Tecnologie emergenti e vulnerabilità: dallo standard della protezione dai rischi al paradigma della promozione dei diritti

Caterina Di Costanzo*

EMERGING TECHNOLOGIES AND VULNERABILITIES: FROM A RISK-BASED APPROACH TO A RIGHTS-PROMOTION PARADIGM

ABSTRACT: This paper explores the relationship between emerging technologies and vulnerabilities through the analytical distinction between the European paradigm of risk protection and an emerging national paradigm oriented toward the promotion of fundamental rights. EU digital regulation largely adopts a precautionary and risk-management approach aimed at safeguarding the internal market and ensuring minimum standards of rights protection. Within this framework, national constitutional systems may develop complementary strategies focused on the active promotion of rights. The Italian case illustrates how digital technologies can operate as enabling infrastructures for dignity, autonomy, and participation, particularly in relation to vulnerable individuals and contexts.

KEYWORDS: new technologies; vulnerabilities; risk-based approach; rights-promotion paradigm; digital constitutional identity

ABSTRACT: Il contributo analizza il rapporto tra tecnologie emergenti e vulnerabilità attraverso l'analisi dei fondamentali aspetti concernenti lo standard europeo della protezione dai rischi e la specifica identità costituzionale nel settore digitale. La regolazione digitale dell'Unione europea – dal Digital Services Act all'AI Act – risulta prevalentemente orientata alla prevenzione e gestione dei rischi connessi all'uso delle tecnologie. In tale quadro, gli ordinamenti nazionali sono chiamati a sviluppare approcci complementari volti a promuovere l'effettività dei diritti fondamentali. Il caso italiano mostra come l'innovazione tecnologica possa configurarsi come infrastruttura abilitante per dignità, autonomia e partecipazione, soprattutto con riferimento alle persone vulnerabili.

KEYWORDS: tecnologie emergenti; vulnerabilità; standard della protezione dai rischi; paradigma della promozione dei diritti; identità costituzionale digitale

* *Docente a contratto di Diritto costituzionale presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze. Mail: caterina.dicostanzo@unifi.it.* *Contributo sottoposto a doppio referaggio anonimo.*

giurisprudenza della dignità tecnologicamente mediata – 3.3. Le riforme abilitanti nei rapporti fra tecnologie e vulnerabilità – 4. Considerazioni conclusive.

1. Introduzione

La progressiva digitalizzazione dei processi e dei servizi preposti alla tutela dei diritti fondamentali impone, ormai in modo strutturale e continuativo, una riflessione articolata e un ripensamento critico delle modalità di elaborazione e di attuazione dell'identità costituzionale italiana. Tale identità è chiamata a essere declinata, nello specifico dell'ambiente digitale, nell'ottica della definizione dell'insieme dei principi e delle garanzie che, nel contesto tecnologico, ridefiniscono il rapporto tra persona, comunità e istituzioni.

In tale prospettiva, la transizione digitale non può essere considerata come un mero processo tecnico o amministrativo, ma viene inquadrata nell'ambito dei fenomeni costituzionalmente rilevanti, che incidono sulle modalità di esercizio dei diritti e sull'effettività della tutela delle persone più vulnerabili.

Questa impostazione richiede che a fianco della "governance del rischio (*risk governance*) europea si sviluppi una adeguata governance dei diritti (*rights governance*)*"* nazionale, potenzialmente espressiva della specificità dell'ordinamento costituzionale nel coniugare innovazione e tutela dei diritti fondamentali. L'identità costituzionale digitale potrebbe divenire così una bussola per orientare la regolazione interna delle tecnologie verso la promozione dei diritti, riaffermando, nell'ordinamento italiano, la sua vocazione personalista e solidale nel nuovo spazio digitale.

Occorre evidenziare sin da subito che non si tratta di modelli di governance contrapposti bensì complementari poiché la governance del rischio europea è diretta soprattutto ad assicurare lo standard minimo della protezione dai rischi, che potremmo chiamare idiosincratici e sistemici, mentre la governance dei diritti nazionale potrebbe essere appropriatamente finalizzata a integrare tale prospettiva con la promozione attiva dei diritti fondamentali.

Ad oggi, la regolazione privilegia la dimensione protettiva — connessa alla gestione dei rischi derivanti dall'uso delle tecnologie — mentre resta ancora poco sviluppato il versante di analisi e implementazione della dimensione promozionale, orientata a realizzare i principi costituzionali di dignità e sviluppo della persona.

Questo contributo ha l'obiettivo di analizzare la regolazione e l'impatto delle innovazioni tecnologiche sui diritti fondamentali collocandosi entro la dicotomia tra protezione dai rischi e promozione dei diritti, concentrandosi su alcuni ambiti fondamentali di tutela delle vulnerabilità rispetto alle quali le nuove tecnologie possono costituire una leva per rilanciare il sistema di protezione dei diritti come strumento di tutela e promozione non solo individuale, ma anche comunitaria.

Nei paragrafi seguenti verrà ricostruito il quadro normativo esistente a livello europeo e nazionale, per evidenziare possibili profili di criticità e potenzialità delle nuove tecnologie nell'ambito della loro complementare disciplina collocata nel pendolo che idealmente scorre fra tutela dai rischi e promozione dei diritti.

2. Il quadro europeo: lo standard della protezione dai rischi

2.1. Le caratteristiche dello standard europeo della protezione dai rischi

Fin dagli anni Novanta del secolo scorso, una delle principali modalità regolatorie eurounitarie è stata quella del "risk regulation model", cioè uno schema tecnico-giuridico fondato su procedure armonizzate, possibilmente trasparenti, e finalizzate all'identificazione, valutazione e gestione dei rischi[1]. Questo modello viene sperimentato e validato in contesti quali le politiche alimentari, ambientali e sanitarie, nel contesto delle quali è stato valorizzato il principio di precauzione quale criterio fondamentale di regolazione (art. 191 TFUE)[2], la sicurezza dei prodotti[3], la protezione dei dati[4], ed oggi, la governance delle nuove tecnologie digitali e dell'intelligenza artificiale.

Occorre ricordare che il diritto dell'Unione europea si è fondato, sin dalle sue origini, su una connessione di tipo "funzionalista", sia tra rafforzamento del mercato interno e tutela dei diritti fondamentali[5] che fra tutele disposte a livello unionale e tutele previste a livello nazionale[6], che trova oggi una delle sue espressioni strategicamente più significative nella regolazione digitale[7]. È indubbio, infatti, che la declinazione

[1] Cfr. G. MAJONE, *Foundations of risk regulation: science, decision-making, policy learning and institutional reform*, in *European journal of risk regulation*, 1, 2010, 5-19; E. VOS, *Three decades of EU risk regulation research*, in *European journal of risk regulation*, 8, 2017, 47-51.

[2] Cfr. D. VOGEL, *The politics of precaution: regulating health, safety, and environmental risks in Europe and the United States*, Princeton, 2012; J. HAMMIT, M. ROGERS, P. SAND, J.B. WIENER (eds.), *The reality of precaution: comparing risk regulation in the United States and Europe*, New York, 2011; E. VOS, M. EVERSON (eds.), *Uncertain risks regulated*, London, 2009.

[3] Nell'Unione europea, il Regolamento (UE) 2023/988 sulla sicurezza generale dei prodotti impone ai fabbricanti e agli altri operatori economici l'obbligo di adottare procedure interne di analisi del rischio, documentazione tecnica e controllo di conformità, al fine di assicurare che i prodotti immessi sul mercato europeo siano sicuri (cfr. artt. 5 e 9).

[4] Come noto, il Regolamento (UE) 2016/679 (GDPR) adotta un approccio basato sul rischio (*risk-based approach*), in base al quale titolari e responsabili del trattamento devono valutare i rischi che le operazioni di trattamento comportano per i diritti e le libertà delle persone fisiche e adottare misure tecniche e organizzative adeguate per mitigarli.

[5] Cfr. E.B. HAAS, *The uniting of Europe: political, social, and economic forces*, Notre Dame, 1958; S.A. DE VRIES, *Balancing fundamental rights with economic freedoms according to the European Court of Justice*, in *Utrecht law review*, 2013; S. DOUGLAS-SCOTT, *The European Union and human rights after the Treaty of Lisbon*, in *Human rights law review*, 2011.

[6] Cfr. E. MUIR, *The fundamental rights implications of EU legislation: some constitutional challenges*, in *Common market law review*, 2014, 229 ss.

[7] In tema di tecnologie occorre fare riferimento anche alla giurisprudenza sovranazionale (Corte di Giustizia UE – CJEU – e Corte europea dei diritti dell'uomo – Corte EDU). In C-634/21 SCHUFA Holding AG, la CJEU ha esaminato il caso della valutazione del merito creditizio automatizzata (profiling) effettuata da SCHUFA Holding AG, chiarendo l'applicabilità dell'art. 22 del GDPR (decisioni automatizzate) e i connessi obblighi di trasparenza; in C-620/22, CK v Magistrat der Stadt Wien, la CJEU ha deciso (27 febbraio 2025) che, in relazione all'art. 15, para. 1, lett. h, GDPR (diritto di accesso ai dati riguardanti il soggetto), il concetto di "informazioni significative sulla logica impiegata" nelle decisioni automatizzate deve essere interpretato come diritto a una spiegazione della procedura e dei principi applicati in funzione della garanzia dell'autodeterminazione digitale; in C-460/20, TU e RE c. Google, con riferimento al diritto di cancellazione (*right to be forgotten*), la CJEU ha affermato che privati possono ottenere la de-indicizzazione di link da un motore di ricerca, come parte del loro diritto alla protezione dei dati personali e della vita privata; in C-293/12, *Digital Rights Ireland*, con la pronuncia dell' 8 aprile 2014 la CJEU ha invalidato la Data Retention Directive e indotto gli Stati membri a riformare le proprie leggi sulle telecomunicazioni. In materia di responsabilità degli

funzionalista della regolazione digitale europea, da un lato, costituisce espressione di questa connessione fra crescita economica e sviluppo del sistema dei diritti, dall'altro, può presentare un rischio di riduzione economicistica qualora non sia accompagnata da adeguate regolazioni nazionali che, oltre ad attuare la disciplina europea, siano capaci di corroborare, nei rispettivi spazi digitali, la piena promozione dei diritti. Se è vero che ancora non abbiamo una definizione consolidata e univoca di cosa si intenda per diritti digitali[8] – se si faccia riferimento con questa espressione a nuovi diritti o semplicemente alla trasposizione, con le dovute modifiche, nello spazio digitale dei diritti già individuati – attualmente la produzione normativa dell'Unione europea in materia risulta essere copiosa e particolarmente impattante sugli ordinamenti nazionali, soprattutto dal punto di vista degli oneri attuativi e conformativi all'ordinamento eurounitario[9].

intermediari digitali, nel caso Delfi AS v. Estonia (ric. n. 64569/09, 16 giugno 2015), la Corte EDU ha ritenuto responsabile un portale di notizie online per commenti anonimi diffamatori degli utenti, nonostante l'esistenza di sistemi di moderazione automatica e di rimozione su segnalazione, valorizzando il ruolo attivo e professionale dell'intermediario e la natura manifestamente illecita dei contenuti.

