendendo più semplice l'accesso ai servizi pubblici e introducendo nuove forme di partecipazione. Nello spazio pubblico digitale, inoltre, alcuni diritti fondamentali assumono una rinnovata centralità: si pensi alla libertà di manifestazione del pensiero, al diritto di informazione, fino a ipotesi di esercizio delle libertà associative in forme del tutto inedite²⁷⁷.

²⁷⁵ Sull'argomento si rinvia a Cfr. B. Rabai, *The role of technology and innovation in digital and social inclusion. The case of disability in a public perspective*, in *MediaLaws*, n. 1/2022, 1 ss.; G. Goggin, *Disability and Digital Inequalities: Rethinking Digital Divides with Disability Theory*, in G.W. Muschert, M. Ragnedda (eds.), *Theorizing Digital Divides*, New York, 2017, 69 ss.; S.J. Macdonald, J. Clayton, *Back to the Future, Disability and the Digital Divide*, in *Disability & Society*, 5/2013, 702 ss.; P. Zuddas, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in Osservatorio AIC, 2/2020, 285 ss.

²⁷⁶ V. De Santis, *Cittadinanza digitale e disuguaglianze*, cit., 10 ss; A. Alu, *Il doppio volto di Internet tra l'accesso e l'uscita e il paradosso della "trappola" digitale*, in *Dir. fam. pers.*, 2/2023, 626 ss.

²⁷⁷ Nel quadro del programma *Next Generation EU*, la digitalizzazione è stata individuata come uno degli assi portanti del Piano nazionale di ripresa e resilienza: la transizione digitale è concepita non soltanto come occasione per accrescere la produttività del sistema economico, ma anche come strumento di coesione territoriale e sociale, volto a ridurre i divari di cittadinanza.

Tuttavia, nonostante i propositi di natura emancipatoria, la dimensione digitale può trasformarsi in fonte di nuove disuguaglianze se non accompagnata da adeguate politiche di inclusione.

L'accesso ai servizi *online*, la semplificazione delle procedure e la rapidità delle interazioni non sono disponibili per tutti in egual misura: una parte significativa della popolazione risulta ancora priva delle infrastrutture adeguate o delle competenze necessarie per utilizzare le tecnologie di base. Non a caso, il Piano Nazionale di Ripresa e Resilienza (PNRR) ha riconosciuto esplicitamente il *digital divide* come un ostacolo strutturale alla piena partecipazione dei cittadini alla vita democratica, all'accesso al mercato del lavoro e alla fruizione dei servizi essenziali²⁷⁸.

L'impossibilità di accedere alla rete e l'incapacità di utilizzare correttamente gli strumenti digitali si traducono dunque in nuovi fattori di disuguaglianza²⁷⁹.

Dunque, in un contesto in cui la vita sociale, economica e politica si svolge sempre più in modalità ibrida tra spazio fisico e spazio virtuale, la mancanza di accesso al digitale può tradursi in una vera e propria limitazione dell'esercizio delle libertà fondamentali²⁸⁰. In questo senso, il divario digitale non è soltanto un problema tecnico, ma diviene un ostacolo alla piena cittadinanza.

In un primo momento, il *digital divide* era ricondotto al solo piano infrastrutturale, ossia alla diseguale disponibilità di dispositivi e connessione²⁸¹. Successivamente, la dottrina ha evidenziato che tale prospettiva non coglieva la complessità del fenomeno²⁸².

È così emersa una seconda dimensione, relativa alle competenze digitali, concernente la capacità di utilizzare gli strumenti digitali in modo critico,

²⁷⁸ PNRR, 18-19, reperibile sul sito istituzionale del Governo.

²⁷⁹ V. De Santis, *Cittadinanza digitale e disuguaglianze*, cit., 10. Sul punto v. anche P. Piras, *L'amministrazione digitale tra divari e doveri. "Non camminare davanti a me, ma al mio fianco"*, in *P.A. Persona e Amministrazione*, 2/2022, 422.

²⁸⁰ A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale fra libertà e uguaglianze*, in *Dir. cost.*, 1/2023, 18.

²⁸¹ Sul punto v. J.A.G.M. Van Dijk, *The deeping divide. Inequality in the information society*, London, 2005, 3-6, ove l'Autore interpreta il divario digitale quale espressione della diseguale distribuzione delle risorse materiali necessarie all'accesso e all'uso delle tecnologie dell'informazione.

²⁸² M. Ragnedda, *Il digital divide. Le disuguaglianze digitali e i suoi vari livelli d'analisi*, in *Quaderni di Teoria Sociale*, 1/2018, 81 ss.

consapevole ed efficace: qui la *digital literacy*²⁸³, la motivazione all'uso e il supporto culturale diventano determinanti²⁸⁴.

Più recentemente l'analisi si è estesa a un terzo livello di *digital divide* relativo agli esiti sociali differenziati dell'uso delle tecnologie: non conta soltanto accedere o saper utilizzare gli strumenti, bensì trasformare tali risorse in opportunità concrete, valorizzando quello che è stato definito 'capitale digitale', ossia l'insieme delle competenze strategiche che consentono di trasformare l'accesso in effettivi benefici educativi, professionali o relazionali²⁸⁵.

Volendosi soffermare sui primi due livelli, il superamento del divario digitale implica anzitutto la garanzia dell'accesso alla rete *Internet*, oggi condizione imprescindibile per il pieno sviluppo individuale e sociale della persona. A conferma di ciò, la Dichiarazione dei diritti in *Internet* qualifica l'accesso alla rete come un 'diritto fondamentale'²⁸⁶.

Analogamente, la Risoluzione sulla Promozione, protezione e godimento dei diritti umani su *Internet* del Consiglio per i diritti umani dell'ONU ha riconosciuto l'accesso a *Internet* come diritto umano riconducibile alla libertà di opinione ed espressione²⁸⁷.

²⁸³ L. Pangrazio, J. Sefton-Green, *Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?*, in *Journal of New Approaches in Educational Research*, 1/2021, 15 ss.

²⁸⁴ Si rinvia a T. Correa, *The participation divide among "online experts": experience, skills and psychological factors as predictors of college students' web content creation*, in *Journal of Computer-Mediated communication*, 1/2010, 71 ss.; E. Hargittai, G. Walejko, *The participation divide: content creation and sharing in the digital age*, in *Information, Communication & Society*, 2/2008, 239 ss.; P. Attewell, *The First and Second Digital Divides*, in *Sociology of Education*, 3/2001, 252 ss.; P. Howard, L. Busch, P. Sheets, *Comparing digital divide: Internet access and social inequality in Canada and the United States*, in *Canadian Journal of Communication*, 1/2010, 109 ss.; H. Ono, M. Zavodny, *Immigrants, English Ability, and the Digital Divide*, in *Social Science Quarterly*, 3/2008, 1135 ss.; M. Hilbert, P. Lopez, C. Vasquez, *Information societies or "ICT equipment societies"? Measuring the digital information processing capacity of a society in bits and bytes*, in *The Information Society*, 3/ 2010, 157 ss.

²⁸⁵ M. Ragnedda, *The Third Digital Divide: a Weberian approach to digital inequalities*, Oxford, 2017.

²⁸⁶ Cfr. M.R. Allegri, *Il diritto di accesso a Internet: profili costituzionali*, in *MediaLaws*, 11 aprile 2021; R. Pisa, *L'accesso ad Internet: un nuovo diritto fondamentale?*, in *Treccani.it*, 7 gennaio 2010; F. Marcelli, *L'accesso a Internet come diritto fondamentale? Tendenze del diritto internazionale e realtà dei fatti*, in M. Pietrangelo (a cura di), *Il diritto accesso a Internet*, Napoli, 2011; V. Cerf, *Internet Access is not a Human Right*, in *The New York Times*, 4 gennaio 2012; C. Lotta, *Un nuovo diritto al tempo del Covid-19? Accesso a Internet e digital divide*, in *Rivista del Gruppo di Pisa*, 2/2020, 61 ss.; T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, in *Rivista AIC*, 1/2011; L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2-3/2012, 263 ss.

²⁸⁷ Consiglio per i diritti umani delle Nazioni Unite, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, Risoluzione del 29 giugno 2012, A/HRC/20/L.13.

Nella stessa direzione, il Rapporto *La Rue* del Comitato ONU per i diritti umani ha chiarito come l'accesso alla rete *Internet* costituisca una vera e propria condizione per l'esercizio dei diritti riconosciuti dalla Dichiarazione universale dei diritti dell'uomo²⁸⁸.

La questione è avvertita anche a livello europeo: il Codice europeo delle comunicazioni elettroniche²⁸⁹ qualifica l'accesso a *Internet* come «servizio universale», imponendo agli Stati membri di assicurare un «insieme minimo di servizi» a tutti gli utenti finali, a un prezzo accessibile e in condizioni non discriminatorie.

Coerentemente con quanto sinora esaminato, il Regolamento UE 2015/2120²⁹⁰ consacra il principio di neutralità della rete, riconoscendo agli utenti il diritto di accedere alle informazioni attraverso un trattamento equo del traffico *Internet*.

A livello nazionale, anche il Codice dell'amministrazione digitale prescrive alle pubbliche amministrazioni di favorire la connettività, prevedendo in particolare che negli uffici e nei luoghi pubblici – in ambito scolastico, sanitario e turistico – una quota della banda non utilizzata dagli uffici sia messa a disposizione degli utenti, secondo le modalità fissate dall'AgID.

In questa prospettiva, la sfera digitale «assume i contorni di una formazione sociale»²⁹¹ ai sensi dell'art. 2 della Costituzione, nella quale la personalità dell'individuo scorge nuove occasioni di sviluppo.

Tale inquadramento prospettato è rilevante non soltanto sul piano teorico, ma anche in relazione alle conseguenze pratiche: se la rete è il luogo in cui si svolge parte significativa della vita umana, la Repubblica ha dunque il dovere di rimuovere gli

²⁸⁸ Consiglio per i diritti umani delle Nazioni Unite, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue, 16 maggio 2011, A/HRC/17/27.

²⁸⁹ Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche, in G.U.U.E., L 321, 17 dicembre 2018, recepita in Italia con d.lgs. 8 novembre 2021, n. 207, in G.U., 27 novembre 2021, n. 282.

²⁹⁰ Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio, del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un *Internet* aperto e le tariffe per le comunicazioni intra-UE, in G.U.U.E., L 310, 26 novembre 2015.

²⁹¹ V. De Santis, *Cittadinanza digitale e disuguaglianze*, cit., 13. L' A. intende la «formazione sociale» come «comunità» di diritti e doveri e più genericamente come organizzazione intermedia tra l'individuo e lo Stato. Sul punto si rimanda a P. Rescigno, *Le formazioni sociali intermedie*, in AA.VV., *Dalla Costituente alla Costituzione*, Accademia nazionale dei Lincei, Roma, 1998; E. Rossi, *Le formazioni sociali nella Costituzione italiana*, Padova, 1989.

ostacoli che impediscono la piena inclusione digitale, in ossequio al principio di eguaglianza sostanziale²⁹².

Accanto al *deficit* infrastrutturale, vi è poi il problema – spesso intrecciato al primo – delle competenze digitali. Segnatamente, questa ‘livello’ di *digital divide* è favorito altresì dalla mancanza delle capacità e competenze necessarie per «partecipare alla società dell’informazione»²⁹³.

L’assenza di alfabetizzazione digitale determina una frattura netta tra chi vive una continuità tra dimensione reale e digitale e chi, invece, non ha mai accesso alla dimensione digitale dell’esistenza²⁹⁴. Le cause rintracciabili sono molteplici: età avanzata, basso livello di istruzione, appartenenza a categorie vulnerabili come migranti o persone detenute. In questi casi, la digitalizzazione, che potrebbe *a contrario* rappresentare uno strumento di inclusione e semplificazione, si traduce in un’ulteriore barriera, rendendo la vita pubblica meno accessibile.

Il legislatore italiano ha già individuato la necessità di affrontare queste lacune: il CAD riconosce il diritto all’alfabetizzazione informatica dei cittadini, precisando che l’accesso ai servizi digitali deve essere facile, sicuro e accessibile a tutti.

Inoltre, la stessa normativa pone in capo allo Stato e alle pubbliche amministrazioni l’obbligo di promuovere e diffondere la cultura informatica con particolare riguardo ai soggetti vulnerabili, ovvero minori e categorie a rischio di esclusione²⁹⁵.

A tal fine, negli anni sono stati introdotti diversi interventi legislativi in materia di istruzione: dall’introduzione della multimedialità come abilità da conseguire dalla scuola primaria e in ciascun ciclo di istruzione²⁹⁶, all’adozione del Piano Nazionale Scuola Digitale (PNSD)²⁹⁷, fino al recente Piano Scuola Digitale 2022-2026,

²⁹² Non mancano, infine, proposte di revisione costituzionale volte a sancire in maniera esplicita un diritto all’accesso a Internet: alcune mirano a modificare l’art. 21 Cost., altre a integrare l’art. 34, nella prospettiva di riconoscere l’accesso come diritto sociale connesso all’istruzione e allo sviluppo della persona. In ogni caso, ciò che emerge è la consapevolezza che l’accesso alla rete costituisce ormai condizione strumentale per l’effettivo esercizio di molteplici diritti fondamentali.

²⁹³ 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.

²⁹⁴ J. Rifkin, *L’era dell’accesso. La rivoluzione della new economy*, Milano, 2000, 21.

²⁹⁵ Art. 8 CAD.

²⁹⁶ D.lgs. 19 febbraio 2004, n. 59, “Definizione delle norme generali relative alla scuola dell’infanzia e al primo ciclo dell’istruzione, a norma dell’articolo 1 della legge 28 marzo 2003, n. 53”.

²⁹⁷ Introdotta dall’art. 1, commi 56-59, della l. 13 luglio 2015, n. 107, recante la riforma del sistema nazionale di istruzione e formazione (c.d. “Buona Scuola”), che ha avviato una strategia organica di innovazione digitale per il sistema scolastico.

finanziato dal PNRR, che rafforza la strategia di innovazione delle istituzioni scolastiche.

È necessario, tuttavia, evidenziare che l'alfabetizzazione digitale non riguarda soltanto i giovani, ma coinvolge diverse fasce di popolazione, compresi anziani e soggetti in condizioni di vulnerabilità economico-culturale.

In ogni caso la via più diretta per colmare il *digital divide* rimane quella di diffondere una cultura della digitalizzazione, capace di garantire a tutti non soltanto l'accesso tecnico, ma anche la consapevolezza e le competenze necessarie per vivere pienamente la cittadinanza nell'era digitale.

1.2. L'educazione digitale. Tra diritto sociale e cittadinanza

La giurisprudenza costituzionale italiana non ha avuto, sinora, numerose occasioni per affrontare direttamente il tema dell'accesso a *Internet* e delle competenze necessarie per il suo utilizzo.

Nelle occasioni in cui la Corte costituzionale si è espressa, essa ha ricondotto la questione dell'accesso ai mezzi informatici a una materia «a finalità di interesse generale, quale è lo sviluppo della cultura, nella specie attraverso l'uso dello strumento informatico»²⁹⁸.