[8] Cfr. M. CAPORALE, *Digital rights, public administrations and the European Union law*, in *European review of digital administration & law*, 2023; M. KUZNETSOV, E. RUSAKOVA, V. ZAITSEV, *Digital rights regulation in the European Union*, in *Proceedings of the 1st International Scientific Forum on Jurisprudence* (WFLAW 2021), 2022, 45, 49; B. CUSTERS, *Imagining additional fundamental rights for the digital era*, in *Computer law & security review*, 2022.

[9] Cfr. K. MEZEI, A. TRÄGER, *Risks and resilience in the European Union's regulation of online platforms and artificial intelligence: Hungary in digital Europe*, in F. GÁRDOS-OROSZ (eds.), *The resilience of the Hungarian legal system since 2010. European Union and its neighbours in a globalized world*, Cham, 2025, 143 ss. Il ricorso sempre più frequente ai regolamenti in luogo delle direttive nel settore digitale evidenzia come tale ambito sia ormai considerato dall'Unione europea un dominio strategico per il processo di integrazione europea. In questa prospettiva, il passaggio da direttive a regolamenti in alcuni settori chiave del digitale appare emblematico. Si pensi, ad esempio, alla sostituzione della precedente direttiva sulla protezione dei dati personali con il Regolamento generale sulla protezione dei dati, che ha introdotto una disciplina uniforme in tutta l'Unione. Analogamente, nel campo dei servizi digitali, il quadro normativo originariamente definito dalla Direttiva sul commercio elettronico è stato aggiornato e rafforzato attraverso l'adozione del *Digital Services Act*, anch'esso strutturato come regolamento direttamente applicabile.

Le principali normative digitali dell'Unione europea — dal *Data Governance Act* (DGA)[10] al *Digital Services Act* (DSA)[11,] sino al *Digital Markets Act* (DMA)[12], all'*Artificial Intelligence Act* (AI Act)[13] e all'*European Health*

[10] Il *Data Governance Act* (DGA - Reg. UE 2022/868) è caratterizzato dalla finalità di creare un quadro di fiducia per la condivisione dei dati tra soggetti pubblici e privati, prevenendo abusi e distorsioni nel riutilizzo dei dati attraverso un insieme articolato di tutele giuridiche, tecniche e organizzative. Gli strumenti di governance del rischio sono i seguenti: previsione di ambienti di trattamento sicuro per dati altamente sensibili (articolo 2, punto 20; considerandа 7, 15, 26, 54); condizioni di riuso dei dati che siano non discriminatorie, trasparenti, proporzionate e giustificate e che siano compatibili con il principio di protezione dei dati personali (art. 5); meccanismi di notifica e vigilanza per i *data intermediaries* (artt. 10–14), che devono garantire neutralità e trasparenza nella gestione dei dati; misure tecniche, giuridiche e organizzative contro accessi o trasferimenti illeciti di dati (articolo 12, par. 1, lett. j–k); procedure per prevenire pratiche fraudolente o abusive (articolo 12, par. 1, lett. g); obblighi di sicurezza e riservatezza (art. 12, par. 1 lett. l), inclusi meccanismi di controllo e verificabilità e sistemi di controllo per prevenire abusi o accessi non autorizzati; registri pubblici dei fornitori di servizi di intermediazione e delle organizzazioni di altruismo dei dati, funzionali alla trasparenza e all'*accountability* del sistema (artt. 20-21); procedure di monitoraggio, segnalazione delle violazioni e applicazione di sanzioni amministrative in caso di uso improprio dei dati (artt. 26 e 34); nonché il rispetto di norme tecniche, codici di condotta e meccanismi di certificazione a supporto di un'applicazione affidabile e coerente del regolamento (considerandа 23 e 32).

[11] Il *Digital Services Act* (DSA - Reg. UE 2022/2065) ha la finalità di garantire un ambiente digitale sicuro, trasparente e conforme ai diritti fondamentali. Qui la *governance* del rischio assume una dimensione sistemica: l'obiettivo è gestire i rischi per la sicurezza, la salute pubblica, la libertà di espressione e la democrazia. Gli strumenti di governance del rischio sono i seguenti: previsione di obblighi in materia di diligenza per un ambiente digitale trasparente e sicuro (artt. 11 ss.); valutazione e mitigazione dei rischi sistemici per le *very large online platforms* (VLOPs) e i *very large online search engines* (VLOSEs) (artt. 34–35); sottoposizione per le piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi a revisioni indipendenti annuali per verificare la conformità alle misure di riduzione dei rischi (art. 37); accesso ai dati per le autorità e i ricercatori abilitati per garantire una forma di controllo pubblico (art. 40); trasparenza dei sistemi e delle pratiche di raccomandazione per le piattaforme digitali (art. 27 – trasparenza dei sistemi di raccomandazione - e art. 38 – obblighi di trasparenza rafforzati per VLOPs/VLOSEs); promozione dei codici di condotta per mitigazione dei rischi sistemici (art. 45); istituzione della funzione di controllo della conformità (art. 41); creazione del sistema di supervisione tramite coordinatori dei servizi digitali (artt. 49-51), previsione di protocolli di crisi (art. 48); poteri speciali di indagine e enforcement della Commissione (artt. 67-76).

[12] *Digital Markets Act* (DMA - Reg. UE 2022/1925) mira a garantire mercati digitali equi e contendibili attraverso una governance ex ante, preventiva e correttiva, rivolta ai *gatekeeper* e orientata a prevenire distorsioni strutturali della concorrenza e pratiche sleali. Gli strumenti di governance del rischio sono i seguenti: un sistema di obblighi e divieti ex ante (artt. 5–7) per prevenire pratiche sleali (es. *self-preferencing*, uso incrociato dei dati tra servizi della stessa piattaforma); obbligo di presentare una relazione annuale dettagliata sulle misure adottate per rispettare gli obblighi derivanti dal DMA (art. 11); riesame periodico della designazione e degli obblighi del *gatekeeper* alla luce dell'evoluzione del mercato (art. 12); indagini di mercato per la designazione dei *gatekeeper* (art. 17); indagini di mercato per pratiche sistemiche di non conformità (art. 19); indicazione delle misure di enforcement della Commissione, delle sanzioni, di misure correttive (artt. 19-30); introduzione di una funzione indipendente di controllo della conformità, con responsabili dotati di autorità, risorse e accesso all'organo di gestione (art. 28).

[13] L'*AI Act* (Reg. UE 2024/1689) adotta un approccio regolatorio basato sul livello di rischio che i sistemi di intelligenza artificiale possono comportare per i diritti fondamentali, la sicurezza e l'ordine pubblico. Tale approccio distingue quattro categorie: sistemi a rischio inaccettabile, vietati dall'art. 5; sistemi di IA ad alto rischio, definiti dall'art. 6 e sottoposti ai requisiti e agli obblighi previsti dagli artt. 8–51; sistemi a rischio limitato, soggetti a obblighi di trasparenza ai sensi dell'art. 52; e sistemi a rischio minimo o nullo, il cui utilizzo resta sostanzialmente libero in assenza di obblighi specifici. Gli operatori devono garantire, per i sistemi di IA ad alto rischio, una serie di requisiti e obblighi previsti dal regolamento: un sistema di gestione del rischio quale processo iterativo e continuo (art. 9), con identificazione, analisi e mitigazione dei rischi lungo l'intero ciclo di vita del sistema; requisiti di qualità e *governance* dei dati e predisposizione della documentazione tecnica (artt. 10-11); obblighi di registrazione automatica degli eventi (*logging*) per garantire tracciabilità e monitoraggio (art. 12); adeguata supervisione umana (art. 14); garanzie di

Data Space (EHDS)[14] — si incentrano sulla disciplina di prodotti digitali (sistemi di intelligenza artificiale, sistemi di cartelle cliniche elettroniche, etc.) e servizi digitali (servizi forniti dalle grandi piattaforme e motori di ricerca, servizi di intermediazione dei dati, etc.) da immettere sul mercato (fisico e virtuale) al fine di contribuire alla sua integrazione e concorrenzialità e si pongono nella prospettiva fondamentale di prevenire e gestire i rischi che ne possono derivare condividendo una struttura regolatoria comune fondata su alcune tecniche di *governance* del rischio già sperimentate in altri settori del diritto eurounitario[15].

In primo luogo, alcuni aspetti qualificanti di queste regolazioni includono un approccio *ex ante*, improntato alla classificazione preventiva dei rischi: si impongono valutazioni preliminari che modulano l'intensità degli obblighi regolatori in funzione del livello di rischio esistente per i diritti fondamentali, la sicurezza

accuratezza, robustezza e cybersecurity del sistema (art. 15); nonché l'obbligo per i *deployer* di effettuare una valutazione d'impatto sui diritti fondamentali (art. 27). Il regolamento prevede inoltre ulteriori strumenti di gestione del rischio, tra cui un sistema di gestione della qualità (art. 17), procedure di valutazione della conformità e marcatura CE (artt. 43–48), registrazione dei sistemi nella banca dati europea (art. 49), obblighi di segnalazione di incidenti gravi (art. 73), e meccanismi di vigilanza del mercato ed *enforcement* (artt. 74–84). Il sistema di vigilanza si fonda sulla cooperazione tra l'*European AI Office* e le autorità nazionali competenti, con la previsione di sanzioni amministrative fino al 7% del fatturato mondiale annuo per le violazioni più gravi (art. 99).