In particolare, il Giudice delle leggi ha individuato nella cultura informatica un bene che la Repubblica è chiamata a promuovere in attuazione dell'art. 9 della Costituzione, senza però spingersi a riconoscere l'accesso alla rete come vero e proprio diritto sociale²⁹⁹, né tantomeno a collegare la carenza di infrastrutture o di alfabetizzazione digitale al diritto all'istruzione³⁰⁰.

²⁹⁸ Corte cost., sent. 7 luglio 2004, n. 307, Considerato in diritto § 3.1. Sulla pronuncia si rinvia ad A. Pace, *I progetti "PC ai giovani" e "PC alle famiglie": esercizio di potestà legislativa esclusiva statale o violazione della potestà regionale residuale*, in *Giur. cost.*, 5/2004, 3221 ss.

²⁹⁹ Non potendo in questa sede soffermarci sul concetto di diritto sociale, si rinvia *ex multis* a L.R. Perfetti, *I diritti sociali. Sui diritti fondamentali come esercizio della sovranità popolare nel rapporto con l'autorità*, in *Dir. pubbl.*, 1/2013, 64 ss.; A. Rovagnati, *Sulla natura giuridica dei diritti sociali*, Torino, 2009; F. Pergolesi, *Alcuni lineamenti dei diritti sociali*, Milano, 1953; M. Benvenuti, *Diritti sociali*, Milano, 2013; G. Corso, *I diritti sociali nella Costituzione italiana*, in *Riv. trim. dir. pubbl.*, 3/1981; G. Pino, *Diritti sociali. Per una critica di alcuni luoghi comuni*, in *Ragion Pratica*, 2/2016, 495 ss.; A. Guazzarotti, *I diritti sociali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Riv. trim. dir. pubbl.*, 1/2013, 9 ss.

³⁰⁰ L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensioni sociali*, in *Pol. dir.*, 2-3/2012, 278-279; M.R. Allegri, *Il diritto di accesso a Internet: profili*

La Corte si è limitata a sottolineare l'esistenza di un interesse pubblico alla diffusione della cultura informatica, ma non chiarisce se e in che misura gravi sulla Repubblica un obbligo di intervenire per rimuovere i divari digitali.

Eppure, risulta sempre più difficile negare che la mancanza di accesso a *Internet* e di adeguate competenze digitali configuri un nuovo diritto sociale emergente, radicato non solo nel principio fondamentale dell'art. 9 Cost., ma anche nel suo logico sviluppo attraverso gli artt. 33 e 34 della Costituzione sul diritto all'istruzione³⁰¹.

In questa prospettiva, la formazione digitale va intesa come parte integrante del diritto all'educazione, poiché rappresenta una condizione imprescindibile per l'esercizio dei diritti di cittadinanza in una società profondamente trasformata dalla tecnologia.

Le politiche pubbliche, pur in modo frammentario, hanno già affrontato la questione dell'inclusione digitale nella prospettiva dei percorsi scolastici e dei servizi educativi: il Piano Nazionale Scuola Digitale e, più di recente, le misure del PNRR hanno enfatizzato il legame indissolubile tra trasformazione digitale ed educazione³⁰².

Lo stesso PNRR, del resto, individua nella transizione verso la società digitale una sfida non solo tecnologica, ma educativa: la partecipazione attiva alla vita democratica ed economica non è pensabile senza una diffusa alfabetizzazione digitale della popolazione. Ciò colloca il problema entro l'orizzonte costituzionale tracciato dagli artt. 2 e 3, co. 2, della Costituzione che impongono alla Repubblica di rimuovere gli ostacoli che impediscono il pieno sviluppo della persona e la sua partecipazione alla vita sociale ed economica.

La cittadinanza digitale, se intesa come nuova forma di cittadinanza sociale, non può dunque essere disgiunta da un robusto investimento educativo.

costituzionali, in *MediaLaws*, 1/2021, 67; A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale*, cit., 23.

³⁰¹ S. Scagliarini, *I diritti costituzionali nell'era di internet: cittadinanza digitale, accesso alla rete e net neutrality*, in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, 3-16.

³⁰² N. Maniscalco, *La tecnologia come fattore di istruzione*, in *Rivista AIC*, 1/2024, 569 ss.; P. Aroldi, L. Zaffaroni, D. Cino, *Il primo lockdown e l'avvio della DAD come banco di prova dei processi di digitalizzazione nella scuola italiana, tra disuguaglianze e inclusione*, in *Sociologia della comunicazione*, 62, 2/2021, 69 ss.; R. Calvano, *L'istruzione, il Covid-19 e le disuguaglianze*, in *Costituzionalismo.it*, 3/2020, spec. 79 ss.

Per renderla effettiva non bastano interventi episodici, ma occorrono programmazione strutturale e finanziamenti stabili.

Lo strumento del PNRR ha costituito un passo importante in questa direzione, ma non sufficiente. Se l'obiettivo è ridurre le disuguaglianze di cittadinanza e rafforzare la coesione territoriale e sociale, saranno necessari strumenti finanziari comuni e una *governance* in grado di superare logiche meramente competitive o di breve periodo.

In assenza di un simile impegno, il rischio è che la digitalizzazione si traduca in un ulteriore fattore di discriminazione, alimentando politiche identitarie e visioni restrittive della cittadinanza ancorate esclusivamente al dato nazionale³⁰³.

Al contrario, rafforzare i diritti di cittadinanza digitale attraverso l'educazione significa colmare i divari di cittadinanza e rendere effettivo il principio di solidarietà, tanto a livello interno quanto a livello europeo.

³⁰³ J.A.G.M. Van Dijk, A.J.A.M. Van Deursen, *Digital Skills: Unlocking the Information Society*, Palgrave Macmillan, New York, 2014.

2. Verso un nuovo paradigma di ‘identità legale digitalizzata’

L’identità digitale non esaurisce la propria funzione nella mera abilitazione di servizi *online* per il cittadino, ma potrebbe essere considerata come infrastruttura giuridica idonea a garantire – o a ricostruire – l’identità legale e, per suo tramite, l’effettivo godimento dei diritti fondamentali.

In tale prospettiva si parlerebbe di ‘identità legale digitalizzata’, intesa come insieme coerente di attestazioni verificabili e opponibili *erga omnes* che consente all’individuo di essere riconosciuto quale soggetto di diritto e di partecipare alla vita civile, economica e politica su basi certe, anche quando la documentazione tradizionale sia assente, incompleta o non prontamente spendibile³⁰⁴.

La prassi amministrativa ha sinora postulato la preesistenza dell’identità legale rispetto a quella digitale: l’amministrazione accerta lo *status* secondo il diritto positivo e solo in un secondo momento lo ‘proietta’ nello spazio informatico mediante credenziali.

La trattazione propone di interrogarsi sulla dinamica inversa: se e come l’identità digitale possa concorrere a costituire identità legale per i soggetti che ne sono privi³⁰⁵. Ci si domanda inoltre quali condizioni tecniche, giuridiche e organizzative potrebbero essere adeguate affinché tale processo avvenga senza sacrificare determinate garanzie.

Il tema in questione è reso urgente da una realtà ampiamente documentata: oltre un miliardo di persone nel mondo non dispone di documenti di identità riconosciuti³⁰⁶. La platea degli interessati è composita e non omogenea – rifugiati, migranti, comunità rurali prive di registri, minoranze escluse – e accomunata da vulnerabilità ricorrenti³⁰⁷. Infatti, tale scenario si traduce nell’impossibilità di godere di diritti essenziali come il diritto all’assistenza sanitaria, all’istruzione, alla partecipazione

³⁰⁴ In questo senso V. Graf Narbel, *Digital Identity*, cit., che parla di «identità digitale come identità fondante», 221-222.

³⁰⁵ A tal proposito si parlerebbe di “identità digitale come identità fondante”. Sul punto si rinvia a V. Graf Narbel, *Digital Identity*, in *Handbook on Data Protection in Humanitarian Action*, ed. M. Marelli, Cambridge University Press, 24 ottobre 2024, 221-222.

³⁰⁶ Così quanto rilevato dalla Banca Mondiale: sul punto v. A. Beduschi, *Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights*, in *Big Data & Society*, gennaio-giugno 2019, 1-6.

³⁰⁷ A. Beduschi *et al.*, *Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for new Digital Identity Systems*, giugno 2017.

alla vita politica del proprio Paese, nonché a una maggiore esposizione al rischio di sfruttamenti e abusi. Non sorprende che le Nazioni Unite abbiano incluso tra gli obiettivi di Sviluppo Sostenibile quello di fornire un'identità legale a tutti entro il 2030³⁰⁸, compresa la registrazione delle nascite, riconoscendo di conseguenza la natura abilitante dell'identità rispetto a una pluralità di diritti e politiche pubbliche³⁰⁹. Su tali premesse, le nuove tecnologie possono divenire un potente strumento per raggiungere questo obiettivo; oggi, infatti, mediano sempre più spesso la verifica e l'identificazione dell'identità delle persone.

La mediazione tecnologica dell'identità è oggi pervasiva: come già affrontato, sistemi centralizzati pubblici, federazioni pubblico-private, credenziali biometriche, *wallet* digitali e, più di recente, soluzioni basate su registri distribuiti. Nei contesti a Stato di diritto consolidato, l'identità digitale è stata prevalentemente un abilitatore di efficienza; altrove, invece, essa costituisce condizione pregiudiziale di riconoscimento legale.

Dunque, se nelle democrazie occidentali avanzate – come l'Italia – l'identità digitale è intesa come un'opportunità per valorizzare e modernizzare l'infrastruttura pubblica; in altri Paesi il tema dell'identità digitale si inserisce in un contesto ben distinto ergendosi a strumento prodromico al riconoscimento dell'identità legale³¹⁰. In tale cornice si colloca la *Self-Sovereign Identity* (SSI)³¹¹, proposta come nuovo paradigma di identità legale digitalizzata.

³⁰⁸ Obiettivo di sviluppo sostenibile 16.9 delle Nazioni Unite, Agenda 2030.

³⁰⁹ Si rammenta che l'art. 6 della Dichiarazione Universale dei Diritti dell'Uomo così sancisce: «Ogni individuo a diritto, in ogni luogo, al riconoscimento della sua personalità giuridica». tuteli espressamente il diritto ad aver attribuita una personalità giuridica, oggi circa un quinto della popolazione globale risulta sprovvisto di un'identità legale.

³¹⁰ M.J. Casey, P. Vigna, *La macchina della verità*, cit., 277.

³¹¹ Sul tema si rinvia a C. Allen, *The Path to Self-Sovereign Identity*, 26 aprile 2016; A. Preukschat, D. Reed, *Self-Sovereign Identity*, cit.; A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, cit.; A. Mühle *et al.*, *A Survey on Essential Components of a Self-Sovereign Identity*, 17 luglio 2018; F. Schardong, R. Custódio, *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*, in *Sensors*, 22/2022;

2.1. Colmare il divario identitario con le tecnologie digitali

Le tecnologie digitali offrono strumenti innovativi per colmare il ‘divario identitario’ che ancora oggi relega oltre un miliardo di persone (tra migranti, rifugiati, apolidi e minoranze emarginate) in una condizione di invisibilità giuridica dovuta alla mancanza di documenti di riconoscimento³¹².

Organizzazioni sovranazionali e agenzie umanitarie hanno dunque avviato iniziative concrete per colmare tale *gap*: la Banca Mondiale, ad esempio, con il programma *Identification for Development* (ID4D) sostiene la diffusione di sistemi nazionali di identificazione digitale inclusivi e affidabili, allo stesso tempo l’Alto Commissariato delle Nazioni Unite per i Rifugiati (UNHCR) combina tecnologie emergenti nei campi profughi al fine di registrare milioni di rifugiati.

Sul piano teorico, si è persino avanzata l’idea che l’accesso a un’identità digitale affidabile e funzionale possa costituire un nuovo diritto fondamentale dell’individuo, aggiuntivo rispetto al tradizionale diritto alla *privacy*³¹³.

In questo contesto, tecnologie come la biometria, la *blockchain* e soluzioni ibride rivestono un ruolo chiave nel fornire riconoscimento legale a chi ne è privo³¹⁴. Programmi pionieristici (e controversi) come *Aadhaar* in India – il più grande sistema biometrico al mondo con oltre 1,2 miliardi di persone registrate attraverso impronte digitali e scansione dell’iride³¹⁵ – dimostrano come sia possibile attribuire un’identità digitale univoca a vastissime fasce di popolazione fino a quel momento prive di documenti, consentendo loro di autenticarsi.

Analogamente, nel campo rifugiati di Azraq in Giordania, il *World Food Programme* (WFP) ha realizzato una piattaforma innovativa che integra la banca dati biometrica dell’UNHCR con un registro *blockchain*.

Simili iniziative hanno dimostrato le opportunità offerte dagli strumenti digitali di identità in termini di inclusione socioeconomica e accesso ai diritti.

³¹² A. Beduschi, *Digital identity*, cit.

³¹³ C. Sullivan, *Digital Identity - An Emergent Legal Concept*, University of Adelaide Press, 2011.

³¹⁴ Sul tema si rinvia a J. Torpey, *The Invention of the Passport. Surveillance, Citizenship, and the State*, Cambridge University Press, 2018; C. Sullivan, *Digital citizenship and the right to digital identity under international law*, in *Computer Law & Security Review*, 32/2016; Id., *Digital identity. From emergent legal concept to new reality*, in *Computer Law & Security Review*, 34/2018.

³¹⁵ R. Abraham *et al.*, *State of Aadhaar Report 2017-18*, maggio 2018.

Allo stesso tempo, però, tali benefici possono essere raggiunti pienamente solo se le soluzioni adottate rispettano rigorosi *standard* di tutela dei diritti.

Il potenziale trasformativo di queste tecnologie va di pari passo con l'emergere di un nuovo paradigma di identità legale digitalizzata orientato all'autodeterminazione dell'individuo: la cosiddetta *Self-Sovereign Identity*.

In prospettiva, la SSI – su cui ci si soffermerà diffusamente in seguito – prefigura un modello in cui l'individuo è posto al centro del proprio ecosistema identitario mediante l'uso di registri distribuiti. Questi ultimi gli consentono infatti di detenere e gestire direttamente le proprie credenziali, senza dover più dipendere da un'autorità centrale per il riconoscimento³¹⁶. Si tratterebbe di un cambio di paradigma radicale: rispetto agli approcci convenzionali all'identità caratterizzati da archivi chiusi e silos di dati controllati da enti terzi.

L'identità auto-sovrana sfrutterebbe infrastrutture decentralizzate per restituire all'individuo il controllo sui propri attributi identificativi e sulle relative condivisioni. Ciononostante, l'adozione su larga scala di biometria, *blockchain* e SSI può comportare altresì significativi rischi e dilemmi etico-giuridici che è necessario bilanciare e valutare attentamente.

Un primo rischio è rappresentato dal c.d. *function creep*, ossia l'ampliamento graduale delle finalità di un sistema di identificazione oltre gli scopi inizialmente dichiarati³¹⁷, una deriva che in assenza di adeguati vincoli normativi può trasformare uno strumento di inclusione in un mezzo di sorveglianza di massa. L'esempio di *Aadhaar* è emblematico in tal senso, avendo visto estendersi nel tempo le proprie applicazioni dal settore dei sussidi pubblici all'autenticazione per servizi bancari, fiscali e telecomunicazioni, spesso in modo surrettizio³¹⁸. Ciò ha sollevato preoccupazioni sul fronte della tutela della *privacy* e del possibile utilizzo secondario dei dati personali senza consenso.