[14] L'*European Health Data Space* (EHDS - Reg. UE 2025/327) ha la finalità di creare uno spazio europeo per l'uso primario e secondario dei dati sanitari. La logica del regolamento EHDS è quella di bilanciare innovazione e tutela dei dati sanitari, prevenendo usi discriminatori o commerciali impropri attraverso un sistema multilivello di governance del rischio: il Comitato dello spazio europeo dei dati sanitari e le autorità competenti condividono informazioni su rischi, incidenti e gestione dei rischi relativi ai sistemi coinvolti (art. 92). Gli strumenti di *governance* del rischio sono i seguenti: specifiche comuni per mitigare rischi tecnici mediante prescrizioni vincolanti per interoperabilità, sicurezza, performance dei sistemi di cartelle cliniche elettroniche (art. 14–15); autorizzazioni e controlli rigorosi per l'accesso ai dati sanitari a fini di ricerca o innovazione (artt. 33–34); documentazione tecnica (art. 37); dichiarazioni di conformità UE (art. 39); istituzione di Autorità nazionali competenti per la vigilanza del mercato (art. 43); gestione dei rischi posti dai sistemi di cartelle cliniche elettroniche e misure di sicurezza avanzate per prevenire rischi di incidenti gravi (art. 44); misure correttive e restrittive in caso di non conformità (art. 63); requisiti per ambienti di trattamento sicuri per l'uso secondario dei dati sanitari, basati su garanzie tecnico-organizzative di sicurezza e protezione dei dati (art. 73 EHDS).

[15] Sulla *governance* europea del rischio, cfr. B. DELOGU (a cura di), *Risk analysis and governance in EU policy making and regulation*, Cham, 2016; A. VAN AAKEN, *Principles and structures of European risk governance, or: how (not) to play a trust game*, in B. DELOGU (a cura di), *Risk analysis and governance in EU policy making and regulation*, cit.; A.M. FARRELL, *The politics of risk and EU governance of human material*, B. DELOGU (a cura di), *in Risk Analysis and Governance in EU Policy Making and Regulation*, cit.; M.A. LANGØY, *An attribute perspective on regulatory regimes in risk governance*, in B. DELOGU (a cura di), *Risk Analysis and Governance in EU Policy Making and Regulation*, cit.

Contra cfr. A. BRADFORD, *The European rights-driven regulatory model*, in A. BRADFORD, *Digital empires: the global battle to regulate technology*, New York, 2023, 105 ss. che interpreta il modello regolatorio europeo, nel confronto con quello statunitense e cinese, come fondato sulla tutela dei diritti piuttosto che sulla integrazione dei mercati. [16] Tutti gli atti richiamati introducono, seppur con modalità differenti, un approccio preventivo alla gestione del rischio quale fondamento della regolazione. L'*AI Act* si basa su una classificazione per livelli di rischio (inaccettabile, alto, limitato, minimo) cui corrispondono obblighi proporzionati. Il *Digital Services Act* (DSA) prevede per i VLOPs e i VLOSEs obblighi di valutazione e mitigazione dei rischi sistemici (artt. 34–35). L'*European Health Data Space* (EHDS) adotta un'impostazione centrata sui rischi di reidentificazione e di uso improprio, e introduce strumenti finalizzati a garantire la qualità/accuratezza dei dati. Il *Data Governance Act* (DGA) si concentra sui rischi di abuso derivanti dall'intermediazione dei dati e dalla loro condivisione transfrontaliera. Infine, il *Digital Markets Act* (DMA) mira a prevenire i rischi per l'equità e la contendibilità all'interno dei mercati digitali.

e la protezione dei dati[16]. Tale impostazione si traduce in obblighi proporzionati e graduati, che distinguono tra rischi elevati – soggetti a vincoli stringenti e procedure di autorizzazione – e rischi minori, per i quali si privilegiano trasparenza e vigilanza leggera.

Un secondo tratto comune è rappresentato dagli obblighi di tracciabilità e accountability: registri di trasparenza, documentazione tecnica dei sistemi e delle operazioni di trattamento, nonché meccanismi di reporting e audit costituiscono strumenti centrali per garantire verificabilità, controllo pubblico e prevenzione degli abusi[17].

Completano il quadro la standardizzazione tecnica (es. marcatura CE, interoperabilità, requisiti di qualità)[18] e una governance multilivello, che distribuisce la gestione del rischio tra istituzioni europee, autorità nazionali, operatori economici e, in alcuni casi, la società civile[19]. Questo insieme coerente di strumenti e

[16] Tutti gli atti richiamati introducono, seppur con modalità differenti, un approccio preventivo alla gestione del rischio quale fondamento della regolazione. L'*AI Act* si basa su una classificazione per livelli di rischio (inaccettabile, alto, limitato, minimo) cui corrispondono obblighi proporzionati. Il *Digital Services Act* (DSA) prevede per i VLOPs e i VLOSEs obblighi di valutazione e mitigazione dei rischi sistemici (artt. 34–35). L'*European Health Data Space* (EHDS) adotta un'impostazione centrata sui rischi di reidentificazione e di uso improprio, e introduce strumenti finalizzati a garantire la qualità/accuratezza dei dati. Il *Data Governance Act* (DGA) si concentra sui rischi di abuso derivanti dall'intermediazione dei dati e dalla loro condivisione transfrontaliera. Infine, il *Digital Markets Act* (DMA) mira a prevenire i rischi per l'equità e la contendibilità all'interno dei mercati digitali.

[17] Un principio cardine che informa trasversalmente tutti questi atti è quello della trasparenza, declinato in forme differenti ma convergenti. Nell'*AI Act* esso si traduce nella previsione di obblighi di predisposizione e aggiornamento della documentazione tecnica, nella registrazione automatica degli eventi (*logging*) e nella tracciabilità dei sistemi, quali strumenti essenziali per garantire verificabilità e responsabilità. Il DSA rafforza tale impostazione imponendo ai prestatori di servizi – in particolare alle VLOP e ai VLOSE – obblighi stringenti di trasparenza e di gestione dei rischi sistemici, tra cui la redazione periodica di report sui rischi (disinformazione, impatti sui diritti fondamentali, sicurezza pubblica, tutela dei minori) e lo svolgimento di audit indipendenti annuali volti a valutare l'adeguatezza delle misure di mitigazione. Il DMA contribuisce a rafforzare la trasparenza dei mercati digitali imponendo ai *gatekeeper* obblighi specifici relativi alle proprie pratiche commerciali e al funzionamento delle piattaforme. Nel DGA la trasparenza caratterizza l'operato dei fornitori di servizi di intermediazione dei dati, chiamati a fornire informazioni chiare sulle modalità di gestione, accesso e riutilizzo dei dati. Infine, nell'EHDS la trasparenza assume una dimensione tecnico-operativa attraverso requisiti di interoperabilità, sicurezza e tracciabilità dei sistemi di cartelle cliniche elettroniche, accompagnati da procedure di test, verifica e conformità tecnica, nonché da meccanismi di gestione degli accessi e di registrazione delle operazioni.

[18] Un ulteriore principio trasversale che emerge in molti di questi atti è quello dell'interoperabilità, sostenuto attraverso la definizione di standard comuni e specifiche tecniche condivise. Nell'EHDS tale principio si traduce nella previsione di standard per le cartelle cliniche elettroniche, formati interoperabili e specifiche tecniche dettagliate (artt. 14–15), funzionali a garantire continuità assistenziale, qualità dei dati e sicurezza degli scambi informativi. Il DGA non definisce standard tecnici specifici, bensì stabilisce un quadro normativo volto a favorire il riutilizzo dei dati, la fiducia nello scambio e la creazione di spazi di dati europei, promuovendo meccanismi per facilitare il riutilizzo dei dati pubblici protetti e servizi di intermediazione neutri, contribuendo indirettamente all'interoperabilità e a condizioni uniformi di accesso ai dati. Nell'*AI Act* l'interoperabilità è collegata alla predisposizione di norme armonizzate e standard tecnici per i sistemi di intelligenza artificiale, volti ad assicurare un'applicazione uniforme del regolamento e la conformità ai requisiti essenziali di sicurezza e affidabilità. Infine, il DMA rafforza il principio attraverso disposizioni volte a garantire l'interoperabilità tra servizi digitali, in particolare nei confronti dei *gatekeeper*, al fine di promuovere contendibilità, concorrenza e libertà di scelta per utenti e imprese.

[19] Tutti gli atti si fondano su un sistema istituzionale di governance multilivello, basato sulla presenza di autorità nazionali dedicate affiancate da organismi europei di coordinamento. Nell'AI Act sono istituite autorità nazionali competenti che operano in raccordo con l'*European AI Office*. Nel DSA, i *Digital Services Coordinators* cooperano con il Board europeo per assicurare un'interpretazione uniforme e un'applicazione coerente delle norme. Nel DMA, il

principi rappresenta la cifra distintiva del modello europeo di regolazione del rischio in ambito digitale: un modello finalizzato a bilanciare dinamicamente innovazione tecnologica e rafforzamento del mercato unico.

Accanto ai menzionati elementi comuni, le normative digitali dell'Unione europea presentano anche aspetti regolatori differenziati, modellati sulle specificità dei settori regolati e sugli obiettivi di policy propri di ciascun atto. Queste differenze riguardano sia la tipologia di rischio regolato, sia le modalità di intervento, che il modello di responsabilità attribuito ai diversi attori.

Anzitutto, le differenze emergono nella natura del rischio affrontato nella sua possibile declinazione di rischio idiosincratico o sistemico. Il DGA introduce una regolazione delle attività degli intermediari di dati e del riutilizzo dei dati protetti concentrandosi sui principi di integrità e sicurezza nei processi di riuso dei dati, introducendo misure di gestione dei rischi legati alla riservatezza, alla trasparenza e all'asimmetria informativa tra attori pubblici e privati[20]; il DSA, invece, è orientato alla governance dei rischi sistemici che emergono negli ecosistemi digitali, quali la disinformazione, la diffusione di contenuti illeciti e le minacce alla libertà di espressione e ai processi democratici. Si tratta, dunque, di un modello regolatorio caratterizzato da una marcata dimensione socio-politica, volto a preservare l'integrità dello spazio pubblico digitale e a garantire un ambiente digitale sicuro, pluralistico e rispettoso dei diritti fondamentali[21]; il DMA si occupa di rischi concorrenziali, prevenendo abusi di posizione dominante da parte dei *gatekeepers* con misure *ex ante* fortemente correttive[22]; l'EHDS introduce una regolazione imperniata sulla tipologia del dato sanitario digitale considerato (primario o secondario) e sui meccanismi di accesso ai dati, con l'obiettivo di affrontare i rischi connessi alla particolare sensibilità delle informazioni sanitarie. In questa prospettiva, il regolamento mira a prevenire fenomeni quali la reidentificazione, l'uso discriminatorio dei dati o qualsiasi trattamento che possa compromettere la privacy, la dignità e, più in generale, i diritti fondamentali delle persone[23]. Infine, l'*AI Act* adotta un modello di classificazione stratificato su quattro livelli, che identifica il rischio in funzione dell'impatto che un sistema di intelligenza artificiale può produrre sul singolo individuo o sulla collettività[24].

Un secondo elemento di diversificazione riguarda i modelli di responsabilità adottati. Nel DGA e nell'EHDS, il fulcro della disciplina è rappresentato dalla fiducia e dalla neutralità dell'intermediario o del soggetto incaricato della custodia dei dati. A tali attori è richiesto di garantire standard di sicurezza elevati, condizioni di utilizzo non discriminatorie e una gestione trasparente dei flussi informativi, così da assicurare un

modello è maggiormente centralizzato, attribuendo alla Commissione europea il ruolo primario di vigilanza e enforcement nei confronti dei *gatekeeper*. Nel DGA, le autorità di intermediazione dei dati condividono competenze e flussi informativi con l'*European Data Innovation Board*, volto a promuovere *standard* comuni e pratiche armonizzate negli spazi europei di dati. Infine, nell'EHDS, le autorità nazionali per la salute digitale svolgono le proprie funzioni in raccordo con il Comitato dello spazio europeo dei dati sanitari, che garantisce il coordinamento a livello dell'Unione.

[20] Cfr. art. 5 del DGA.

[21] Cfr. sui rischi sistemici artt. 34-35; sulla disinformazione art. 34 e *consideranda* 68-70; sulla libertà di espressione artt. 14, 34 e 48 del DSA.

[22] Cfr. artt. 3, 5, 6 del DMA.

[23] Cfr. artt. 5-7, 14-15, 33-38, 50-53 dell'EHDS.

[24] Cfr. artt. 5 (sistemi vietati) e 6 (sistemi ad alto rischio) del Regolamento (UE) 2024/1689 sull'intelligenza artificiale. Per le categorie di rischio limitato (capo IV) e per i sistemi di rischio minimo, non sono previsti requisiti stringenti e uniformi analoghi a quelli stabiliti per i sistemi ad alto rischio.

ecosistema data-driven affidabile e orientato alla tutela degli interessi degli individui e delle comunità[25]. Il DSA introduce un regime di responsabilità graduata basata sulla dimensione della piattaforma (VLOPs - *Very Large Online Platforms*/VLOSEs - *Very Large Online Search Engines*), con la previsione di obblighi crescenti proporzionali al potenziale impatto sistemico[26]. A sua volta, il DMA rovescia la logica classica del modello antitrust tradizionale fondato sul controllo ex post, sostituendola con un sistema di obblighi ex lege imposti alle grandi piattaforme digitali che, sulla base di criteri quantitativi e qualitativi stabiliti dal regolamento, sono qualificate come *gatekeeper*, operando tale qualificazione a prescindere dalla prova di un abuso, ma configurando un modello di responsabilità strutturale volto a prevenire condotte distorsive e a preservare l'equità e la contendibilità dei mercati digitali[27], mentre l'*AI Act* affida l'onere della dichiarazione di conformità principalmente al fornitore del sistema di IA, il quale è tenuto ad attivare in autonomia procedure di valutazione, documentazione e mitigazione del rischio lungo l'intero ciclo di vita del prodotto, configurandosi un modello di responsabilizzazione preventiva, in cui il provider deve garantire che il sistema soddisfi i requisiti essenziali di sicurezza, trasparenza, qualità dei dati e governance del rischio, prima e durante la sua immissione e permanenza sul mercato[28].

Infine, anche gli strumenti regolatori principali differiscono: l'*AI Act* enfatizza in modo significativo la standardizzazione tecnica e la dimensione certificativa, prevedendo l'adozione di standard comuni, norme tecniche armonizzate e procedure di valutazione della conformità che culminano nella marcatura CE dei sistemi ad alto rischio[29]; il DMA si incentra su strumenti economico-concorrenziali di immediata cogenza, imponendo obblighi direttamente applicabili ai *gatekeeper* senza necessità di dimostrare, caso per caso, un abuso di posizione dominante[30]; il DSA valorizza in modo centrale gli strumenti volti alla gestione dei rischi sistemici e alla trasparenza, includendo tra i meccanismi chiave di controllo pubblico anche l'accesso dei ricercatori abilitati ai dati delle piattaforme[31]; l'EHDS si fonda su strumenti specificamente orientati al controllo degli accessi e alla garanzia della qualità del dato, al fine di assicurare un utilizzo sicuro, affidabile e tecnicamente adeguato delle informazioni sanitarie digitali[32]; mentre il DGA si basa su strumenti volti a garantire la neutralità dell'intermediario e a rafforzare la fiducia nei servizi di intermediazione dei dati[33].

[25] Cfr. artt. 12-13 del DGA; artt. 51 e 54 dell'EHDS.
[26] Cfr. artt. 33-43 del DSA.
[27] Cfr. artt. 3, 5, 6 del DMA.
[28] Cfr. artt. 9, 11, 16 dell'*AI Act*.
[29] Cfr. artt. 40-48 dell'*AI Act*.
[30] Cfr. artt. 3 e 5–7 e, quanto ai poteri di *enforcement* della Commissione, in particolare gli artt. 18–21 e 29–30 del DMA.
[31] Cfr. art. 40 e considerando 97-98 del DSA.
[32] Tale impostazione emerge, nell'ambito dell'EHDS, dagli articoli 5–7, relativi all'accesso e all'utilizzo dei dati sanitari elettronici nell'uso primario; dagli articoli 14–15, che stabiliscono standard tecnici e requisiti di interoperabilità per i sistemi di cartella clinica elettronica; e dagli articoli 33–38, che disciplinano gli obblighi dei fabbricanti e degli altri operatori economici dei sistemi EHR, prevedendo requisiti di documentazione tecnica, informazione agli utenti e conformità ai requisiti di sicurezza, interoperabilità e qualità dei sistemi.
[33] Tale principio è sancito, nell'ambito del DGA, dagli articoli 11–14, che impongono obblighi di indipendenza, assenza di conflitti di interesse e condizioni eque e non discriminatorie per l'intermediazione; nonché sulla base degli articoli 29-30 prevedendo meccanismi di coordinamento e orientamento a livello europeo, affidati al Comitato europeo per l'innovazione in materia di dati, al fine di garantire un'applicazione coerente e affidabile delle regole di governance dei dati.

In sintesi, le differenze tra le normative digitali unionali riflettono non una frammentazione settoriale, considerato anche che i regolamenti digitali "dialogano" fra loro[34], ma una adattabilità funzionale del modello della regolazione digitale europea alle specificità dei singoli settori[35]: un impianto di governance del rischio condivisa ma flessibile, capace di declinarsi in forme diverse a seconda del contesto tecnologico, degli attori coinvolti e degli interessi in gioco.

In questa prospettiva, è opportuno rimarcare come la più recente regolazione europea in materia digitale sia stata, in ogni caso, collocata all'interno di un impianto caratterizzato da un approccio programmatico antropocentrico — esplicitamente menzionato, tra l'altro, al punto n. 9, lett. A, della Dichiarazione europea sui diritti e i principi digitali (2022)[36], e richiamato nell'*AI Act* (Reg. UE 2024/1689)[37].

Nel quadro attuale, la regolazione risponde alla funzione di protezione — garantendo sicurezza e prevenzione dei rischi — mentre sul piano programmatico, nell'ambito di un percorso decennale di transizione digitale[38], l'ordinamento unionale promuove esplicitamente anche una regolazione nazionale orientata

[34] Nel loro insieme, i regolamenti digitali europei si "parlano" attraverso una rete di rinvii incrociati che non è casuale, ma esprime una strategia normativa integrata: ciascun atto mantiene la propria autonomia funzionale, ma opera in coordinamento con gli altri per governare, da prospettive diverse, i rischi connessi al potere digitale. Al GDPR rinviano trasversalmente l'*AI Act*, il DSA, il DMA, il DGA e l'EHDS. Tra DSA e DMA operano clausole di coordinamento orizzontale; rinvii funzionali e sistematici caratterizzano i rapporti tra DSA e *AI Act* e tra *AI Act* e EHDS; mentre tra EHDS e DGA si configura un coordinamento di tipo funzionale, fondato sul rapporto tra disciplina orizzontale e regolazione settoriale.

[35] Occorre segnalare che la Commissione europea ha presentato il 19 novembre 2025 il cosiddetto *Digital Omnibus Package*, composto da due proposte di regolamento: COM(2025) 836 final, che modifica i regolamenti (UE) 2024/1689 e (UE) 2018/1139 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale, e COM(2025) 837 *final*, relativo a interventi di semplificazione e coordinamento del quadro normativo digitale dell'UE. Tale pacchetto regolativo mira a razionalizzare il quadro normativo digitale dell'Unione europea, incidendo su diverse discipline – tra cui protezione dei dati, governance dei dati, intelligenza artificiale e sicurezza informatica – al fine di ridurre sovrapposizioni regolatorie e semplificare gli obblighi di *compliance*.