Ulteriore pericolo concerne la profilazione e la discriminazione: sistemi digitali onnipervasivi che raccolgono dati biometrici e comportamentali potrebbero facilitare l'aggregazione di informazioni sensibili e la creazione di profili dettagliati

³¹⁶ A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, cit.

³¹⁷ V. Graf Narbel, *Digital Identity*, cit., 222.

³¹⁸ R. Schroeder, *Aadhaar and the Social Credit System: Personal Data Governance in India and China*, in *International Journal of Communication*, 16/2022, 2373 ss.

su individui o gruppi vulnerabili (come minoranze etniche o rifugiati), con il rischio di perpetuare *bias* o alimentare pratiche discriminatorie.

Diviene dunque cruciale, in fase di progettazione e *governance* di queste identità digitali, adottare rigorosi principi di minimizzazione dei dati raccolti e di controllo sugli accessi, prevenendo usi impropri.

2.2. La centralizzazione e i limiti del tradizionale approccio all'identità digitale

Ad oggi l'approccio tradizionale delle istituzioni all'identità digitale non può ritenersi adeguato a perseguire gli obiettivi prefissati con riferimento alla tutela diretta e immediata dei diritti umani.

Come sottolineato da un *report* della Commissione europea³¹⁹, è possibile individuare almeno tre ordini di problemi: l'eccessiva frammentazione dell'attuale struttura dell'identità digitale, il debole collegamento tra le informazioni “*offline*” e quelle digitalizzate, e la mancanza di sicurezza dei dati dei cittadini.

Prestando particolare attenzione a quest'ultimo profilo, occorre evidenziare che gli attacchi informatici volti all'acquisizione di dati personali – *data breach* – sono sempre più frequenti e di vasta scala³²⁰.

Il caso che ha fatto comprendere a tutto il mondo l'inadeguatezza dell'approccio moderno alla gestione delle identità è emblematico: si tratta dell'attacco portato a termine nel 2018 contro *Aadhaar*, il *database* biometrico utilizzato dall'India per identificare ogni suo cittadino³²¹. Attraverso tale attacco conosciuto come «*the largest data breach in the world*», vennero sottratti i dati sensibili – nomi, numeri dei documenti e coordinate bancarie – di oltre un miliardo di persone.

Oltre alle ovvie riflessioni imposte sul piano della *cybersecurity*, esempi come questo dimostrano quanto sia arduo trovare una soluzione definitiva ai problemi evidenziati. Episodi simili non rappresentano un'eccezione isolata: negli ultimi anni

³¹⁹ European Commission, *A European Strategy for Data*, Brussels, 2020.

³²⁰ La Commissione europea, nel suo *European Digital Identity Framework Progress Report 2024*, ha segnalato come la vulnerabilità dei sistemi centralizzati di gestione dell'identità digitale costituisca una delle principali minacce alla fiducia dei cittadini, sottolineando che i *data breach* non compromettono soltanto dati sensibili, ma erodono anche la legittimità giuridica delle credenziali digitali (European Commission, 2024).

³²¹ A. Abraham *et al.*, *State of Aadhaar*, Report 2017-2018.

si sono verificati numerosi *breach* ad alto impatto che evidenziano i rischi intrinseci dei sistemi di identità centralizzati³²².

Finché la prova dell'identità richiederà la presenza di una sola entità chiamata alla raccolta delle informazioni necessarie per attestare l'identità di un individuo – lo Stato – sarà sufficiente un singolo e ben calibrato attacco per appropriarsi di dati di milioni di persone. Dunque, i principali problemi riscontrabili allo stato dell'arte sono riconducibili soprattutto alla centralizzazione del sistema di gestione dell'identità.

I limiti di tale modello accentrato non riguardano soltanto la sicurezza dei dati, ma anche – e soprattutto – la circostanza che tale modello tende a escludere larghi segmenti di popolazione globale.

Come accennato, nelle odierne strutture centralizzate restano ai margini proprio i soggetti più vulnerabili: coloro che non hanno facile accesso alle istituzioni preposte al rilascio di documenti (rifugiati, individui che si trovano in zone di guerra, residenti in Paesi in via di sviluppo privi di un'anagrafe capillare). È proprio su tali aspetti che interverrebbe la tecnologia *blockchain*. Questa tecnologia eliminando la necessaria presenza di un intermediario centrale, permetterebbe di ripensare alla radice il meccanismo finora utilizzato per certificare l'identità di un soggetto³²³.

In tale prospettiva, ogni individuo potrebbe attestare e custodire la propria identità senza la mediazione di un governo o di un'autorità unica, ma semplicemente inserendo (e validando) i propri dati identificativi all'interno di un sistema distribuito³²⁴.

³²² E. Krul *et al.*, *SoK: Trusting Self-Sovereign Identity*, in *Proceedings on Privacy Enhancing Technologies*, 3/2024, 297.

³²³ C. Allen, *The Path to Self-Sovereign Identity*, cit.

³²⁴ Si tratta di una serie di informazioni – che potrebbero essere identità digitali – registrate in blocchi. Ogni blocco è legato a quello precedente e crea una catena; ogniqualvolta viene aggiunto un nuovo blocco, tutti ricevono un aggiornamento e così tutti hanno sempre la stessa versione del registro. L'aspetto fondamentale su cui si fonda tale tecnologia è il meccanismo di consenso, ovvero, il processo attraverso il quale tutti i partecipanti della rete si accordano sulla validità delle informazioni inserite (e sulla loro inclusione nella catena). In assenza di una figura centrale di controllo, questo sistema di consenso assicura che le informazioni registrate siano corrette e accettate da tutti. Si tratta di criteri convenzionali: il fatto che il validatore sia casuale crea fiducia. Il meccanismo di consenso comunemente utilizzato è la *proof of work*, paragonabile banalmente a una gara matematica. I partecipanti – denominati minatori – utilizzano la potenza di calcolo dei loro computer per risolvere problemi complessi e il primo tra loro che arriva alla soluzione ha il diritto di aggiungere l'informazione. Altri meccanismi di consenso sono la *proof of stake*, caratterizzato dal

Tale tecnologia consente di riflettere circa una nuova ‘idea’ di identità digitale, non più fondata sul controllo unilaterale di un ente centrale, bensì su un ecosistema decentralizzato di attestazioni verificabili.

Secondo la dottrina, l’identità auto-sovrana rappresenterebbe lo strumento atto a responsabilizzare gruppi emarginati, inclusi i rifugiati, offrendo loro un’identità portabile e riconosciuta su base globale al di là dei tradizionali confini statali³²⁵.

La *blockchain* potrebbe così fungere da piattaforma universale di certificazione dell’identità, contribuendo a realizzare quel diritto all’identità legale invocato in ambito internazionale.

Una simile e potenziale infrastruttura, incentrata sull’autodeterminazione e sul controllo individuale dei dati, sarebbe in grado di garantire ad ogni persona il riconoscimento come soggetto di diritto anche al di fuori dei contesti amministrativi classici.

Senza dubbio, la *blockchain* quale forma di verifica universale dell’identità potrebbe giocare un ruolo importante nell’implementazione di un diritto personale all’identità, con una forte visione di autonomia personale e sovranità sui dati³²⁶.

La possibilità di creare un registro immutabile e gestito in modo assolutamente decentralizzato potrebbe permettere nuove applicazioni nel campo dell’identità digitale finora impensabili.

La tecnologia emergente dell’identità auto-sovrana (SSI) promette di offrire una nuova infrastruttura di identità digitale per l’era post-industriale³²⁷.

fatto che il diritto di aggiungere informazioni non si basi sulla potenza di calcolo bensì sulla quantità di moneta digitale che un partecipante possiede e mette a garanzia.

³²⁵ M. Cheesman, *Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity*, in *Geopolitics*, 27/2022, 134-159; v. anche A. Zwitter, M. Boisse-Despiaux, *Blockchain for humanitarian action and development aid*, cit.

³²⁶ P. De Filippi, A. Wright, *Blockchain and the Law: the Rule of Code*, Harvard University Press, 2018.

³²⁷ A. Preukschat, D. Reed, *Self-Sovereign Identity*, cit.

2.3. Il nuovo paradigma dell'identità digitale auto-sovrana

L'identità digitale auto-sovrana³²⁸ – attraverso la tecnologia *blockchain* – si propone quale forma di certificazione universale dell'identità, utile per creare un registro globale e immune da manomissioni di dati personali di importanza vitale³²⁹. L'adozione di modelli identitari fondati sulla logica auto-sovrana evidenzia vantaggi che, sia sul piano teorico sia applicativo, si presentano con particolare evidenza.

In primo luogo, il paradigma in questione consente un rafforzamento del controllo individuale sui dati personali, coerentemente con i principi di autodeterminazione informativa già affermati dal diritto europeo in materia di protezione dei dati.

In tal senso, la gestione delle credenziali digitali attraverso *wallet* personali consente all'utente di selezionare puntualmente quali attributi condividere e con quali soggetti, realizzando una forma di *data minimization by design* che appare difficilmente raggiungibile attraverso altri modelli di gestione identitaria³³⁰.

In secondo luogo, la SSI offre un potenziale significativo di *empowerment* per i gruppi vulnerabili, tradizionalmente esclusi dai circuiti formali dell'identificazione legale. Rifugiati, apolidi o persone residenti in Stati privi di anagrafe efficiente potrebbero infatti vedersi riconosciuta un'identità digitale anche in assenza dei tradizionali documenti statali. Ne consegue una prospettiva di inclusione giuridica e sociale che si allineerebbe con il già citato obiettivo dell'Agenda 2030 delle Nazioni Unite.

Un ulteriore beneficio è rappresentato dal valore inclusivo della SSI, che può fungere da strumento per ridurre il c.d. *identity divide*.

³²⁸ John Edge, già banchiere e imprenditore nel settore delle tecnologie finanziarie, nel 2016 fondò l'organizzazione ID2020 con l'obiettivo di garantire un'identità digitale sicura a tutti gli individui privi di documenti ufficiali, in particolare i minori. L'iniziativa, sostenuta in collaborazione con le Nazioni Unite, si propose inizialmente di raggiungere tale risultato entro il 2020, termine poi esteso al 2030 in coerenza con l'Agenda ONU per lo sviluppo sostenibile (obiettivo 16.9). Durante un convegno organizzato presso le Nazioni Unite, la tensione emersa tra rappresentanti governativi e tecnologi mise in luce la contrapposizione fra la concezione tradizionale dell'identità come prerogativa dello Stato e l'idea innovativa di "auto-sovrana" dell'identità, intesa come capacità dell'individuo di attestare e gestire autonomamente i propri attributi personali.

³²⁹ M.J. Casey, P. Vigna, *La macchina della verità*, cit., 278.

³³⁰ R. Soltani, U.T. Nguyen, A. An, *A Survey of Self-Sovereign Identity Ecosystem*, cit., 2021.

Nei contesti in cui l'accesso a servizi essenziali – sanitari, educativi, finanziari – dipende dall'esistenza di un'identità legalmente riconosciuta, la possibilità di attestare la propria esistenza giuridica tramite credenziali decentralizzate assume la funzione di diritto abilitante che permette l'effettivo godimento di una pluralità di diritti fondamentali³³¹.

Infine, la dimensione della sicurezza cibernetica costituisce un ulteriore punto di forza: sebbene il *ledger* distribuito non elimini in assoluto la vulnerabilità, esso ne ridimensiona l'impatto, evitando che una singola violazione possa compromettere milioni di identità³³².

Su tali premesse, l'identità digitale auto-sovrana non è da intendersi soltanto come un'evoluzione sul piano tecnologico, ma come una riconfigurazione giuridica del rapporto tra individuo, Stato e mercato, nella quale l'utente diviene soggetto attivo, custode delle proprie informazioni personali.

Un nodo cruciale del dibattito sulla *Self-Sovereign Identity* (SSI) riguarda la scelta dell'infrastruttura tecnologica sottostante. Se l'identità digitale auto-sovrana nasce con l'intento di superare i limiti del modello centralizzato – caratterizzato dalla concentrazione di dati in registri unici e vulnerabili – occorre tuttavia interrogarsi su quale tipologia di *blockchain* sia più adatta a reggere un sistema di gestione dell'identità che aspiri ad essere al tempo stesso universale, sicuro ma conforme ai principi giuridici fondamentali.

Le *blockchain permissionless* e pubbliche – come Bitcoin o Ethereum³³³ – garantiscono la massima apertura e portabilità: chiunque può accedere alla rete e partecipare al processo di validazione. Tale architettura, almeno in astratto, realizzerebbe pienamente la visione di un'identità “senza frontiere”, opponibile ovunque e non dipendente da un'autorità centrale.

³³¹ A. Beduschi, *Digital Identity*, cit.

³³² P. Dunphy, L. Garratt, F.A.P. Petitcolas, *Decentralizing Digital Identity: Open Challenges for Distributed Ledgers*, in *2018 IEEE European Symposium on Security and Privacy Workshops*, 2018, 75 ss.

³³³ Bitcoin ed Ethereum rappresentano due esempi paradigmatici di *blockchain permissionless* e pubbliche: la prima, introdotta da Satoshi Nakamoto nel 2008 ha inaugurato l'uso di registri distribuiti per transazioni crittografiche senza intermediari; la seconda, lanciata nel 2015, ha esteso tale modello introducendo gli *smart contract* e piattaforme programmabili, ponendo le basi per l'odierna economia decentralizzata.

Tuttavia, proprio l'immutabilità e la trasparenza radicale che contraddistinguono queste reti pongono seri problemi di compatibilità con la tutela dei dati personali e con il diritto all'oblio sancito dal GDPR³³⁴. Una registrazione identitaria resa in maniera permanente e pubblicamente accessibile potrebbe infatti tradursi in un controllo pervasivo della vita dell'individuo, vanificando l'aspirazione all'autodeterminazione che SSI intende promuovere.

All'opposto, le *blockchain permissioned* e private garantiscono un controllo più puntuale, consentendo di limitare l'accesso e la scrittura nel registro a soggetti selezionati. Questa soluzione offre indubbi vantaggi in termini di conformità regolatoria e *accountability*, rendendo più semplice attribuire responsabilità giuridiche ai validatori³³⁵. D'altra parte, il rischio è che tale modello riproduca le stesse logiche di accentramento proprie dei sistemi tradizionali, con la conseguente dipendenza dagli attori che governano l'accesso e il pericolo di escludere intere fasce di popolazione prive di riconoscimento statale o di rapporti con i grandi operatori di mercato³³⁶.

Per questo, la dottrina più avvertita e alcuni esperimenti internazionali sembrano convergere verso una soluzione ibrida o *public-permissioned*. In questo modello l'uso della rete è pubblico e aperto (così da garantire interoperabilità, inclusione e portabilità transnazionale), ma il processo di validazione è riservato a un numero selezionato di soggetti accreditati (istituzioni pubbliche, università, enti certificatori, organizzazioni internazionali). Tale configurazione consente di coniugare l'apertura globale con un adeguato grado di responsabilità giuridica: i validatori sono identificati, sottoposti a regole di *governance* e sanzionabili in caso di abuso, mentre i dati personali non vengono scritti in chiaro sulla *blockchain*, ma restano nella disponibilità esclusiva dell'individuo, custoditi nel proprio *wallet*³³⁷. L'adozione di un modello ibrido permette dunque di contemperare esigenze contrapposte: da un lato, garantire la sovranità dell'individuo sui propri dati e la possibilità di esercitare i propri diritti fondamentali in chiave digitale; dall'altro, assicurare che l'infrastruttura identitaria non diventi terreno di anarchia

³³⁴ Cfr. M. Finck, *Blockchains and data protection in the European Union*, in *European Data Protection Law Review*, 4(1), 2018, 17 ss.; A. Beduschi, *Digital identity*, cit.

³³⁵ R. Soltani, U. T. Nguyen, A. An, *A survey of Self-Sovereign Identity ecosystem*, cit.

³³⁶ P. Dunphy, L. Garratt, F.A.P. Petitcolas, *Decentralizing Digital Identity*, cit.

³³⁷ A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity*, cit.

tecnologica, ma si regga su un quadro regolatorio giuridico-istituzionale capace di garantire affidabilità, sicurezza e inclusione.

In tal senso, l'ibridazione si rivela la via più coerente con la natura della SSI: non semplice innovazione tecnica, ma vera e propria riconfigurazione giuridica dei rapporti tra attori³³⁸.

Nel quadro sinora prospettato il controllo sui dati non è più monopolio esclusivo dell'autorità centrale, né affidato a una rete completamente anonima, bensì esercitato in un contesto regolato, multilaterale che tutela sia l'autonomia personale sia gli interessi collettivi di sicurezza e giustizia³³⁹.

2.4. L'identità digitale auto-sovrana nell'ottica della tutela dei diritti umani: sfide e prospettive

Le organizzazioni sovranazionali e i documenti ufficiali hanno in più occasioni messo in evidenza il potenziale della *Self-Sovereign Identity* quale infrastruttura di identità di nuova generazione.

L'Unione europea sta esplorando l'integrazione dei principi della SSI nel proprio quadro normativo, mentre rapporti della Banca Mondiale e del *World Economic Forum* ne hanno sottolineato la dimensione sociale e politica, quale strumento idoneo a fornire riconoscimento affidabile a vasti segmenti di popolazioni attualmente privi di identità legale³⁴⁰. Segnatamente, l'idea di impiegare la tecnologia *blockchain* in ambito identitario è nata inizialmente proprio per affrontare emergenze di natura umanitaria.

Il primo esperimento di rilievo è stato condotto nel campo profughi siriano di Azraq, in Giordania, dove dal 2017 il *World Food Programme* (WFP) ha avviato il progetto *Building Blocks*. L'iniziativa ha integrato *blockchain* e sistemi di riconoscimento

³³⁸ V. A. Bazarhanova, K. Smolander, *The Review of Non-Technical Assumptions in Digital Identity Architectures*, in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, 6408 ss. Il confronto empirico condotto da Bazarhanova dimostra come le scelte architetturali incidano profondamente sugli equilibri di *governance*. Dai casi oggetto di analisi emerge come la tecnologia *blockchain* non sostituisca automaticamente i modelli tradizionali, ma piuttosto li ibrida, fungendo da leva per ridisegnare i rapporti tra Stato, mercato e individuo.

³³⁹ F. Glaser, *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis*, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 1543 ss.

³⁴⁰ A. Giannopoulou, *Digital Identity Infrastructures*, cit.

biometrico consentendo ai rifugiati siriani di ottenere sostentamento alimentare attraverso la semplice scansione oculare, in assenza di documenti tradizionali o denaro contante ³⁴¹. Tale esperienza ha permesso non soltanto di prevenire abusi nella distribuzione degli aiuti, ma anche di realizzare un modello efficiente di gestione decentralizzata dell'identità, dimostrando come l'infrastruttura auto-sovrana possa essere funzionale alla tutela dei diritti fondamentali³⁴².

Il caso di Azraq ha rivelato, inoltre, una dimensione ulteriore. I campi profughi sono a corto di 'capitale sociale' – come definito dai politologi – inteso come reti di relazioni e legami di fiducia consolidatisi nel tempo che consentono alle comunità di funzionare e interazioni sociali³⁴³.

In termini generali, il capitale sociale designa l'insieme delle risorse relazionali e comunitarie a cui gli individui attingono per perseguire i propri obiettivi. Nei contesti di fuga forzata e sfollamento, esso assume una valenza cruciale: oltre alla perdita dei beni materiali, i rifugiati vedono spesso smarrite le prove della propria identità, i titoli di studio e le referenze lavorative, oltre alle reti di relazioni costruite nel tempo. Un sistema di identità digitale auto-sovrana applicato ai contesti umanitari potrebbe dunque rappresentare uno strumento di riscatto, trasformando dati personali certificati in risorse attivabili. In tal modo, l'identità digitale diverrebbe veicolo di ricostruzione del capitale sociale perduto.

Parallelamente alle sperimentazioni in ambito umanitario, il paradigma della SSI mostra la sua potenziale portata anche in altri settori, dal settore pubblico a quello educativo fino al settore sanitario, delineandosi come un modello capace di garantire all'individuo un controllo effettivo sui propri dati.

Nel settore sanitario, ad esempio, l'identità digitale auto-sovrana (SSI) potrebbe essere impiegata per garantire effettività al diritto alla salute e alla protezione dei dati personali. I *database* clinici, frammentati e non interoperabili, rendono difficile

³⁴¹ Ogni transazione è stata tracciata su un libro mastro immutabile gestito dal *World Food Programme* e interconnesso al *database* biometrico dell'UNHCR con benefici in termini di efficienza amministrativa, tracciabilità degli aiuti e prevenzione delle frodi.

³⁴² Ricostruzione di un'identità opponibile a terzi anche in assenza di titoli statali tradizionali. V. Thomson Reuters Foundation, *In Jordan, refugees scan irises to collect aid. But is it ethical?* (13 dicembre 2022), sul funzionamento e sulle questioni etiche (consenso, uso dei dati).

³⁴³ Si rinvia alla letteratura sul capitale sociale, in particolare a R.D. Putnam, *Bowling Alone. The Collapse and Revival of American Community*, New York, 2000; P. Bourdieu, *The Forms of Capital*, New York, 1986, sul capitale sociale inteso come risorsa relazionale attivabile da reti di fiducia e cooperazione.

per il cittadino avere una visione unificata della propria ‘storia sanitaria’³⁴⁴. Con soluzioni basate su SSI, ogni paziente potrebbe conservare in un eventuale portafoglio digitale informazioni mediche rilasciate dai vari enti sanitari (dati anagrafici, vaccinazioni, referti, prescrizioni) e decidere di volta in volta quali condividere e con chi. Ciò garantirebbe la riduzione di errori clinici e la tutela della riservatezza, poiché i dati resterebbero sotto il controllo diretto dell’individuo, evitando concentrazioni in archivi centralizzati vulnerabili a violazioni. Inoltre, sistemi SSI possono abilitare forme avanzate di consenso informato digitale, consentendo al paziente di revocare o limitare in qualsiasi momento l’accesso ai propri dati, in linea con i principi del GDPR.

Analogamente, il settore dell’istruzione rappresenta un campo privilegiato per l’applicazione della SSI. Attraverso tale tecnologia, scuole, università ed enti di certificazione potrebbero rilasciare diplomi e certificazioni digitali come credenziali verificabili, firmate crittograficamente e annesse all’identità digitale dell’individuo. Tali attestati, immediatamente condivisibili e difficilmente falsificabili, semplificherebbero l’accesso a opportunità di studio e di lavoro in altri Paesi, come mostrato da progetti pilota dell’*European Blockchain Services Infrastructure* (EBSI) per le lauree digitali, che dal 2021 coinvolgono oltre dieci Stati membri³⁴⁵.

Tuttavia, la tecnologia non costituisce una soluzione ‘onnicomprensiva’: le sue caratteristiche qualificanti – trasparenza, immutabilità e decentralizzazione – se assunte in maniere acritica e in assenza di adeguati bilanciamenti, entrano in frizione con i diritti fondamentali consolidati.

L’immutabilità, se da un lato garantisce la stabilità e l’affidabilità delle registrazioni, dall’altro può precludere l’esercizio effettivo di prerogative quali il diritto alla rettifica e alla cancellazione dei dati personali, riconosciuti dal GDPR

³⁴⁴ A. Siqueira, A. F. Da Conceição, V. Rocha, *Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review*, in *ACM Comput. Surv.* 1, 1/2021, 1 ss. Il documento analizza in modo sistematico come le tecnologie *Blockchain* e le identità auto-sovrane possano essere applicate alle soluzioni sanitarie, in particolare alla gestione delle cartelle cliniche elettroniche. V. anche A. Azaria *et al.*, *MedRec: Using blockchain for medical data access and permission management*, in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, 25 ss.

³⁴⁵ Sui progetti pilota EBSI avviati dal 2021 e coinvolgenti oltre una decina di Stati membri, v. *European Commission & European Blockchain Partnership*, 2021.

agli articoli 16 e 17. Analogamente, la trasparenza, intesa come garanzia di *accountability* dei sistemi, può comportare indebite forme di esposizione di dati sensibili; mentre la decentralizzazione, benché rappresentata come superamento del potere centralizzato, non assicura di per sé una reale distribuzione del potere, potendo anzi favorire nuove concentrazioni oligopolistiche³⁴⁶.

A queste criticità se ne affiancano almeno altre due, di natura trasversale.

In primo luogo, il *digital divide*: competenze, connettività e accesso a dispositivi sicuri non sono uniformemente distribuiti e possono trasformare la SSI in uno strumento selettivo. I dati Eurostat mostrano che nel 2023 solo il 56% degli europei (16-74 anni) possedeva competenze digitali almeno di base, ben al di sotto del *target* dell'80% fissato dalla “*Digital Decade*” per il 2030: la carenza risulta più marcata tra anziani, disoccupati e con riferimento ad alcuni Stati membri, con evidenti implicazioni per l'accesso a credenziali digitali e *wallet* di nuova generazione.

Ulteriore aspetto da tenere in considerazione concerne la dimensione sociale dell'accettazione. Diversi studi qualitativi e quantitativi hanno infatti evidenziato che la disponibilità ad adottare sistemi SSI da parte di cittadini e organizzazioni è condizionata da una combinazione di fattori tecnologici, organizzativi e culturali.

In primo luogo, emerge con forza il tema della fiducia. Gli utenti tendono ad accettare una tecnologia di identità solo se percepiscono affidabilità tanto nelle soluzioni tecniche quanto negli attori che ne compongono l'ecosistema. Ciò implica la necessità di modelli di *governance* trasparenti e condivisi, capaci di ridurre i timori legati a un uso improprio delle credenziali o a possibili squilibri di potere all'interno delle reti di validatori³⁴⁷.

Un secondo elemento riguarda l'usabilità. La complessità dei *wallet* SSI o la difficoltà di comprendere concetti come *Decentralized Identifiers* e *Verifiable Credentials* possono costituire ostacoli significativi all'adozione.

³⁴⁶ P. Dunphy et al., *Decentralizing Digital Identity: Open Challenges for Distributed Ledgers*, in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2018, 75 ss.

³⁴⁷ M. Friedewald, A. Papageorgiou, *Factors influencing the adoption of self-sovereign identity: A qualitative analysis*, in *Proceedings of the 56th Hawaii International Conference on System Sciences*, 2023.

È stato osservato che gli utenti comuni raramente percepiscono immediatamente un vantaggio concreto in termini di maggiore controllo sui propri dati; al contrario, ciò che ne determina la scelta è spesso la semplicità d'uso e la possibilità di integrare agevolmente la tecnologia nelle pratiche quotidiane³⁴⁸.

La percezione del controllo sui dati personali costituisce un ulteriore nodo critico. Se da un lato la SSI promette di restituire all'individuo la titolarità delle informazioni, dall'altro la ricerca empirica mostra come la maggioranza degli utenti non riconosca spontaneamente questa caratteristica come un beneficio reale.

Alcuni autori hanno parlato di una vera e propria “chimera del controllo”, sottolineando come, senza un adeguato quadro giuridico – ad esempio quello offerto dal GDPR – la SSI rischi di trasformarsi in uno strumento di *over-disclosure*, cioè in un meccanismo che incentiva la condivisione di più dati del necessario³⁴⁹.

In assenza di casi d'uso concreti e interoperabili, il valore percepito della tecnologia resta limitato, ostacolandone l'accettazione sociale³⁵⁰.

³⁴⁸ T. Guggenberger, A. Rieger, A. Wenninger, *Accept Me as I Am or See Me Go: A qualitative analysis of user acceptance of SSI applications*, in *Proceedings of the 56th Hawaii International Conference on System Sciences*, 2023.

³⁴⁹ F. Metzger, N. Martin, *The chimera of control: Perceptions of data control in self-sovereign identity systems*, *Human Technology*, 2/2024, 183 ss.

³⁵⁰ M. Kubach *et al.*, *Social acceptance of self-sovereign identity: Empirical findings and implications*, in *Computers*, 11(3), 45, 2022.

3. Conclusioni. Il futuro dell'identità digitale tra realtà e mito

Le analisi svolte in questa sede – maturate all'intersezione tra ricostruzione concettuale, inquadramento socio-istituzionale e tutela dei diritti – hanno inteso misurarsi con le sfide inedite che l'identità digitale pone nell'ordinamento contemporaneo.

Pur strettamente legata all'identità personale, la multidimensionalità dell'identità digitale presenta tratti autonomi e profili problematici specifici. I dati che la compongono si formano e circolano spesso al di fuori della piena consapevolezza dell'interessato, dando luogo a una 'proliferazione' di attributi che non sempre coincidono con l'identità reale e che, talvolta, sono raccolti e aggregati senza un consenso pienamente informato.

Quanto messo in evidenza ha permesso di mettere a fuoco alcune questioni cruciali sul rapporto tra la costruzione libera della propria personalità in rete e le influenze – spesso opache – esercitate da piattaforme e algoritmi, incidendo sui diritti fondamentali, dal diritto all'identità al diritto all'oblio.

Un altro snodo concettuale affrontato riguarda i modelli di gestione dell'identità digitale. Il lavoro ha individuato essenzialmente tre paradigmi, distinti per il grado di centralizzazione e per il ruolo di Stato e privati: modelli federati, centralizzati e decentralizzati. Lo studio comparativo di questi modelli ha messo in evidenza l'impossibilità di individuare una soluzione perfetta: ogni architettura identitaria richiede compromessi tra efficienza, sicurezza, *privacy* e controllo dell'utente.

In questo senso, un bilanciamento ideale tra tali elementi si ritiene già esistente nel diritto UE vigente: nella prospettiva del Regolamento eIDAS 2 lo Stato permane *trust anchor* degli attributi qualificati (identità anagrafica, *status* e poteri), ne garantisce qualità, validità e tutela; al contempo, l'utente custodisce e presenta le proprie credenziali tramite *wallet* sotto il suo controllo. In tale architettura, non solo l'equilibrio tra *accountability* e autodeterminazione si ricostituisce, ma si riducono le asimmetrie informative e il rischio di sorveglianza tipico dei modelli centralizzati o federati, senza sacrificare la spendibilità legale delle identità nei rapporti pubblici e privati.