[36] La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale del 2022 definisce un quadro di principi fondamentali, quali la centralità della persona, la necessità di inclusione e solidarietà, la garanzia di libertà di scelta, la partecipazione civica nello spazio pubblico digitale, la sicurezza dei dati e la sostenibilità delle tecnologie, che orientano l'impiego delle nuove tecnologie nello spazio digitale dell'Unione. Essa impegna gli Stati membri e le Istituzioni europee, nell'ambito delle rispettive competenze, a tutelare i diritti delle persone e a garantire che la transizione digitale avvenga in modo equo, inclusivo e sostenibile, nel rispetto dei valori dell'Unione e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE.

[37] Il Regolamento (UE) 2024/1689 richiama espressamente, anche sulla base del *White paper on AI*, l'approccio antropocentrico in più punti del testo normativo. Tale orientamento è affermato nei *consideranda* 1, 6 e 8, che ribadiscono la centralità della persona umana nello sviluppo, nell'impiego e nel controllo dei sistemi di intelligenza artificiale. Il riferimento ricompare nel *considerandum* 176, relativo agli obblighi di *governance* e supervisione umana. Il principio è inoltre formalizzato nell'articolo 1, paragrafo 1, che definisce la finalità del Regolamento nel garantire che i sistemi di IA operino in modo sicuro e rispettoso dei diritti fondamentali, della dignità umana e dei valori dell'Unione.

[38] Cfr. Decennio digitale europeo: obiettivi digitali per il 2030. L'agenda digitale dell'Unione europea assume un ruolo strategico per lo sviluppo economico e per il rafforzamento del mercato interno. Sul piano delle politiche sociali, essa sottolinea le potenzialità delle nuove tecnologie nel creare occupazione, migliorare la salute, potenziare l'assistenza sociale e costruire uno spazio digitale sicuro. Tali obiettivi trovano sintesi nel percorso per il decennio digitale, che fissa al 2030 l'orizzonte temporale della transizione. In questo quadro si colloca la Comunicazione COM (2021) 118 *final* del 9 marzo 2021 (Bussola per il digitale 2030), che delinea gli indirizzi per l'evoluzione digitale europea. Rilevante anche il Libro bianco del 14 aprile 2022, volto a proporre la digitalizzazione di alcuni aspetti del processo elettorale per ridurre l'astensionismo involontario.

alla dimensione antropocentrica nella prospettiva dello sviluppo delle capacità, dell'inclusione e dell'autonomia delle persone.

3. Il quadro nazionale: verso un paradigma promozionale

3.1. L'identità costituzionale nel settore digitale

Come noto, l'identità costituzionale rappresenta, nel diritto dell'Unione, il nucleo essenziale dei principi e delle strutture fondamentali che definiscono l'ordinamento di ciascuno Stato membro[39].
Si tratta, dunque, di una sorta di clausola di salvaguardia che delimita l'integrazione europea, imponendo all'Unione di rispettare i valori e i principi costituzionali fondamentali, compresi quelli relativi ai diritti fondamentali e alla sovranità democratica.
In altri termini, l'art. 4, paragrafo 2, del TUE stabilisce un equilibrio dinamico tra integrazione europea e sovranità nazionale, riconoscendo che l'appartenenza all'Unione non può compromettere l'identità fondante e costituzionale degli Stati membri[40].
Nel passaggio dallo standard eurounitario della protezione dai rischi al paradigma nazionale della promozione dei diritti è possibile cogliere il senso peculiare di questa nozione.
Nel contesto della progressiva digitalizzazione delle strutture e dei servizi, l'art. 4, para. 2, del TUE può essere letto come fondamento per lo sviluppo di un'identità costituzionale digitale nazionale, in quanto l'Unione promuove un quadro comune di regolazione tecnologica, ma gli Stati conservano, all'interno dei margini normativi lasciati alla loro discrezionalità, il diritto e il dovere di declinare tali strumenti in coerenza con la propria identità costituzionale, ossia con i principi fondamentali che definiscono la relazione tra persona, diritti e istituzioni.
Per il nostro ordinamento costituzionale, ciò significa che la digitalizzazione dei servizi a tutela dei diritti fondamentali deve essere primariamente orientata dai principi personalisti, solidaristici e partecipativi della Costituzione (artt. 2, 3, 118)[41], che possono rappresentare una declinazione concreta dell'identità costituzionale italiana nello spazio digitale[42].

---

[39] Sulla nozione di identità costituzionale, cfr. P. FARAGUNA, *Alla ricerca dell'identità costituzionale tra conflitti giurisdizionali e negoziazione politica*, in *Costituzionalismo.it*, 3, 2016; P. FARAGUNA, *Unamendability and constitutional identity in the Italian constitutional experience*, in *European journal of law reform*, 2019; F. FABBRINI, O. POLLICINO, *Constitutional identity in Italy: European integration as the fulfilment of the Constitution*, in *EUI law working paper*, 2017; S. POLIMENI, *L'identità costituzionale come controlimite*, in *Ianus*, 2017.

[40] L'articolo 4, paragrafo 2, TUE stabilisce che «L'Unione rispetta l'uguaglianza degli Stati membri dinanzi ai Trattati nonché la loro identità nazionale, insita nelle strutture fondamentali politiche e costituzionali, compreso il sistema delle autonomie locali e regionali. Essa rispetta le funzioni essenziali dello Stato, in particolare per quanto riguarda la salvaguardia della sua integrità territoriale, il mantenimento dell'ordine pubblico e la tutela della sicurezza nazionale».

[41] Come osserva Fares, l'introduzione delle nuove tecnologie nei diritti sociali impone di «rimodellare le regole del gioco» nel bilanciamento tra efficienza tecnologica e tutela della dignità, dell'autonomia e dell'eguaglianza. Cfr. G. FARES, Diritti sociali e nuove tecnologie, GdP Genova 18-19 giugno 2021, 2 ss., accessibile al link https://gruppodipisa.it/images/convegni/2021_Convegno_Genova/Guerino_Fares_Diritti_sociali_e_nuove_tecnologie.pdf (ultima consultazione 12/03/2026).

[42] Sul costituzionalismo digitale, cfr. A. SIMOCINI, E. LONGO, *Digital constitutionalism and fundamental rights: reconfiguring liberty and power*, in G. DE GREGORIO, O. POLLICINO, P. VALCKE (eds.), *The Oxford handbook of digital constitutionalism*, Oxford, 2026; E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in *International review of*

È possibile affermare che l'identità costituzionale digitale italiana si possa fondare, pertanto, su tre assi portanti[43]. Anzitutto, sulla centralità della persona e sulla dignità umana (art. 2 Cost.), che impongono di considerare la tecnologia come strumento abilitante delle libertà e non come fattore di deresponsabilizzazione o sostituzione dell'umano. In secondo luogo, sulla solidarietà come principio fondamentale in materia di tutela effettiva delle persone maggiormente vulnerabili, poiché le piattaforme digitali e le innovazioni implementate possono costituire, ove gestite secondo precisi canoni, potenti strumenti di uguaglianza sostanziale, contribuendo a ridurre le diseguaglianze territoriali, sociali ed economiche. Infine, sul principio di autonomia e partecipazione (artt. 3, 48 e 118 Cost.), che apre a nuove forme di cittadinanza digitale, di amministrazione condivisa e di sussidiarietà tecnologica, nelle quali le persone e le comunità non sono solo utenti, ma co-produttori di valore pubblico, contribuendo in modo attivo alla progettazione, al controllo e alla valutazione delle soluzioni digitali che li riguardano.

3.2. Priorità costituzionali e infrastrutture abilitanti: verso una giurisprudenza della dignità tecnologicamente mediata

Il tema delle infrastrutture abilitanti[44], orientate tanto sul piano normativo quanto su quello tecnologico alla promozione e allo sviluppo della persona umana, si intreccia profondamente con la questione delle priorità costituzionali[45], sollecitando una riflessione sul modo in cui il progresso tecnologico possa essere ricondotto entro la cornice dei principi fondamentali e orientato alla realizzazione effettiva dei diritti di cittadinanza.

Nell'ambito della giurisprudenza costituzionale sulle priorità di spesa, la sentenza della Corte costituzionale n. 195 del 2024 offre un punto di riferimento significativo per comprendere come, all'interno dell'ordinamento costituzionale, sia possibile definire le gerarchie tra le diverse destinazioni di risorse pubbliche. In particolare, la Corte ribadisce che la spesa costituzionalmente necessaria – specie nel settore della tutela della salute e delle politiche sociali ove la copertura dei costi è finalizzata a garantire livelli essenziali delle prestazioni (LEP) il cui soddisfacimento costituisce presupposto per l'effettività dei diritti – assume

law, computers & technology, 2019; ID., *Constitutionalism in the digital age*, in J. POHLE, R. SCHWARZ, U. HÖPPNER (eds.), *Don't give up, stay idealistic and try to make the world a better place*, in *Liber amicorum for Ingolf Pernice*, Berlin, 2020; G. DE GREGORIO, *Digital constitutionalism in Europe. Reframing rights and powers in the algorithmic society*, Cambridge, 2022; G. DE GREGORIO, R. RADU, *Digital constitutionalism in the new era of internet governance*, in *International journal of law and information technology*, 2022.

[43] Per alcuni elementi fondamentali del dibattito nell'ordinamento italiano, cfr. M. OLIVETTI, *Diritti fondamentali e nuove tecnologie: una mappa del dibattito italiano*, in *Revista estudos institucionais*, 2020; P. PASSAGLIA, *Internet nella costituzione italiana: considerazioni introduttive*, in *Consulta online*, 2013; S. SCAGLIARINI, *Identità digitale e tutela della privacy*, in *relazione al Convegno annuale dell'Associazione 'Gruppo di Pisa'*, Genova, 18-19 giugno 2021; A. LAMBERTI, *Costituzionalismo digitale*, in *Consulta online*, 2, 2025.

[44] Sulla *capability approach*, si vedano A. SEN**,** *Commodities and capabilities*, New York-Oxford, 1985; M.C. NUSSBAUM, *Creating capabilities: the human development approach,* Cambridge, 2011.