Resta, tuttavia, un dato di fondo che ha attraversato l'intera analisi: almeno per ora, non è possibile immaginare di sganciare il concetto di identità in senso tecnico-giuridico (in tutte le sue varianti) dal concetto di Stato-nazione.

L'idea di *Self-Sovereign Identity* può considerarsi senz'altro rivoluzionaria sul piano propriamente operativo, ma la custodia delle credenziali, il riconoscimento, la responsabilità e il rimedio non possono che rimanere ancorati a un ordinamento pubblico che attribuisce valore, disciplina i conflitti, assicura la revoca e sanziona gli abusi. Fuori da questa cornice, l'identità digitale rischia di perdere efficacia giuridica e affidabilità sociale.

Nel corso della ricerca si è altresì esaminato l'impatto delle tecnologie emergenti (intelligenza artificiale, biometria e *blockchain*) sull'evoluzione dell'identità digitale, constatando come abbiano aperto nuove opportunità ma anche inedite criticità.

La tecnologia *blockchain*, infine, è stata approfondita come infrastruttura per l'identità decentralizzata: l'uso di registri distribuiti e di *standard* come gli identificatori decentralizzati e le credenziali verificabili mira a garantire immutabilità e sicurezza crittografica nell'attestazione di attributi identitari.

Tuttavia, sono emerse anche in questo ambito importanti criticità.

Anzitutto, le piattaforme *blockchain* pubbliche presentano problemi di scalabilità e costi che ne limitano l'uso su larga scala; inoltre, è stato sottolineato il problema dell'interoperabilità tra diversi ecosistemi (*standard* eterogenei possono impedire il riconoscimento reciproco delle credenziali).

Una questione cruciale è poi quella della *governance*: per sua natura la *blockchain* manca di meccanismi chiari di responsabilità e controllo, il che complica la gestione delle identità in caso di errori o necessità di revoca. Paradossalmente, l'assenza di un'autorità centrale rende difficile stabilire regole condivise e conduce spesso al ricorso a nuovi intermediari di fatto (ad esempio gestori di *wallet*) non sottoposti ad alcun regolatore.

Queste considerazioni suggeriscono che l'innovazione tecnologica, da sola, non basta: perché le soluzioni identitarie emergenti siano sostenibili e rispettose dei diritti, esse vanno accompagnate da adeguati *framework* normativi.

Un problema rilevato in tutti questi ambiti è la tensione continua tra autonomia informativa dell'individuo e istanze di sorveglianza e controllo. Da un lato, i sistemi di identità digitale di nuova generazione (soprattutto quelli decentralizzati) aspirano a restituire all'utente il pieno governo dei propri dati personali, riducendo la dipendenza da grandi piattaforme centralizzate e limitando ingerenze di terzi. Dall'altro lato, se implementate in modo invasivo, le identità digitali possono diventare potenti strumenti di tracciamento delle attività dei cittadini.

In questo contesto, la tesi ha rivolto un particolare sguardo critico all'evoluzione del paradigma dell'identità digitale auto-sovrana e al perché l'entusiasmo iniziale verso di esso sembrerebbe recentemente in calo.

Benché l'SSI incarnasse l'ideale di un'identità pienamente controllata dall'individuo, libera da intermediari, diversi fattori ne stanno frenando la diffusione su larga scala. In primo luogo, emergono significative barriere tecnico-sociali: la gestione di credenziali decentralizzate richiede competenze e strumenti non banali (portafogli digitali, chiavi crittografiche, ecc.), creando un serio problema di usabilità per l'utente medio.

In secondo luogo, la mancanza di un ecosistema maturo limita l'utilità pratica percepita dell'SSI. Affinché un'identità decentralizzata abbia valore, deve essere ampiamente riconosciuta e accettata da servizi sia pubblici sia privati (enti governativi, banche, datori di lavoro, *provider online*); tuttavia, l'adozione istituzionale di *standard* SSI e di credenziali verificabili è ancora limitata.

Di conseguenza, molti considerano le credenziali auto-sovrane come un complemento – non un sostituto – dei tradizionali documenti d'identità e profili digitali esistenti.

In conclusione, dalle riflessioni condotte emerge l'impossibilità – almeno allo stato attuale – di concepire un'identità digitale pienamente slegata dall'intermediazione statale.

Per quanto si immagini un futuro in cui ogni individuo possa attestare la propria identità in maniera del tutto autonoma, l'esperienza odierna mostra che l'identità, per essere effettiva e riconosciuta, mantiene un nesso costitutivo con l'autorità pubblica e con l'ordinamento giuridico.

Del resto, gli Stati hanno storicamente il ruolo di garanti dell'identità (basti pensare all'anagrafe, ai registri civili, ai documenti ufficiali) e non sono disposti a rinunciare facilmente a questo potere che attiene alla sovranità e al controllo sociale.

Inoltre, come si è argomentato, la spendibilità pratica di qualsiasi attestazione identitaria dipende dal riconoscimento da parte di terzi; anche l'identità più 'autogestita' deve in ultima analisi essere riconosciuta e validata da entità esterne (Stati, istituzioni sovranazionali, organizzazioni private) per acquisire valore legale e sociale.

Alla luce di ciò, più che vagheggiare un'identità del tutto priva di Stato, occorre immaginare modelli di cooperazione tra attori pubblici e privati: modelli in cui l'autorità pubblica continui a svolgere una funzione di garanzia (in termini di certificazione, tutela dei diritti, inclusività) e al contempo l'individuo venga posto realmente al centro del controllo e della gestione dei propri dati personali.

In altri termini, l'identità digitale del prossimo futuro tenderà verosimilmente a una forma ibrida, dove elementi di auto-sovranià individuale e intervento statale coesistono e si bilanciano. Anche nell'era della decentralizzazione, dunque, l'identità rimane ancorata a una dimensione relazionale e pubblica: per quanto digitalizzata e distribuita, essa trova significato e tutela solo all'interno di un quadro istituzionale che ne riconosce la validità.

In chiusura, è necessaria una precisazione che delimiti l'ambito di validità dell'argomentazione: l'ipotesi di un'identità digitale interamente autogestita e priva di intermediazione pubblica risulta plausibile solo in contesti eccezionali, ovvero in situazioni caratterizzate dall'assenza di uno Stato funzionale o dalla carenza di istituzioni di riferimento. Basti pensare ai territori contraddistinti da sovranità fragile, a casi di fallimento istituzionale o a scenari di emergenza umanitaria. In simili circostanze, comunità internazionali, organizzazioni intergovernative ed enti non statali sono spesso chiamati a supplire temporaneamente alle funzioni tipicamente esercitate dallo Stato.

Tuttavia, si deve riconoscere che anche in scenari tanto eccezionali una soluzione identitaria completamente autogestita avrebbe carattere meramente provvisorio e presenterebbe limiti intrinseci sotto il profilo del riconoscimento giuridico.

La precarietà di tale soluzione conferma, in ultima analisi, che la (ri)istituzionalizzazione rimane l'esito auspicabile.

Bibliografia

- Abraham A. *et al.*, *State of Aadhaar*, Report 2017-2018.
- Alaimo A.M., *Il Regolamento sull'Intelligenza Artificiale. Un treno al traguardo con alcuni vagoni rimasti fermi*, in *federalismi.it*, 25/2024, 231 ss.
- Alexander M., *A survey on essential components of a selfsovereign identity*, in *Computer Science Review*, vol. 30, 80 ss., 2018.
- Allegri M.R., *Il diritto di accesso a Internet: profili costituzionali*, in *MediaLaws*, 11 aprile 2021.
- Allegri M.R., *Il diritto di accesso a Internet: profili costituzionali*, in *MediaLaws*, 1/2021, 67 ss.
- Allen C., *The Path to Self-Sovereign Identity*, 26 aprile 2016.
- Alpa G., Andenas M., *L'Europa dei diritti e i diritti fondamentali*, in Alpa G., Andenas M. (a cura di), *Fondamenti del diritto privato europeo*, Milano, 2005, 53 ss.
- Alpa G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 3/2017, 723-724.
- Alpa G., *Il diritto di essere sé stessi*, Milano, 2021.
- Alu A., *Il doppio volto di Internet tra l'accesso e l'uscita e il paradosso della "trappola" digitale*, in *Dir. fam. pers.*, 2/2023, 626 ss.
- Amirante C., voce *Cittadinanza (teoria generale)*, in *Enc. dir.*, vol. VI, Roma, 2003, 1 ss.
- Amoretti F., Gargiulo E., *Dall'appartenenza materiale all'appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, in *Pol. dir.*, 3/2010, 353 ss.
- Arena G., *Il principio della sussidiarietà orizzontale nell'art. 118, u.c., della Costituzione*, in *Studi in onore di Giorgio Berti*, Napoli, 2005, 217 ss.
- Aroldi P., Zaffaroni L., Cino D., *Il primo lockdown e l'avvio della DAD come banco di prova dei processi di digitalizzazione nella scuola italiana, tra disuguaglianze e inclusione*, in *Sociologia della comunicazione*, 2/2021, 69 ss.
- Attewell P., *The First and Second Digital Divides*, in *Sociology of Education*, 3/2001, 252 ss.

- Azaria A. et al., *MedRec: Using blockchain for medical data access and permission management*, in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, 25 ss.
- Azzariti G., *La cittadinanza. Appartenenza, partecipazione, diritti delle persone*, in *Dir. pubbl.*, 1/2011, 425 ss.
- Baldini D., *The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet*, in *Italian Journal of Public Law*, 1/2024, 297 ss.
- Barbera A., “Nuovi diritti”: *attenzione ai confini*, in Califano L. (a cura di), *Corte costituzionale e diritti fondamentali*, Torino, 2004.
- Bardino N., *Rapporti con la pubblica amministrazione e identità e domicilio digitali*, in Ciriello A., Maugeri M. (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 26 ss.
- Bauman Z., *Intervista sull'identità*, Roma-Bari, 2003.
- Bauman Z., Lyon D., *La sorveglianza nella modernità liquida*, Roma-Bari, 2015.
- Bavetta G., (voce) *Identità (diritto alla)*, in *Enc. dir.*, XIX, Milano, 1979.
- Bay M., *What is Cybersecurity? In search of an encompassing definition for the post-Snowden era*, in *French journal for media research*, 6/2016, 1 ss.
- Beduschi A. et al., *Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for new Digital Identity Systems*, giugno 2017.
- Beduschi A., *Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights*, in *Big Data & Society*, gennaio-giugno 2019, 1 ss.
- Bentham J., *Panopticon ovvero la casa d'ispezione*, Venezia, 1983, 1997.
- Bentivegna S., *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Roma-Bari, 2009.
- Benvenuti M., *Diritti sociali*, Milano, 2013.
- Berti G., *Cittadinanza, cittadinanze e diritti fondamentali*, in *Riv. dir. cost.*, 1997, 3 ss.
- Bin R., *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992.

- Birch D., *Identity is the New Money*, London Publishing Partnership, 2004.
- Biscottini G., voce *Cittadinanza*, in *Enc. dir.*, vol. VII, Roma, 1960, 140 ss.
- Boden M.A., *L'Intelligenza Artificiale*, Bologna, 2019, 119 ss.
- Bonavita S., *Il corpo elettronico*, in Cassano G., Previti S. (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020.
- Bonneau J. et al., *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, in *IEEE Symposium on Security and Privacy*, 2015.
- Bontempi V. (a cura di), *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, 2022.
- Borg A., *Prefazione*, Basile A. (a cura di), *Blockchain la nuova rivoluzione industriale*, Palermo, 2019.
- Bourdieu P., *The Forms of Capital*, New York, 1986.
- Bradley J., Hill B., Sakimura N., *Identity Management Using a Centralized Authority. In Proceedings of the 2014 IEEE International Conference on Identity*, in *Security and Behavior Analysis (ISBA)*, Hong Kong, 14-18 luglio 2014, 1 ss.
- Cadamuro E., *Le nuove sfide per la tutela dei dati biometrici nella costruzione dell'identità digitale: tra istanze europee e sistema nazionale*, in *Riv. trim. dir. pen. econ.*, 3-4/2024, 364 ss.
- Calvano R., *L'istruzione, il Covid-19 e le diseguaglianze*, in *Costituzionalismo.it*, 3/2020, 79 ss.
- Caporale M., *Dalle smart cities alla cittadinanza digitale*, in *federalismi.it*, 2/2020, 30 ss.
- Capoti D., Colacchi E., Maggioni M., *Bitcoin Revolution: la moneta digitale alla conquista del mondo*, Milano, 2015.
- Cardarelli F., *Amministrazione digitale, trasparenza e principio di legalità*, in *Il Dir. inf.*, 2/2015, 227.
- Cardon D., *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Milano, 2016.
- Caridà R., *I diritti di cittadinanza inclusiva tra esigenze di sicurezza e doveri di solidarietà*, in *federalismi.it*, 14/2017.
- Carlone E. (a cura di), *Codice dell'amministrazione digitale*, Rimini, 2005.

- Carloni E., *La riforma del Codice dell'amministrazione digitale*, in *Giorn. dir. amm.*, 2011, 469 ss.
- Carotti B., *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giorn. dir. amm.*, 1/2017, 7 ss.
- Carotti B., *Il correttivo al Codice dell'amministrazione digitale: una meta-riforma*, in *Giorn. dir. amm.*, 2/2018, 131 ss.
- Carotti B., *Le finzioni dell'intelligenza senza corpo, o dell'“AI Act”*, in *Giorn. dir. amm.*, 1/2025, 31 ss.
- Carretero J. *et al.*, *Federated identity architecture of the European eID System*, in *IEEE Access*, 6/2018, 75302 ss.
- Cartabia M., *Cittadinanza europea*, in *Enc. giur. Treccani*, vol. VI, Roma, 1995.
- Casey M.J., Vigna P., *La macchina della verità. La blockchain e il futuro di ogni cosa*, Milano 2018.
- Cassese S., *Il cittadino e l'amministrazione pubblica*, in *Riv. trim. dir. pubbl.*, 1998, 1015 ss.
- Cavallaro M.C., *Intelligenza artificiale, interesse pubblico e complessità della scelta amministrativa*, in *Amministrativamente*, 3/2024, 936 ss.
- Cavallo Perin R., Galetta D.U. (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020.
- Cavallo Perin R., *La configurazione della cittadinanza amministrativa*, in *Dir. amm.*, 1/2004, 201 ss.
- Cavani V., *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in *Dir. pubbl. comp.*, 1/2023, 223 ss.
- Cerf V., *Internet Access is not a Human Right*, in *The New York Times*, 4 gennaio 2012.
- Chadwick D.W., *Federated identity management*, in *Foundations of Security Analysis and Design*, Springer, 2009, 96 ss.
- Cheesman M., *Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity*, in *Geopolitics*, 27/2022, 134 ss.
- Cheng H.K., Subhaiyoti B., Hong G., *The debate on net neutrality: a policy perspective*, in *Information system research*, 1, 2011, 60 ss.

- Cheung A.S.Y., Chen Y., *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, in *Law & Social Inquiry*, vol. 47, 4, 1137 e ss.
- Chierici M., *La "blockchain": una lettura giuridica per uno sguardo verso il futuro*, in *Cyberspazio e diritto*, 3/2018, 385 ss.
- Citino Y., *Cittadinanza "a punti" e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, in *Dir. comp.*, 22 giugno 2022.
- Citron D.K., Solove D., *Risk and Anxiety: A Theory of Data Breach Harms*, in *Texas Law Review*, 96(4), 2018, 737 ss.
- Clarke R., *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, 1988, 498 ss.
- Clarke R., *The Digital Persona and Its Application to Data Surveillance*, in *The Information Society*, 10/1994, 77 ss.
- Clerici R., voce *Cittadinanza*, in *Digesto disc. pubbl.*, vol. III, Torino, 1989, 112 ss.
- Cocuccio M., *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam.*, 2/2016, 963 ss.
- Compaine B.M., *The Digital Divide: Facing a Crisis or Creating a Myth?*, Cambridge, 2003.
- Contissa G., Galli F., *AI Act e diritti fondamentali: presupposti tecnologici e ricadute normative*, in *Quad. cost.*, 3/2024, 738 ss.
- Copaccioli S., *Criptovalute e Bitcoin: un'analisi giuridica*, Milano, 2015.
- Corasaniti G., *Identità digitale tra dati personali e relazioni funzionali*, in Ciriello A., Maugeri M. (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 246 ss.
- Cordini G., *Elementi per una teoria giuridica della cittadinanza*, Padova, 1998.
- Correa T., *The participation divide among "online experts": experience, skills and psychological factors as predictors of college students' web content creation*, in *Journal of Computer-Mediated communication*, 1/2010, 71 ss.
- Corso G., *I diritti sociali nella Costituzione italiana*, in *Riv. trim. dir. pubbl.*, 3/1981.
- Cortese F., *Cittadinanza e liberalizzazioni*, in Cortese F. et al. (a cura di), *Dallo status di cittadino ai diritti di cittadinanza. Quaderni della facoltà di giurisprudenza*, 2, 2014, 17 ss.

- Costa P., *Cittadinanza*, Roma-Bari, 2017.
- Costantino F., *Autonomia dell'amministrazione e innovazione digitale*, Napoli, 2012.
- Costantino F., *L'uso della telematica nella pubblica amministrazione*, in Romano A. (a cura di), *L'azione amministrativa. Saggi sul procedimento amministrativo*, Torino, 2016, 246 ss.
- Costantino F., *La c.d. cittadinanza digitale*, in *Dir. pubbl.*, 1/2023, 143 ss.
- Costanzo P., *Avete detto "diritti digitali?"*, in *Diritto, Mercato, Tecnologia*, 2/2016, 145 ss.
- Costanzo P., *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in *Rass. parl.*, 4/2012, 852 ss.
- Čučko Š., Turkanović M., *Decentralized and self-sovereign identity: Systematic mapping study*, in *IEEE Access*, 4/2016, 1 ss.
- Cuocolo L., *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2-3/2012, 263 ss.
- Cuocolo L., *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensioni sociali*, in *Pol. dir.*, 2-3/2012, 278 ss.
- Cuomo L., *Profili giuridici del trattamento biometrico dei dati*, in *Riv. it. med. leg.*, 1/2014, 43 ss.
- D'Acquisto G., *Blockchain e GDPR: verso un approccio basato sul rischio*, in *federalismi.it*, 2/2021, 53 ss.
- D'Acunto L. (a cura di), *Net (or not) Neutrality? Web e regolazione*, Napoli, 2017.
- D'Aloia A., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, 1/2019, 4 ss.
- D'Aloia A., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021.
- D'Alterio E., Mattarella B.G. (a cura di) *La riforma della pubblica amministrazione. Commento alla legge 124/2015 (Mafia) e ai decreti attuativi*, Milano, 2017.
- Das R., *The science of Biometrics: Security technology for identity Verification*, Routledge, 2019.

- Davydov S. (a cura di), *Internet in Russia. A Study of the Runet and Its Impact on Social Life*, Springer, 2020.
- De Cupis A., *Il diritto all'identità personale. Parte prima: il diritto al nome*, Milano, 1949.
- De Filippi P., Wright A., *Blockchain and the Law*, Cambridge (MA), 2018.
- De Filippi P., Wright A., *Blockchain and the Law: the Rule of Code*, Harvard University Press, 2018.
- De Giovanni E., *Il codice dell'Amministrazione digitale: genesi, evoluzione, principi costituzionali e linee generali*, in *Rassegna Avvocatura dello Stato*, 3/2018, 155 ss.
- De Pasquale T., *Problemi interpretativi della nozione giuridica di cittadinanza: un concetto «europeizzato» di diritto pubblico interno? La controversa relazione tra cittadinanza dell'Unione europea e cittadinanze nazionali degli Stati membri*, in *Riv. it. dir. pubbl. comunit.*, 2012, 445 ss.
- De Santis V., *Cittadinanza digitale e diseguaglianze*, in *Italian Papers On Federalism*, 1/2025, 1 ss.
- De Santis V., *Identità e persona all'epoca dell'intelligenza artificiale: riflessioni a partire dall'IA Act*, in *federalismi.it*, 19/2024, 151 ss.
- Del Gatto S., *Il riconoscimento facciale. A che punto siamo?*, in *Giorn. dir. amm.*, 5/2022, 692 ss.
- Denninger E., *Diritti all'uomo e Legge fondamentale*, Torino, 1998.
- Der U., Jähnichen S., Sürmeli J., *Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution*, in *Computers and Society*, 5 dicembre 2017.
- Di Donato F., *Lo stato trasparente. Linked open data e cittadinanza attiva*, Pisa, 2010.
- Di Maria E., Miceli S., *Le frontiere dell'e-government: cittadinanza elettronica e riorganizzazione dei servizi in rete*, Milano, 2004.
- Dourish P., *Algorithms and their others: Algorithmic culture in context*, in *Big Data & Society*, 2/2016, 3 ss.
- Drake W., Wilson E., *Multistakeholderism, Civil Society and Global Diplomacy: The Case of the World Summit on the Information Society*, in Drake W., Wilson

- E. (eds.), *Governing Global Electronic Networks: International Perspectives on Policy and Power*, MIT Press, Cambridge (MA), 2008, 539 ss.
- Ducato R., *I dati biometrici*, in Cuffaro V. et al. (a cura di), *I dati personali del diritto europeo*, Torino, 2019.
- Duni G., *L'amministrazione digitale. Il diritto amministrativo nella evoluzione della telematica*, Milano, 2008.
- Dunphy P. et al., *Decentralizing Digital Identity: Open Challenges for Distributed Ledgers*, in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2018, 75 ss.
- Dunphy P., Garratt L., Petitcolas F.A.P., *Decentralizing Digital Identity: Open Challenges for Distributed Ledgers*, in *2018 IEEE European Symposium on Security and Privacy Workshops*, IEEE, 2018, 75 ss.
- Epstein D., *The making of information governance: the case of the Internet Governance Forum*, in *Journal of Information Technology*, 2/2013, 137 ss.
- Faini F., *Blockchain e diritto. La «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e previdenza*, 1/2020, 297 ss.
- Faini F., *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019.
- Faini F., *Diritto all'esistenza digitale*, in *BioLaw Journal - Rivista di BioDiritto*, n. 3/2019, 91 ss.
- Faini F., *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, 16/2020, 79 ss.
- Faini F., *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in *Dir. inf.*, 4/2019, 1099 ss.
- Faini F., *Regolazione della società e protezione dei diritti nell'era tecnologica*, in Cassano G., Previti S. (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 17 ss.
- Faini F., *Società tecnologica, amministrazione pubblica e diritti digitali*, in Casadei T., Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Padova, 2021, 17 ss.

- Falco G., *Identità personale*, in *Nuovo dig. it.*, VI, Torino, 1938.
- Fanti V., *Intelligenza artificiale e diritto amministrativo: prospettive, limiti e pericoli*, in *Dir. e proc. amm.*, 4/2022, 1001 ss.
- Farina M., *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?*, in *federalismi.it*, 21/2020, 170 ss.
- Farina M., *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale: riflessioni (meta)giuridiche tra crisi di identità e necessità di tutela dei diritti fondamentali dell'individuo*, in *Rivista elettronica di Diritto, Economia, Management*, 1/2020, 42 ss.
- Ferrajoli L., *Cittadinanza, proprietà, diritti della persona*, in *Pol. econ.*, 1993, 49 ss.
- Finck M., *Blockchains and data protection in the European Union*, in *European Data Protection Law Review*, 4(1), 2018, 17 ss.
- Finocchiaro G., (voce) *Identità personale (diritto alla)*, in *Dig. disc. priv., sez. civ.*, V agg., Torino, 2010.
- Finocchiaro G., *Intelligenza Artificiale. Quali regole?*, Bologna, 2024.
- Finocchiaro G., *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 4/2022, 1085 ss.
- Finocchiaro G.D., *Una prima lettura del reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, in *Nuove leggi civili commentate*, 3/2015, 419 ss.
- Fiorelli A., Cassano A.R., *La rivoluzione tecnologica della blockchain*, in Cassano G., Previti S. (a cura di), *Il diritto di Internet nell'era digitale*, cit., 253 ss.
- Floridi L. (ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Berlino, 2014.
- Floridi L., *Etica dell'intelligenza artificiale*, Milano, Cortina, 2022.
- Floridi L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2007.
- Forte P., *Diritto amministrativo e Data Science. Appunti di intelligenza amministrativa artificiale (AAI)*, in *P.A. Persona e Amministrazione*, 1/2020, 247 ss.
- Foucault M., *Sorvegliare e punire. Nascita della prigione*, Torino, 1993.

- Fragale E.N., *La cittadinanza amministrativa al tempo della digitalizzazione*, in *Dir. amm.*, 2/2022, 471 ss.
- Francucci I., *Trasparenza, blockchain e gestione dei rifiuti*, in *Dir. amm.*, 1/2024, 273 ss.
- Friedewald M., Papageorgiou A., *Factors influencing the adoption of self-sovereign identity: A qualitative analysis*, in *Proceedings of the 56th Hawaii International Conference on System Sciences*, 2023.
- Frosini T.E., *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 4/2020, 465 ss.
- Frosini T.E., *Il diritto costituzionale di accesso a internet*, in *Rivista AIC*, 1/2015, 2 ss.
- Frosini T.E., *Il diritto costituzionale di accesso ad Internet*, in *Rivista AIC*, 1/2011.
- Frosini V., *Cibernetica, diritto e società*, Milano, 1968 e *Informatica, diritto e società*, Milano, 1988.
- Fry H., *Hello World. Essere umani nell'era delle macchine*, nella traduzione di Migliori A., Torino, 2018.
- Fry H., *Hello World. Essere umani nell'era delle macchine*, nella traduzione di A. Migliori, Torino, 2018.
- Galetta D.U., Corvalán J.G., *Intelligenza artificiale per una Pubblica Amministrazione 4.0?*, in *federalismi.it*, 3/2019, 7 ss.
- Galič M., Timan T., Koops B.J., *Bentham, Deleuze and Beyond: an Overview of Surveillance Theories from the Panopticon to Participation*, in *Philosophy & Technology*, 30/1, 2017, 10 ss.
- Gallone G., *"Blockchain" e "Big data" nel settore pubblico: spunti in tema di G.D.P.R. "compliance"*, in *federalismi.it*, 14/2022, 66 ss.
- Gallone G., *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Dir. ec.*, 3/2019, 187 ss.
- Gallone G., *Digitalizzazione, amministrazione e persona: per una "riserva di umanità" tra spunti codicistici di teoria giuridica dell'automazione*, in *PA Persona e Amministrazione*, 1/2023, 329 ss.
- Gallone G., *Riserva di umanità e funzioni amministrative*, Padova, 2023.
- Gargiulo P., *Le forme della cittadinanza*, Roma, 2012.

- Garofalo G., *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in *Dir. fam.*, 3/2021, 1505 ss.
- Gasparri G., *Timidi tentativi giuridici di una messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*, in *Dir. inform.*, 3/2015.
- Gates K.A., *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York, 2011.
- Glaser F., *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis*, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 1543 ss.
- Glasser U., Vajihollahi M., *Identity management architecture*, in *Security Informatics*, Springer, 2010, 97 ss.
- Gleason P., *Identifying Identity. A Semantic History*, in *The Journal of American History*, vol. 69, 4/1983.
- Goggin G., *Disability and Digital Inequalities: Rethinking Digital Divides with Disability Theory*, in Muschert G.W., Ragnedda M.(eds.), *Theorizing Digital Divides*, New York, 2017, 69 ss.
- Gometz G., Tawa Folarin M., *Voto elettronico presidiato e blockchain*, in *Ragion pratica*, 2/2018, 317 ss.
- Graf Narbel V., *Digital Identity*, in M. Marelli (ed.), *Handbook on Data Protection in Humanitarian Action*, Cambridge University Press, 2004, 212 ss.
- Grassi P.A., Garcia M.E., Fenton J.L., *Digital Identity Guidelines*, National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.SP.800-63-3>.
- Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Milano, 2014.
- Griffiths J., *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, Zed Books, Londra, 2019.
- Grosso E., *Le vie della cittadinanza. Le grandi radici. I modelli storici di riferimento*, Padova, 1997.

- Gstrein O.J., Kochenov D., *Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?*, in *Frontiers in Blockchain*, 3/2020.
- Guastini R., *Diritti*, in Comanducci P., Guastini R. (a cura di), *Analisi e diritto*, Torino, 1994.
- Guazzarotti A., *I diritti sociali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Riv. trim. dir. pubbl.*, 1/2013, 9 ss.
- Guggenberger T., Rieger A., Wenninger A., *Accept Me as I Am or See Me Go: A qualitative analysis of user acceptance of SSI applications*, in *Proceedings of the 56th Hawaii International Conference on System Sciences*, 2023.
- Hardjono T., Pentland A., *Open Algorithms for Identity Federation*, in *Advances in Information and Communication Networks*, 2019, 24 ss.
- Hargittai E., Hinnant A., *Digital Inequality: Differences in Young Adults' Use of the Internet*, in *Communication Research*, 5/2008, 602 ss.
- Hargittai E., *Second Level Digital Divide: Differences in People's Online Skills*, First Monday, in www.firstmonday.org, 7, 4/2002.
- Hargittai E., Walejko G., *The participation divide: content creation and sharing in the digital age*, in *Information, Communication & Society*, 2/2008, 239 ss.
- Heilweil R., *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That's Progress*, in *Vox*, 11 giugno 2020.
- Helsper E.J., *The digital disconnect. The social causes and consequences of digital inequalities*, Londra, 2021.
- Heudin J.C., *Intelligence Artificielle. Manuel de survie*, Science-eBook, 2017.
- Hilbert M., Lopez P., Vasquez C., *Information societies or "ICT equipment societies"? Measuring the digital information processing capacity of a society in bits and bytes*, in *The Information Society*, 3/ 2010, 157 ss.
- Howard P., Busch L., Sheets P., *Comparing digital divide: Internet access and social inequality in Canada and the United States*, in *Canadian Journal of Communication*, 1/2010, 109 ss.
- Hu M., *Biometric surveillance and big data governance*, in Gray D., Henderson S.E. (eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge, 2017.
- Hughes E., *A Cypherpunk's Manifesto*, 9 marzo 1993.