[45] Sul tema, cfr. L. CARLASSARE, *Priorità costituzionali e controllo sulla destinazione delle risorse*, in *Costituzionalismo.it*, 1, 2013; C. SALAZAR, *Sui diritti sociali e il principio di solidarietà*, in *Rivista AIC*, 1, 2024; F. GABRIELE, *Diritti sociali, unità nazionale e risorse (in)disponibili: sulla permanente violazione-inattuazione della parte prima (quella "intoccabile"!) della costituzione*, in *Rivista AIC*, 3, 2013; F. MODUGNO, *Interpretazione costituzionale*, in *Annali della Facoltà Giuridica dell'Università di Camerino*, 8, 2019.

un rilievo prioritario, imponendo che, in un contesto di risorse limitate, siano ridotte in via preferenziale le spese indistinte rispetto a quelle volte a garantire i diritti sociali fondamentali[46].

Questa prospettiva risulta oggi di particolare attualità se letta alla luce del potenziale abilitante delle nuove tecnologie nel campo della promozione dei diritti fondamentali. Strumenti digitali, intelligenza artificiale, telemedicina e piattaforme di *welfare* innovativo non costituiscono solo costi, ma investimenti strategici funzionali a realizzare la spesa costituzionalmente necessaria, in quanto permettono di rendere maggiormente effettiva la tutela dei diritti fondamentali.

In questo senso, si può osservare come l'innovazione tecnologica stia progressivamente penetrando nelle aree di maggiore criticità dei servizi sanitari e sociali, incidendo in modo diretto sull'accessibilità e sulla qualità delle prestazioni. Gli ambiti che meglio esemplificano tale dinamica riguardano, ad esempio, l'integrazione socio-sanitaria (con le piattaforme digitali integrate per la condivisione dei dati clinici e socio-sanitari, i teleconsulti multidisciplinari, gli strumenti di case management digitale), la sanità territoriale (con la telemedicina e il telemonitoraggio, le Centrali operative territoriali digitalizzate (COT), la robotica assistiva e domotica) e le situazioni di fragilità socio-economica (con gli sportelli digitali inclusivi, i sistemi di *welfare* digitale**,** le tecnologie per la mediazione interculturale digitale).

La preferenza qualitativa riconosciuta alle spese dirette alla tutela dei diritti sociali può essere, dunque, interpretata come un principio di orientamento anche per le scelte di innovazione tecnologica pubblica, orientandole verso soluzioni capaci di ridurre le diseguaglianze di accesso e potenziare la capacità del sistema di rispondere ai bisogni delle fasce più fragili.

In tale contesto, nella sentenza n. 275 del 16 dicembre 2016, la Corte costituzionale ha affermato con chiarezza che la tutela delle persone con disabilità costituisce una priorità costituzionale, superiore anche alle esigenze di bilancio o ai vincoli finanziari delle amministrazioni pubbliche[47].

Nell'orientamento consolidato della Corte viene, ad esempio, affermato che la condizione giuridica della persona con disabilità è il punto di confluenza di un complesso di principi «che attingono ai fondamentali motivi ispiratori del disegno costituzionale»[48].

Secondo tale orientamento, deve essere letta anche la recente sentenza n. 3 del 2025 della Corte costituzionale che dichiara l'illegittimità costituzionale degli artt. 9, terzo comma, della legge 17 febbraio 1968, n. 108, "Norme per la elezione dei Consigli regionali delle Regioni a statuto normale, e 2, comma 6, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale – CAD", nella parte in cui non

[46] A partire dalla sentenza della Corte costituzionale n. 169 del 2017 (e poi nelle sentenze n. 87 del 2018, n. 197 del 2019, n. 220 del 2021 e n. 45 del 2025), la nozione di spesa costituzionalmente necessaria ha progressivamente assunto una valenza dinamica: essa non solo individua i settori che devono essere preservati dai tagli, ma potrebbe essere letta come una prefigurazione di quei settori nei quali l'innovazione tecnologica può ampliare l'efficacia e la sostenibilità della tutela dei diritti fondamentali. In tal senso, l'impiego delle tecnologie digitali e dell'intelligenza artificiale nei servizi di cura e assistenza può essere considerato parte integrante della realizzazione dei diritti costituzionalmente previsti, nella misura in cui consente di superare barriere territoriali, economiche e sociali, garantendo una più equa accessibilità alle prestazioni sanitarie e assistenziali.

[47] Nel paragrafo 3.1 del considerato in diritto della sentenza della Corte costituzionale n. 275 del 2016 si legge: «È la persona, con la sua dignità, a venire prima di ogni altra logica, anche di bilancio. La garanzia dei diritti incomprimibili deve essere sempre assicurata, poiché nessuna esigenza finanziaria può giustificare il sacrificio dei diritti fondamentali della persona».

[48] Cfr., *ex plurimis*, sentenza della Corte costituzionale n. 42 del 2024, che richiama la sentenza n. 83 del 2019, e, nello stesso senso, la sentenza n. 110 del 2022.

prevedono per l'elettore, che non sia in grado di apporre una firma autografa per certificata impossibilità derivante da un grave impedimento fisico o perché si trova nelle condizioni per esercitare il voto domiciliare, la possibilità di sottoscrivere un documento informatico con firma elettronica qualificata, cui è associato un riferimento temporale validamente opponibile ai terzi[49].

La questione, sollevata dal Tribunale di Civitavecchia, si incentra sulla possibile natura discriminatoria della norma nei confronti delle persone con disabilità, rilevando i parametri di cui agli artt. 2, 3, 48 e 49 Cost.[50].

Nella motivazione la Corte prende in considerazione il fattore dinamico dell'evoluzione tecnologica e dell'inclusione digitale considerando che il CAD promuove la digitalizzazione delle pubbliche amministrazioni, ma esclude ancora dai processi di digitalizzazione le "consultazioni elettorali". Tale esclusione ha determinato l'impossibilità per le persone con disabilità di utilizzare la firma digitale in fase di presentazione delle liste[51].

Questo approdo normativo si pone in tensione con il principio personalista sancito dall'art. 2 Cost.**,** il quale impone di riconoscere che la dignità della persona risulta lesa ogniqualvolta sia lo stesso ordinamento giuridico a produrre – attraverso una determinata previsione o un divieto – una condizione di inabilità giuridica o di bisogno artificiale di assistenza in capo a un soggetto che, sul piano sostanziale e realistico, sarebbe pienamente in grado di svolgere l'attività in questione[52]. In tali casi, infatti, non è la persona a essere realmente incapace, ma è la norma stessa che, mediante una scelta eteronomica, la priva di autonomia, contraddicendo la finalità costituzionale di promuovere lo sviluppo e la responsabilità individuale. Ribadita la necessità di favorire la partecipazione democratica e rimuovere gli ostacoli (art. 3, comma 2, Cost.), la Corte cita la Convenzione ONU sui diritti delle persone con disabilità e la legge 22 dicembre 2021, n. 227, recante "Delega al Governo in materia di disabilità".

Viene affermata l'inadeguatezza della disciplina tradizionale di riferimento (art. 28 DPR 570/1960) poiché la procedura verbale davanti a testimoni e notaio per chi non può firmare è ormai sproporzionata e lesiva della dignità, data la possibilità tecnologica di firmare digitalmente.

Il *tertium comparationis* individuato dalla Corte è rappresentato dall'art. 1, comma 344, della legge 30 dicembre 2020, n. 178, "Bilancio di previsione dello Stato per l'anno finanziario 2021", che ammette la

[49] Su questa sentenza si veda L. TRUCCO, *La possibilità di sottoscrizione digitale delle candidature: dall'amministrazione del Lazio alla libertà della persona*, in *Le regioni*, 3, 2025.

[50] Il fatto alla base della questione di costituzionalità vede il ricorrente, affetto da SLA, disposto a sottoscrivere una lista elettorale regionale tramite firma digitale, di cui disponeva e che usava autonomamente.
Gli uffici elettorali e Regione Lazio avevano negato questa possibilità, richiamando l'art. 2, comma 6, CAD, che esclude le consultazioni elettorali dal suo ambito di applicazione.

[51] In riferimento a queste situazioni, in particolare con riguardo alle persone che non sono in grado di apporre una firma autografa ma risultano capaci, utilizzando le moderne tecnologie, di apporne una digitale, la preclusione derivante dall'art. 2, comma 6, CAD, incide sui loro diritti politici di cui agli artt. 48 e 49 Cost., tra cui senz'altro rientra quello di sottoscrivere una lista di candidati che possa essere sottoposta al voto degli elettori; si tratta, infatti, di una attività che, concorrendo alla formazione dell'offerta elettorale, attiene direttamente al diritto di elettorato attivo. Il soggetto, grazie allo sviluppo tecnologico, *id est* la firma digitale, ben potrebbe autonomamente apporre la sottoscrizione necessaria alla presentazione delle candidature, se non incontrasse la preclusione derivante dall'art. 2, comma 6, CAD, che invece lo trasforma, dal punto di vista formale e giuridico, in un inabile, costringendolo a dover ricorrere alla più gravosa e complessa dichiarazione verbale resa davanti a due testimoni e a un soggetto abilitato a verbalizzarla, secondo quanto previsto dall'art. 28, quarto comma, del d.P.R. n. 570 del 1960.

[52] Su questo si veda, in particolare, il paragrafo 4.2 del considerato in diritto della sentenza in discorso n. 3 del 2025.

sottoscrizione mediante firma digitale per i referendum e le iniziative legislative popolari, ma non per le elezioni, determinando così una differenza di disciplina che è stata, pertanto, sottoposta a sindacato costituzionale alla luce dei principi di ragionevolezza e di eguaglianza.

La Corte conclude affermando un principio rilevantissimo, per la materia che ci occupa, ossia che le persone con disabilità devono poter utilizzare la firma digitale per esercitare i propri diritti politici, poiché la tecnologia costituisce strumento di autonomia, dignità e partecipazione democratica, concludendo che l'esclusione assoluta della firma digitale dalle consultazioni elettorali è irragionevole e contraria agli artt. 2, 3, 48 e 49 Cost.[53].

Sulla stessa linea e nel senso della promozione della dimensione personalista delle nuove tecnologie, occorre ricordare l'ordinanza, anch'essa recente, della I Sezione della Cassazione civile del 5 febbraio 2025, n. 6584, che presenta un suo peculiare carattere "costituzionale" in materia di validità e adeguatezza degli strumenti di tutela delle persone vulnerabili. La pronuncia ha ad oggetto il ricorso contro il decreto del Tribunale di Bolzano che aveva confermato l'amministrazione di sostegno per un uomo con disabilità fisica (deficit di linguaggio e udito) ma pienamente lucido e autonomo[54].

In questo caso la Cassazione ha accolto il ricorso poiché il provvedimento del giudice del reclamo è stato ritenuto dal giudice di legittimità intrinsecamente contraddittorio. Il giudice del reclamo aveva, infatti, confermato la capacità del ricorrente di autodeterminarsi e tuttavia aveva confermato il provvedimento del giudice tutelare di nomina di un amministratore di sostegno in ragione di una disabilità fisica di cui il ricorrente era portatore sin dalla nascita e che non aveva inciso sulla possibilità di condurre una vita autonoma.

Qui il giudice di legittimità aggiunge un elemento ulteriore e specifico in riferimento alle disabilità fisiche del ricorrente, relative all'udito e all'uso della parola, ossia che rappresentano ostacoli naturalistici che possono essere superati attualmente con la promozione istituzionale del ricorso a strumenti e tecnologie (dispositivi tecnologici, strumenti di comunicazione dedicati a chi ha questo tipo di problematiche, etc.) che abilitano la persona a superare le difficoltà esistenti nell'ottica della effettiva garanzia dei loro diritti.

A fronte di questa rilevante distinzione tra ostacoli naturali e ostacoli giuridici, la valutazione giudiziaria rappresenta il livello istituzionalmente più idoneo a bilanciare i diversi interessi in gioco e a verificare, caso per caso, se la persona sia in grado di gestire autonomamente i propri interessi mediante l'impiego di strumenti tecnologici, ausili digitali o reti di supporto familiare. In questa prospettiva, la funzione giudiziale diventa un presidio essenziale per evitare che l'ordinamento produca barriere giuridiche indebite e, al contrario, per garantire che l'autonomia della persona sia valutata nella sua effettiva dimensione concreta e relazionale.

---

[53] In materia, si vedano N. FIANO, *Il legislatore alla prova della digitalizzazione della raccolta delle firme per promuovere referendum e leggi di iniziativa popolare e… per la presentazione delle candidature alle elezioni?*, in *Rivista del Gruppo di Pisa*, 1, 2023; S. CECCANTI, *Firme elettroniche anche per la presentazione delle liste elettorali: il salto da fare nella SPID democracy, come e perché*, in *Nomos. Le attualità nel diritto*, 3, 2022; S. TROILO, *L'iniziativa popolare nei referendum di riforma costituzionale in Italia*, in C. GARRIDO LÓPEZ, E. CEBRIÁN ZAZURCA (a cura di), *La iniciativa ciudadana vinculada al referéndum: modelos comparados*, Madrid, 2023, 255-277.

[54] Il fatto posto a base della controversia riguarda un ricorrente, invalido al 100%, il quale viveva da solo, guidava e gestiva in piena autonomia la propria vita quotidiana. La nipote del ricorrente aveva chiesto la nomina di un amministratore di sostegno; il giudice tutelare aveva accolto l'istanza e poi il Tribunale aveva confermato tale provvedimento. L'interessato ricorre in Cassazione denunciando violazione degli artt. 404 ss. c.c. e dell'art. 12 della Convenzione ONU sui diritti delle persone con disabilità (CRPD).

In tal senso, la Corte di cassazione conclude con nettezza che l'adozione di una misura limitativa della capacità, quale l'amministrazione di sostegno, costituisce un'interferenza nell'autonomia personale che può ritenersi ammissibile solo quando sia specificamente giustificata, necessaria e proporzionata rispetto alle effettive condizioni del beneficiario. In tale prospettiva, la disabilità – in particolare quando incida su funzioni fisiche come l'udito o il linguaggio – non può essere considerata di per sé un limite alla capacità di agire, soprattutto ove risulti che tali menomazioni possono essere compensate mediante strumenti tecnologici, dispositivi di supporto o adeguate reti familiari e sociali.
Come sottolineato dalla Corte, con un'argomentazione molto simile a quella che abbiamo rilevato nella sentenza summenzionata della Corte costituzionale n. 3 del 2025, il principio personalista di cui all'art. 2 Cost. impone di riconoscere che la dignità della persona è vulnerata ogniqualvolta sia l'ordinamento stesso, attraverso un proprio divieto o una propria previsione, a trasformare in "inabile" un individuo che sarebbe invece in grado, con l'ausilio di mezzi adeguati, di compiere autonomamente determinate attività. L'intervento ordinamentale deve pertanto orientarsi sempre verso il riconoscimento delle capacità residue e potenziabili, evitando che la misura adottata si traduca in una compressione ingiustificata dell'autodeterminazione. La tecnologia, in questo quadro, non rappresenta soltanto oggetto di protezione passiva, ma diviene un vero e proprio mezzo di promozione dell'autonomia e della dignità, capace di abilitare l'espressione della volontà della persona vulnerabile e di sostenere la gestione indipendente e autonoma della sua vita e dei suoi interessi.

3.3. Le riforme abilitanti nei rapporti fra tecnologie e vulnerabilità

Nel contesto della progressiva digitalizzazione dei servizi a tutela dei diritti fondamentali, come è emerso nel corso della trattazione, la categoria della vulnerabilità assume una rilevanza crescente[55].
La vulnerabilità si configura sempre più come una nozione complessa e multidimensionale che si pone in un rapporto bidirezionale e ambivalente con la digitalizzazione e il crescente ricorso alle tecnologie[56].
Da una parte, la vulnerabilità può costituire il risultato di processi tecnologicamente mediati di tutela dei diritti fondamentali qualora i rischi delle nuove tecnologie incidano su situazioni preesistenti determinando possibilità di esclusione digitale, asimmetria informativa, dipendenza, incapacitazione cognitiva[57];

[55] Cfr. sul rilievo della categoria e sulla nozione di *digital inclusion*, cfr. M.R. BARTOLOMEI, A. CAVA, *Vulnerability, digital technologies and international law: reflections on contemporary migration flows*, in *Law, technology and humans*, 2024.
[56] Sulle vulnerabilità digitali, cfr. H. SAKARIASSEN, *Multidimensional digital vulnerability among older adults*, in *Nordicom review*, 46, 2025; Z. ESPINOSA ZÁRATE, C. CAMILLI J. PLAZA-DE-LA-HOZ, *Digitalization in vulnerable populations: a systematic review in Latin America*, in *Social indicators research*, 170, 2023; A. ROSSI, R. CARLI, M.W. BOTES, A. FERNANDEZ, A. SERGEEVA, L. SÁNCHEZ CHAMORRO, *Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multidimensional nature of digital vulnerability*, in *Computer law & security review*, 55, 2024; M. GEORGIOU, L. D'HAENENS, A. ZAKI, V. DONOSO, E. BOSSENS, *Digital skills of and for lives marked by vulnerability: being young, refugee, and connected in Europe*, in *European journal of communication*, 39, 2024; M. BECK, *Empowering vulnerability: the social model of disability and digital government*, in *Technology and regulation*, 2024; C. DEL BUCCHIA, C. LANCELOT MILTGEN, C.A. RUSSELL, C. BURLAT, *Empowerment as latent vulnerability in techno-mediated consumption journeys*, in *Journal of business research*, 2021.
[57] Cfr. M. TOMASI, L. BUSATTA, M. FASAN, C. NARDOCCI, S. PENASA, S. SULMICELLI, *Vulnerabilità e intelligenza artificiale – Editoriale,* in *Rivista di biodiritto,* 1S, 2024; S. CORRADI*, Comprendere la vulnerabilità. Pluralismo ontologico e sistemi di intelligenza artificiale nel diritto*, in *Rivista di biodiritto*, 1S, 2024.

dall'altra, stiamo assistendo a una tendenza emergente nel settore che considera l'impatto specifico sulle vulnerabilità come uno dei fattori determinanti al fine di valutare l'utilità delle tecnologie e monitorarne il funzionamento[58].

In prima analisi, le nuove tecnologie possono aggravare vulnerabilità già esistenti o crearne di nuove, oppure ridurre i margini di vulnerabilità proteggendo la persona sulla scia dei valori costituzionali menzionati finalizzati a incrementare accessibilità ai servizi, inclusione e partecipazione della persona.

A fianco, quindi, delle opportunità che insistono sul rapporto fra vulnerabilità e capacitazione mediante il ricorso appropriato alle nuove tecnologie occorre evidenziare l'esistenza di una serie di criticità che vanno, anch'esse, adeguatamente considerate.

Occorre annoverare criticità di ordine trasversale e criticità più specifiche e caratterizzanti questo settore di intervento.

Fra le criticità di ordine trasversale occorre menzionare un possibile disallineamento tra le scelte tecnologiche da opzionare e le priorità costituzionali di spesa e intervento.

Senza una chiara qualificazione delle tecnologie come infrastrutture costituzionalmente necessarie gli interventi normativi che vanno nella direzione della promozione dei diritti delle persone vulnerabili rischiano di essere episodici, frammentati o subordinati a logiche di efficienza economica.

Fra le criticità più specifiche, occorre annoverare i rischi connessi alla sostituzione della relazione di cura e assistenza della persona vulnerabile e quindi un possibile rischio di impoverimento della dimensione relazionale, una possibile deresponsabilizzazione istituzionale e una riduzione della persona a "utente" o, peggio ancora, a fonte di "dati".

Un altro insieme di criticità concerne l'eventualità di una riduzione tecnicistica della vulnerabilità, trattata come variabile da gestire o da "compensare" tramite soluzioni standardizzate[59].

Questa impostazione evidenzia almeno due problematiche connesse e riguardanti la naturalizzazione della vulnerabilità come dato individuale, anziché riconoscerla come condizione relazionale, ecologica e sistemica, e il rischio di produrre nuove forme di esclusione quando le tecnologie sono progettate senza tener conto dei contesti di vita, delle capacità residue e delle reti sociali della persona[60].

Le vulnerabilità non possono più ormai essere intese, infatti, in senso statico o meramente individuale, ma come condizione relazionale e dinamica, che dipende dal grado di esposizione delle persone a fattori e interventi esterni, sociali, economici o tecnologici.