- Iannuzzi A., Filosa F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2/2019.
- Iannuzzi A., Laviola F., *I diritti fondamentali nella transizione digitale fra libertà e uguaglianze*, in *Dir. cost.*, 1/2023, 18.
- Ippolito M., *La disintermediazione dei processi nella pubblica amministrazione: l'impatto della tecnologia "blockchain"*, in *ambientediritto.it*, 2/2021, 36 ss.
- Irti N., *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2001.
- Johnson D.R., Post D., *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 5/1996, 1367 ss.
- Kafka F., *Il processo*, Milano, 1984.
- Kaiser B., *La dittatura dei dati*, Milano, 2019.
- Kewell B., Adams R., Parry G., *Blockchain for Good?*, in *Strategic Change*, 26/2017, 429 ss.
- Kitchin R., *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, Sage, Los Angeles, 2014.
- Kleinwächter W., *The Power of Ideas: Internet Governance in a Global Multi Stakeholder Environment*, Marketing für Deutschland, Berlino, 2007.
- Kochenov D., *Cittadinanza. La promessa di un alchimista*, Bologna, 2020, 204.
- Kostka G., *China's social credit systems and public opinion: Explaining high levels of approval*, in *New media & Society*, 21/2019, 1565 ss.
- Krul E. et al., *SoK: Trusting Self-Sovereign Identity*, in *Proceedings on Privacy Enhancing Technologies*, 3/2024, 297 ss.
- Kubach M. et al., *Selfsovereign and decentralized identity as the future of identity management?*, in *Open Identity Summit 2020*, 2020.
- Kubach M. et al., *Social acceptance of self-sovereign identity: Empirical findings and implications*, in *Computers*, 45/2022.
- Kwet M., *The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud*, in *The Intercept*, 14 luglio 2020.
- Laatikainen G., Kolehmainen T., Abrahamsson P., *Self-Sovereign Identity Ecosystems: Benefits and Challenges*, in *12th Scandinavian Conference on Information Systems*, Orkanger, Norway, 17 giugno 2021.

- Lam T., *The People's Algorithms: Social Credits and the Rise of China's Big (Br)other*, in A. Mennicken, R. Salais (eds.), *The New Politics of Numbers. Utopia, Evidence and Democracy*, Palgrave Macmillan, Cham, 2022, 71 ss.
- Landini S., *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. industr.*, 4-5/2017, 180 ss.
- Law K., Mik E., *Pause the blockchain legal revolution*, in *International and Comparative Law Quarterly*, 69/2020, 135 ss.
- Le H.V.A. et al., *Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees*, in *Computers*, 14/2025, 2 ss.
- Learned-Miller E. et al., *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020.
- Lessig L., *Code and Other Laws of Cyberspace*, New York, 1999.
- Lessig L., *Code: Version 2.0*, Basic Books, New York, 2006.
- Levante G., *Il sistema pubblico di identità digitale*, in <https://www.notartel.it/notartel/pdf-studi/sistema-pubblico-id-digitale-1-2020-DI.pdf>, 1/2020, 2 ss.
- Liang F. et al., *Costructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy & Internet*, 10/2018, 415 ss.
- Lippolis V., *La cittadinanza europea*, Bologna, 1994.
- Lo Sapio G., *Il tormentato rapporto tra "blockchain" e pubblica amministrazione nel prisma dei contratti pubblici*, in *federalismi.it*, 26/2023, 112 ss.
- Lo Sapio G., *L'"Artificial Intelligence Act" e la prova di resistenza per la legalità algoritmica*, in *federalismi.it*, 16/2024, 265 ss.
- Lombardi P., *Giudice amministrativo e cittadinanza: quale contributo per un concetto giuridicamente sostenibile?*, in *federalismi.it*, 20/2018.
- Longo A., Scorza G., *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Milano, 2020.
- Longo E., Pin A., *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *DPCE*, 1/2023, 103 ss.
- Lotta C., *Un nuovo diritto al tempo del Covid-19? Accesso a Internet e digital divide*, in *Rivista del Gruppo di Pisa*, 2/2020, 61 ss.

- Luciani F., *Brevi note sull'innovazione tecnologica come strumento di buona amministrazione*, in *La Cittadinanza europea*, 2/2022, 199 ss.
- Luciani M., *Quale identità?*, in Somma A. et al. (a cura di), *Dialoghi con Guido Alpa*, Roma, 2018.
- Lyon D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002.
- Macchia M., *Blockchain and Public Authorities: a Field Yet to Be Explored*, in *Erdal*, 2/2021, 19 ss.
- Macchia M., *Blockchain e pubblica amministrazione*, in *federalismi.it*, 2/2021, 117 ss.
- Macchia M., Mascolo A., *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in *Giorn. dir. amm.*, 4/2022, 556 ss.
- Macdonald S.J., Clayton J., *Back to the Future, Disability and the Digital Divide*, in *Disability & Society*, 5/2013, 702 ss.
- Macrì I., *L'identità digitale, nuovo documento di riconoscimento*, in *Azienditalia*, 3/2021, 475 ss.
- Malaschini A., *Il regolamento europeo sull'intelligenza artificiale (IA), l'orientamento italiano e i diversi indirizzi di Stati Uniti e Regno Unito*, in *Rass. Parl.*, 1/2024, 35 ss.
- Malcom J., *Multi-stakeholder governance and the Internet Governance Forum*, Terminus Press, Perth, 2008.
- Manca G., *Introduzione*, in *Il regolamento eIDAS n. 2024/1183, n. spec. Rivista elettronica di Diritto, Economia, Management*, 4/2024, 9 ss.
- Manfredi L., *Progetto Pilota per la realizzazione, su Blockchain, del Fascicolo Sanitario Elettronico con il coinvolgimento dei Fondi Sanitari Integrativi nel flusso di dati*, in *federalismi.it*, 21/2023, 226 ss.
- Manganaro F., *Dalla cittadinanza alle cittadinanze. Questioni su un concetto polimorfico*, in *AmbienteDiritto.it*, 4/2022.
- Manganaro F., *Vecchi problemi e nuove prospettive della cittadinanza*, in Manganaro F., Romano Tassone A. (a cura di), *Persona ed amministrazione. Privato, cittadino, utente e pubbliche amministrazioni*, Torino, 2004.

- Mangiameli Amato A.C., *Intelligenza artificiale, "big data" e nuovi diritti*, in *Riv. inf. dir.*, 1/2022, 93 ss.
- Maniscalco N., *La tecnologia come fattore di istruzione*, in *Rivista AIC*, 1/2024, 569 ss.
- Mantellero A., *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.*, 1, 2012, 135 ss.
- Marcelli F., *L'accesso a Internet come diritto fondamentale? Tendenze del diritto internazionale e realtà dei fatti*, in Pietrangeli M. (a cura di), *Il diritto accesso a Internet*, Napoli, 2011.
- Marchesi M., *Blockchain pubbliche e permissioned: una questione di fiducia*, in *federalismi.it*, 2/2021, 140 ss.
- Marchetti B., *Intelligenza artificiale, poteri pubblici e "rule of law"*, in *Riv. it. dir. pubbl.*, 1/2024, 49 ss.
- Marongiu D., *Il governo dell'informatica pubblica*, Napoli, 2007.
- Marongiu D., *L'attività amministrativa automatizzata*, Santarcangelo di Romagna, 2005.
- Marshall T.H., *Citizenship and Social Class*, in *Inequality and Society*, Manza J., Sauder M. (ed.), New York, 2009.
- Marsocci P., *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *AIC*, 1/2015, 1 ss.
- Martines F., *La digitalizzazione della pubblica amministrazione*, in *MediaLaws*, 2/2018, 146 ss.
- Masucci A., *Procedimento amministrativo e nuove tecnologie*, Torino, 2011.
- Matassa M., *Blockchain e pubblica amministrazione: stato dell'arte e prospettive*, in *IdF*, 3/2021, 803 ss.
- Mathiason J., *Internet Governance: The New Frontier of Global Institutions*, Routledge, Abingdon, 2009.
- Maull R. et al., *Distributed ledger technology: Applications and implications*, in *Strategic Changes*, 26/2017.
- Mayer-Schönberger V., Cuckier K., *Big data: A revolution that will transform how we live, work and think*, Houghton Mifflin Harcourt, Boston-New York, 2013.

- Mazzei G., *Big data come beni comuni globali e principi in tema di public utilities*, in *federalismi.it*, 12, 162-184, 2023.
- Mazzeo A., Nastri M., *Identificazione in rete: identità digitale e identità personale*, in Ciriello A., Maugeri M. (a cura di), *Identità digitale, processo e rapporti tra privati*, Milano, 2024, 41 ss.
- McCarthy J. et al., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Stanford, 31 agosto 1955.
- Menegazzi Munari F., *Cittadinanza europea: una promessa da mantenere*, Torino, 1996.
- Merloni F. (a cura di), *Introduzione, all'e-Government. Pubbliche amministrazioni e società dell'informazione*, Torino, 2005.
- Metzger F., Martin N., *The chimera of control: Perceptions of data control in self-sovereign identity systems*. *Human Technology*, 20(2)/2024, 183 ss.
- Metzl J.F., *Information Technology and Human Rights*, in *Human Rights Quarterly*, 4/1996, 705 ss.
- Mindus P., *Cittadini e no. Forme e funzioni dell'inclusione e dell'esclusione*, Firenze, 2014.
- Minsky M.L., *Semantic Information Processing*, Cambridge (MA), 1968.
- Mobilio G., *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso "Glukhin c. Russia"*, in *DPCE online*, 1/2024, 695 ss.
- Mobilio G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.
- Modugno F., *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995.
- Mollo F., *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *federalismi.it*, 28/2024.
- Mollo F., *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, in *federalismi.it*, 19/2023, 267 ss.
- Morelli A., *Persona e identità personale*, in *BioLaw Journal*, 2/2019.
- Moro G., *Cittadinanza*, Milano, 2020.

- Morrone A., *Le forme della cittadinanza nel Terzo Millennio*, in *Quad. cost.*, 2015, 303 ss.
- Mossberger K., Talbert C.J., Stansbury M., *Virtual Inequality. Beyond the Digital Divide*, Washington, 2003.
- Mueller M., *Networks and States. The global Politics of Internet Governance*, MIT Press, Cambridge (MA), 2010.
- Mühle A. et al., *A Survey on Essential Components of a Self-Sovereign Identity*, 17 luglio 2018.
- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, reperibile su [https:// bitcoin.org/bitcoin.pdf](https://bitcoin.org/bitcoin.pdf).
- Nannipieri L., *Sulla "Dichiarazione dei diritti in Internet". Alcune annotazioni critiche*, in *Inf. dir.*, 2/2014, 127 ss.
- 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.
- Napolitano C., *Inclusione sociale e trasformazione digitale: dal digital divide all'esclusione algoritmica*, in *Democrazia e Diritti Sociali*, 1/2025, 179 ss.
- Nardocci C., *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU "Glukhin c. Russia"*, in *BioLaw Journal - Rivista di BioDiritto*, 1/2024, 279 ss.
- Nascimbene B., *Diritti di cittadinanza e libertà di circolazione nell'Unione europea*, Padova, 2012.
- Nastri M., *Identità digitale e identità personale: un percorso di sintesi*, in Giordano R. et al. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022.
- Neroni Rezende I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, 3/2020, 375 ss.
- Nida-Rümelin J., Weidenfeld N., *L'umanesimo digitale. Un'etica per l'epoca dell'Intelligenza Artificiale*, Milano, 2019.
- Niger S., *Il diritto all'identità personale*, in Finocchiaro G. (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Padova, 2008, 113 ss.

- Norris P., *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge, 2001.
- Novelli C., *L'“Artificial Intelligence Act” (AIA) Europeo: alcune questioni di implementazione*, in *federalismi.it*, 2/2024, 95 ss.
- O'Leary S., *The Evolving Concept of Community Citizenship*, London, Kluwer, 1996.
- Oliveri F., *Per una teoria generale dei diritti digitali*, in *Dem. dir. soc.*, 1/2025, 203 ss.
- Olivi G., *“Big Data”, metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Dir. ind.*, 2/2020, 181 ss.
- Ono H., Zavodny M., *Immigrants, English Ability, and the Digital Divide*, in *Social Science Quarterly*, 3/2008, 1135 ss.
- Orefice M., *I big data. Regole e concorrenza*, in *Politica del diritto*, 4, 2016, 697-744.
- Orofino A.G., *Firme elettroniche e procedimenti amministrativi*, Bari, 2008, 83 ss.
- Orofino A.G., *La semplificazione digitale*, in *Dir. econ.*, 3/2019, 87 ss.
- Orofino A.G., *Pubblici servizi, digitalizzazione e intelligenza artificiale*, in Giordano R. et al. (a cura di), *Il diritto nell'era digitale*, Milano, 2022, 541 ss.
- Ortalda A., Leucci S., *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Riv. it. inf. e dir.*, 1/2022, 145 ss.
- Orwell G., *1984*, Milano, 1950.
- Othman A., Callahan J., *The Horcrux Protocol: a Method for Decentralized Biometric-based Self-sovereign identity*, in *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN)*, luglio 2018, 1-7.
- Otranto P., *Net Neutrality e poteri amministrativi*, in *federalismi.it*, 3, 2019, 2-45.
- Pace A., *I progetti “PC ai giovani” e “PC alle famiglie”: esercizio di potestà legislativa esclusiva statale o violazione della potestà regionale residuale*, in *Giur. cost.*, 5/2004, 3221 ss.
- Pagliantini S., *La base giuridica dell'AI Act ex art. 114 Tfu: l'intelligenza artificiale tra mercato e persona*, in *Foro it.*, 1/2025, 19 ss.

- Pajno A., Donati F., Perrucci A. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022.
- Palladino A., “Oblivio 4.0” tra identità digitale e cancellazione dati: quale diritto?, in *De Iustitia*, 2/2019, 76 ss.
- Palumbo S., *La transizione digitale della pubblica amministrazione italiana nella prospettiva europea. Considerazioni alla luce del Piano nazionale ripresa e resilienza*, in *Dir. econ.*, 1/2023, 163 ss.
- Pangrazio L., Sefton-Green J., *Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?*, in *Journal of New Approaches in Educational Research*, 1/2021, 15 ss.
- Pasceri G., *Intelligenza artificiale, algoritmo e machine learning. La responsabilità del medico e dell'amministrazione sanitaria*, Milano, 2021, 15 ss.
- Pascuzzi G., *La cittadinanza digitale*, Bologna, 2021.
- Pellizzari S., *La cittadinanza amministrativa tra diritto europeo e diritto nazionale*, in Cortese F. et al. (a cura di), *Dallo status di cittadino ai diritti di cittadinanza*, Napoli, 2014.
- Perfetti L.R., *I diritti sociali. Sui diritti fondamentali come esercizio della sovranità popolare nel rapporto con l'autorità*, in *Dir. pubbl.*, 1/2013, 64 ss.
- Pergolesi F., *Alcuni lineamenti dei diritti sociali*, Milano, 1953.
- Perri P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020.
- Pesce G., *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018.
- Pesce G., *Funzione amministrativa, intelligenza artificiale e Blockchain*, Napoli, 2021.
- Petruso R., Smorto G., *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *La Nuova Giurisprudenza Civile Commentata*, 4/2024, 989 ss.
- Picozza E., *Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence*, in *Giur. it.*, 7/2019, 1657 ss.
- Pietrangelo M., *Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione: luci ed ombre*, in *ID*, 1-2/2005, 73 ss.

- Pike S., Dickson F., *Identity on the Blockchain Special Report: Forecast and Analysis for Blockchain-Based Identity Solutions*, Jul 2018 - *Special Study*, 2018.
- Pino G., *Diritti sociali. Per una critica di alcuni luoghi comuni*, in *Ragion Pratica*, 2/2016, 495 ss.
- Pino G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.
- Pino G., *L'identità personale*, in Rodotà S., Tallacchini M. (a cura di), *Trattato di biodiritto*, vol. I, *Ambito e fonti del biodiritto*, Milano, 2010, 298.
- Piras P., *L'amministrazione digitale tra divari e doveri. "Non camminare davanti a me, ma al mio fianco"*, in *P.A. Persona e Amministrazione*, 2/2022, 422.
- Pirni A., Carnavale A., *The challenge of regulating emerging technologies. A philosophical framework*, in Palmerini E., Stradella E. (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, 2013.
- Pisa R., *Il digital divide e le iniziative per superarlo*, in Marcelli F., Marsocci P., Pietrangelo M. (a cura di), *La Rete Internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015.
- Pisa R., *L'accesso ad Internet: un nuovo diritto fondamentale?*, in *Treccani.it*, 7 gennaio 2010.
- Podgorelec B., Alber L., Zefferer T., *What is a (Digital) Identity Wallet? A Systematic Literature Review*, in *IEEE 46th Annual Computers, Software, and Applications Conference*, 2022, 809 ss.
- Pollicino O., *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quad. cost.*, 3/2023, 569 ss.
- Pollicino O., *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online*, in *Riv. trim. dir. pubbl.*, 4, 2022, 1051 ss.
- Ponce Solé J., *Il regolamento dell'unione europea sull'intelligenza artificiale, la discrezionalità amministrativa e la riserva di umanità*, in *Riv. trim. dir. pubbl.*, 3/2024, 825 ss.

- Porena D., *Il problema della cittadinanza. Diritti, sovranità e democrazia*, Torino, 2011.
- Preukschat A., Reed D., *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credential*, New York, 2021.
- Previti L., *La decisione amministrativa robotica*, Napoli, 2022.
- Previti L., *La proposta di regolamento europeo in materia di intelligenza artificiale tra incertezze applicative ed esigenze di semplificazione*, in *Rassegna trimestrale dell'Osservatorio AIR*, 1/2023, 19 ss.
- Prosperetti E., *Identità digitale ed elettronica nazionale e transfrontaliera nell'accesso ai servizi pubblici e privati e prospettive di utilizzo nei contratti online e nei servizi bancari*, in Cassano G., Previti S. (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, 434 ss.
- Provolo D., *Il sistema sanzionatorio del novellato codice della privacy e la tutela penale patchwork dei dati genetici e dei dati biometrici*, in *Riv. trim. dir. pen. econ.*, 1-2/2019, 242 ss.
- Putnam R.D., *Bowling Alone. The Collapse and Revival of American Community*, New York, 2000.
- Quadri R., voce *Cittadinanza*, in *Novissimo Dig. It.*, vol. III, Torino, 1959, 307 ss.
- Rabai B., *The role of technology and innovation in digital and social inclusion. The case of disability in a public perspective*, in *MediaLaws*, 1/2022, 1 ss.
- Raffiotta E.C., *Appunti in materia di diritto all'identità personale*, in *Forum Quad. Cost.*, 26 gennaio 2010.
- Raffiotta E.C., Baroni M., *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal - Rivista di BioDiritto*, 1/2022.
- Raffiotta E.C., Baroni M., *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in Pajno A., Donati F., Perrucci A. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022.
- Ragnedda M., *Il digital divide. Le disuguaglianze digitali e i suoi vari livelli d'analisi*, in *Quaderni di Teoria Sociale*, 1/2018, 81 ss.
- Ragnedda M., *The Third Digital Divide: a Weberian approach to digital inequalities*, Oxford, 2017.

- Randazzo A., *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *dirittifondamentali.it*, 3/2021, 363 ss.
- Raskin M., Yermack D., *Digital Currencies, Decentralized Ledgers, and the Future of Central Banking*, in Conti-Brown P., Lastra R.M. (eds.), *Research Handbook on Central Banking*, 2018, 474 ss.
- Ratha N.K., Connell J.H., Bolle R.M., *Enhancing security and privacy in biometrics-based authentication systems*, in *IBM Systems Journal*, 40.3/2001, 614 ss.
- Remotti F., *Contro l'identità*, Roma-Bari, 2001.
- Rescigno P., *Le formazioni sociali intermedie*, in AA.VV., *Dalla Costituente alla Costituzione*, Accademia nazionale dei Lincei, Roma, 1998.
- Resta G., *Identità personale e identità digitale*, in *Dir. inform. e inf.*, 3/2007, 515.
- Ricciulli F., *I diritti digitali: verso un'identità unica europea*, in *Dir. pubbl. eur. – Rass. online*, 1/2024, 190 ss.
- Rich E., Knight K., *Artificial Intelligence*, New York, 1991.
- Rifkin J., *L'era dell'accesso. La rivoluzione della new economy*, Milano, 2000.
- Ristolainen M., *Should 'runet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West*, in *Journal of information warfare*, 4, 2017, 112 ss.
- Rittenberg H., *Who Are You: A Primer on Digital Identity*, in *Journal of Technology and Intellectual Property*, 3 maggio 2022.
- Rodotà S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997.
- Rodotà S., *Il diritto di avere diritti*, Bari, 2012.
- Rodotà S., *Identità e Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari-Roma, 2018.
- Rodotà S., *Tecnologie e diritti*, Bologna, 2021.
- Rodríguez Ayuso J.F., *Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014*, in *federalismi.it*, 24/2017, 2 ss.
- Romanelli Grimaldi C., voce *Cittadinanza*, in *Enc. giur.*, vol. III, Roma, 1988, 1 ss.

- Romanosky S., *Examining the Impact of Data Breach Disclosure Laws*, in *Journal of Policy Analysis and Management*, 35(3), 2016, 641 ss.
- Roosendaal A., *Digital Personae and Profiles as Representations of Individuals*, in *Privacy and Identity: IFIP AICT*, vol. 320, 2010, 226 ss.
- Rossi E., *Le formazioni sociali nella Costituzione italiana*, Padova, 1989.
- Rovagnati A., *Sulla natura giuridica dei diritti sociali*, Torino, 2009.
- Rubechini P., *Blockchain e pubblica amministrazione italiana: i primi passi di un cammino ancora lungo*, in *Giorn. dir. amm.*, 3/2021, 298 ss.
- Rubechini P., *Tecnologia blockchain e fiducia amministrativa*, Napoli, 2023.
- Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.
- Ruffolo U., Amidei A., *La regolazione ex ante dell'intelligenza artificiale tra gestione del rischio by design, strumenti di certificazione preventiva e «autodisciplina» di settore*, in Pajno A., Donati F., Perrucci A., *Intelligenza artificiale e diritto*.
- Ruoppo R., *Il regolamento UE in materia di Intelligenza Artificiale (c.d. AI Act): un quadro normativo uniforme per la tutela dei diritti fondamentali*, in *Rass. dir. civ.*, 3/2024, 996 ss.
- Russel S.J., Norvig P., *Artificial intelligence. A modern approach*, New Jersey, 2010.
- Samuel A.L., *Some Studies in Machine Learning Using the Game of Checkers*, in *Journal of Research and Development*, 3/1959, 210 ss.
- Santosuosso A., *Intelligenza artificiale e diritti. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, 6 ss.
- Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996.
- Sartori L., *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Bologna, 2006.
- Sarzana di S. Ippolito F., Nicotra M., *Diritto alla blockchain, intelligenza artificiale e IoT*, Milano, 2018.
- Satchell C. et al., *Identity crisis: user perspectives on multiplicity and control in federated identity management*, in *Behaviour & Information Technology*, 1/2011, 51 ss.

- Scagliarini S., *I diritti costituzionali nell'era di internet: cittadinanza digitale, accesso alla rete e net neutrality*, in Casadei T., Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche*, 3 ss.
- Scantamburlo T., Charlesworth A., Cristianini N., *Machine Decisions and Human Consequences*, in Yeung K., Lodge M. (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019.
- Schardong F., Custódio R., *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*, in *Sensors*, 22/2022.
- Schroeder R., *Aadhaar and the Social Credit System: Personal Data Governance in India and China*, in *International Journal of Communication*, 16/2022, 2373 ss.
- Sciascia G., *Reputazione e potere: il "social scoring" tra distopia e realtà*, in *Giorn. dir. amm.*, 3/2021, 317 ss.
- Sciulli G., *Il diritto all'oblio e l'identità digitale*, Bologna, 2014.
- Sica S., Giannone Codiglione G., *La libertà fragile. Pubblico e privato al tempo della rete*, Napoli, 2014.
- Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, 69 ss.
- Simoncini A., *Sovranità e potere nell'era digitale*, in Frosini T.E. et al. (a cura di), *Diritti e libertà in Internet*, Firenze, 2017.
- Singh G., et al., *Biometric Identification System: Security and Privacy Concern*, in S. Awasthi S. et al. (eds.), *Artificial Intelligence for a Sustainable Industry 4.0.*, Springer, 2021.
- Siqueira A., Da Conceição A.F., Rocha V., *Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review*, in *ACM Comput. Surv* 1, 1/ 2021, 1 ss.
- Soltani R., Nguyen U.T., A. An, *A Survey of Self-Sovereign Identity Ecosystem, Security and Communication Network*, in *Security and Communication Networks*, 2021.
- Spiniello C., *È (ancora) tempo di costituzionalismo digitale*, in *Rivista italiana di informatica e diritto*, 1/2025, 580 ss.

- Stokkink Q. et al., *A truly selfsovereign identity system*, in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 2021, 1 ss.
- 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 *Rivista AIC*, 4/2016, 1 ss.
- Suffia G., *La "società liquida" e il caso Snowden*, in Ziccardi G., Perri P. (a cura di), *Tecnologia e diritto*, vol. III, Milano, 2019, 23 ss.
- Sundararajan S., *Moldova Eyes Blockchain IDs to help curb child trafficking*. Coin Desk, <https://www.coindesk.com/moldova-eyes-blockchain-ids-to-help-curb-child-trafficking/>, 2017.
- Thuermer G., Koesten L., Simperl E., *Talking Metadata. Understanding Privacy Implications of Volunteer Contributions in Citizen Science Projects*, in *Etica & politica - Ethics & politics*, 2/2023, 197 ss.
- Tincani P., *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 2/2018, 61 ss.
- Tobin A., Reed D., *The Inevitable Rise of Self-Sovereign Identity*, the Sovrin Foundation, 29(2016)18, 2016.
- Tommasi S., *"Digital services act" e "artificial intelligence act": tentativi di futuro da armonizzare*, in *Persona e Mercato*, 2/2023, 279 ss.
- Torchia L., *Lo Stato digitale*, Bologna, 2023.
- Toth K.C., Anderson-Priddy A., *Self-Sovereign digital identity - a paradigm shift for identity*, in *IEEE Secur. Priv.*, 17/2019, 17 ss.
- Trucco L., *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004.
- Tsakalakis N., Stalla-Bourdillon S., O'Hara K., *Data Protection by Design for Cross-Border Electronic Identification: Does the EIDAS Interoperability Framework Need To Be Modernised?*, in Kosta E. et al. (eds.), *Privacy and Identity Management. Fairness, Accountability and Trasparency in the Age of Big Data*, Springer, 2019.
- Turing A., *Computing Machinery and Intelligence*, in *Mind*, 59/1950, 433 ss.

- Turing A., *On Computable Numbers, with an Application to the Entscheidungsproblem*, in *Proceedings of the London Mathematical Society*, 1936, 230 ss.
- Turkle S., *Life on the Screen. Identity in the Age of the Internet*, Simon & Schuster, New York, 1995.
- Ursi R., *Diritto amministrativo generale*, Milano, 2024.
- Vaccari S., *Note minime in tema di Intelligenza Artificiale e decisioni amministrative*, in *Giustamm.it*, 10/2019, 1 ss.
- Van Dijk J.A.G.M., *The deeping divide. Inequality in the information society*, London, 2005.
- Van Dijk J.A.G.M., Van Deursen A.J.A.M., *Digital Skills: Unlocking the Information Society*, New York, 2014.
- Vantin S., *I divari digitali nell'epoca della rete globale*, in Casadei T., Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, 2024.
- Vardi N., *“Criptovalute” e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. inform.*, 3/2015.
- Vasak K., *A 30 years struggle. the sustained efforts to give force of law to the Universal Declaration of Human Rights*, in *The UNESCO Courier*, 1977, 29-32.
- Verzaro M., *La blockchain e il fabbisogno di personale nella pubblica amministrazione*, in *federalismi.it*, 2/2021, 195 ss.
- Vigorito A., *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *MediaLaws*, 1/2023, 104 ss.
- Votta F., *L'amministrazione pubblica e la tecnologia “blockchain”*, in *Giorn. dir. amm.*, 4/2022, 450 ss. Caldarelli S., *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra “mito” e realtà giuridica*, in *Dir. inform.*, 4/2020, 857 ss.
- Walton G., *China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China*, Rights & Democracy, 2001.

- Wang D., Zhao J., Wang Y., *A Survey on Privacy Protection of Blockchain: The Technology and Application*, in *IEE Access*, 8/2020.
- Wang F., De Filippi P., *Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion*, in *Frontiers in Blockchain*, 2/2020.
- Warwick K., Shah H., *Turing's Imitation Game*, Cambridge (UK), 2016.
- Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 12 marzo 2015.
- Wu T., *Network Neutrality, Broadband Discrimination*, in *Journal on Telecommunications and High Technology Law*, 2, 2003, 141 ss.
- Wu T., *The Master Switch: The Rise and Fall of Information Empires*, Alfred A. Knopf, New York, 2010.
- Zagrebelsky G., *Il diritto mite*, Torino, 1992.
- Zencovich Z., (voce) *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993.
- Ziccardi G., *Controllo, sorveglianza e segreto: una prospettiva informatico-giuridica*, in Ziccardi G., Perri P. (a cura di), *Tecnologia e diritto*, vol. III, Milano, 2019, 3 ss.
- Ziccardi G., *Diritti digitali*, Milano, 2022.
- Zincone G., *Da sudditi a cittadini*, Bologna, 1992.
- Zorzi Galgano N., *Il Regolamento UE 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contr. impr.*, 1/2025, 45 ss.
- Zorzi Galgano N., *Le due anime del GDPR e la tutela del diritto alla privacy*, in Zorzi Galgano N. (a cura di), *Persona e mercato dei dati*, Milano, 2019, 35 ss.
- Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.
- Zuddas P., *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio AIC*, 2/2020, 285 ss.
- Zwitter A.J., Boisse-Despiaux M., *Blockchain for humanitarian action and development aid*, in *J. Int. Humanit. Action*, 3/2018, 1 ss.