---

[58] Cfr. M. FASAN, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del Coronavirus*, in *Rivista di biodiritto*, 1S, 2020.

[59] Queste criticità riguardano la tensione tra standardizzazione dei sistemi tecnologici, necessaria per interoperabilità, sicurezza e sostenibilità, e personalizzazione delle prestazioni, richiesta dai principi costituzionali di dignità e autonomia. Quando le riforme privilegiano logiche uniformi, algoritmiche o procedurali, senza spazi di adattamento caso per caso, si corre il rischio di comprimere l'autodeterminazione e sostituire la valutazione umana con automatismi decisionali.

[60] Un nodo critico centrale è rappresentato dal *digital divide*, che non è solo infrastrutturale, ma anche cognitivo (competenze digitali), culturale, linguistico, e socio-economico. Gli interventi normativi, se non accompagnati da politiche strutturate di alfabetizzazione**,** mediazione e accompagnamento, possono determinare una selezione implicita dei beneficiari, favorendo chi è già in grado di utilizzare gli strumenti digitali e lasciando indietro le persone più fragili.

Alla luce dei documenti internazionali – in particolare, della Convenzione ONU sui diritti delle persone con disabilità (2006)[61], degli orientamenti del Consiglio d'Europa[62] e della Commissione UE[63] – la vulnerabilità può essere configurata come condizione che può attraversare diverse fasi della vita e molteplici e contesti di fragilità. In tale prospettiva, essa supera la tradizionale logica categoriale e si inserisce in una visione inclusiva fondata sulla promozione dell'eguaglianza sostanziale, della non discriminazione e del rispetto della dignità della persona.

La Corte costituzionale ha chiaramente riconosciuto la vulnerabilità come categoria di tutela costituzionale autonoma[64], progressivamente ampliando la portata di tale nozione, collegandola ai principi personalista e solidaristico[65]. Le recenti pronunce costituzionali e di legittimità menzionate in materia di disabilità e autonomia (Corte cost. n. 3/2025; Cass. civ. n. 6584/2025) mostrano come la tecnologia, se adeguatamente regolata, possa divenire strumento di emancipazione, abilitando la persona a esercitare diritti civili e politici e a vivere in autonomia.

Si potrebbe affermare che la "rimozione di ostacoli" nella prospettiva dell'uguaglianza in senso sostanziale, include, in senso proattivo, anche l'esito di un processo continuativo di creazione di capacità (*capacitazione*, abilitazione).

Questo "rinnovato" paradigma dell'eguaglianza in ambiente digitale si afferma anche in ragione del fatto che la vulnerabilità non può più essere intesa esclusivamente come dato biologico o condizione individuale, ma emerge sempre più chiaramente come condizione "ecologica", sistemica e relazionale, prodotta dall'interazione fra individui, istituzioni e tecnologie. In tale prospettiva, la governance dei diritti non può limitarsi alla protezione formale delle persone vulnerabili, ma deve farsi carico della configurazione degli ambienti, anche tecnologici, affinché essi siano realmente inclusivi e abilitanti.

Si tratta di declinare una forma di "eguaglianza ecologica", nel rapporto fra persone nell'ambito di sistemi sempre più complessi, che assicuri ad ogni individuo la possibilità di agire efficacemente nei contesti digitali e organizzativi in cui si esercitano diritti fondamentali. Solo collocando al centro dei sistemi complessi la promozione dello sviluppo della persona umana, è possibile evitare che le tecnologie riproducano o

[61] Il riferimento principale rimane la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, adottata a New York il 13 dicembre 2006 e ratificata in Italia con la legge 3 marzo 2009, n. 18. Tale Convenzione impegna gli Stati aderenti a promuovere, tutelare e garantire il pieno ed eguale godimento di tutti i diritti umani e delle libertà fondamentali da parte delle persone con disabilità (art. 1, co. 1), senza alcuna forma di discriminazione fondata sulla disabilità (art. 4). Essa richiama, inoltre, il rispetto della dignità, dell'autonomia individuale, dell'indipendenza della persona e dei principi di non discriminazione, partecipazione effettiva e inclusione sociale (art. 3).
Va altresì ricordato che la Convenzione richiede agli Stati firmatari di favorire la ricerca, lo sviluppo e la diffusione di beni, servizi e tecnologie, incluse quelle informatiche e comunicative, nonché di dispositivi di ausilio adeguati alle esigenze delle persone con disabilità.

[62] Il Consiglio d'Europa ha adottato, il 30 novembre 2016, la *Strategy on the rights of persons with disabilities* 2017-2023 che definisce le priorità per il periodo 2017-2023. È stata elaborata anche la *Recommendation No. R(92)6 on the standardization of rights of persons with disabilities* (9 aprile 1992) che stabilisce linee guida per gli Stati membri nei settori dell'istruzione, formazione professionale, occupazione, integrazione sociale.

[63] Strategia dell'UE per i diritti delle persone con disabilità 2021-2030.

[64] Sentenze della Corte costituzionale n. 89 del 2024, n. 242 del 2019, n. 66 del 2025, n. 132 del 2025, n. 111 del 2025.

[65] Cfr. sentenze della Corte costituzionale n. 275 del 2016, n. 141 del 2019, n. 158 del 2020, n. 62 del 2020, n. 83 del 2019, n. 232 del 2018, n. 19 del 2022.

amplifichino barriere preesistenti, e garantire invece un effettivo empowerment nelle dinamiche sociali e istituzionali contemporanee.

Come sopra considerato, a fronte dello standard unionale di tipo precauzionale, alcuni ordinamenti – per primo in ordine cronologico, occorre menzionare quello italiano[66] – sono in procinto di costruire una infrastruttura sistemica abilitante, dove la tecnologia viene considerata sempre più strumento abilitante e di capacitazione e non solo oggetto di attenzione precauzionale.

Questo porta a delineare un "paradigma della promozione dei diritti", che si affianca e integra quello della protezione dai rischi sviluppatosi a livello europeo.

Le recenti riforme, espressive di un emergente sistema abilitante, rappresentano l'attuazione concreta delle priorità costituzionali in materia di dignità, uguaglianza, solidarietà, autonomia e diritto alla partecipazione da parte di tutte le persone, riformulando la relazione tra welfare, tecnologia e diritti.

Un primo riferimento è rappresentato dall'Ecosistema nazionale di welfare digitale, che include investimenti e riforme attuate nell'ambito del PNRR[67], e in particolare in relazione ai connessi processi di digitalizzazione attivati trasversalmente nell'ambito delle singole missioni, nonché nell'ambito dei settori considerati (si pensi ai servizi pubblici) dalle linee di indirizzo del Piano Triennale per l'Informatica nella pubblica amministrazione (2024–2026)[68]. Queste misure puntano a personalizzare le prestazioni e a promuovere una governance *evidence-based*, nella quale la digitalizzazione diventi infrastruttura di cittadinanza e strumento di uguaglianza sostanziale.

In secondo luogo, la legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale",[69] che, ponendosi in un rapporto di integrazione e complementarietà con il regolamento (UE) 2024/1689 (*AI Act*)[70], costituisce il primo quadro normativo nazionale sull'intelligenza

[66] Una ricerca comparativa sull'attuazione dell'AI Act segnala che la maggior parte degli Stati membri non avrà leggi nazionali organiche sull'IA prima del 2026, cfr. *Most EU countries won't have national AI laws ready before 2026, EU study shows*, disponibile al seguente link: https://www.mlex.com/mlex/articles/2404648/most-eu-countries-won-t-have-national-ai-laws-ready-before-2026 eu-study-shows?utm (ultima consultazione 12/03/2026). Cfr. anche *Riunione interparlamentare su Democrazia, innovazione e legge sull'intelligenza artificiale: uno scambio interparlamentare*, Bruxelles, 8 dicembre 2025.

[67] Presidenza del Consiglio dei Ministri, *Piano Nazionale di Ripresa e Resilienza* (PNRR), approvato con Decisione di esecuzione del Consiglio dell'Unione europea del 13 luglio 2021.

[68] Il Piano triennale è stato aggiornato nel 2025. Cfr. anche Agenzia per l'Italia Digitale, AGID (2024), *Strategia italiana per l'intelligenza artificiale 2024-2026*.

[69] La legge italiana sull'intelligenza artificiale, legge 23 settembre 2025, n. 132, intitolata *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, è stata approvata il 17 settembre ed è entrata in vigore il 10 ottobre 2025. La legge si compone di sei capi, per un totale di 28 articoli e fornisce previsioni complementari rispetto al regolamento europeo sull'intelligenza artificiale in modo da valorizzare la specificità e l'identità costituzionale. È una legge di principio e di delega, che inquadra l'impianto etico, istituzionale e di governance per l'attuazione nel nostro ordinamento del Regolamento (UE) 2024/1689 sull'AI. I principi fondamentali della legge sono quelli di centralità della persona, trasparenza, sicurezza, innovazione e tutela dei diritti. Occorre evidenziare che il comma 1 dell'art. 1 afferma che la legge n. 132 promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. A fianco di questa dimensione promozionale persiste la preoccupazione, al 2 periodo del 1 comma, rispetto a «la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale».

Il comma 2 chiarisce che le disposizioni della legge n. 132 si interpretano e si applicano conformemente al diritto dell'Unione europea.

[70] Sull'*enforcement* dell'*AI act*, cfr. K. SÖDERLUND, S. LARSSON, *Enforcement design patterns in EU law: an analysis of the AI Act*, in *Digital society*, 2024; C. NOVELLI, P. HACKER, J. MORLEY, J. TRONDAL, L. FLORIDI, *A Robust governance for the*

artificiale in un Paese membro dell'Unione europea, e «Promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità»[71].

L'approccio si sposta così da una logica difensiva a una visione proattiva e promozionale: l'intelligenza artificiale non è più soltanto oggetto di controllo, ma può divenire un potenziale mezzo di emancipazione individuale e collettiva[72].

Nell'ambito dell'uso dell'intelligenza artificiale nel settore sanitario e della disabilità (art. 7), la legge mira a migliorare l'autonomia e la qualità della vita, garantendo accessibilità, sicurezza, trasparenza e interoperabilità dei sistemi di intelligenza artificiale.

In questa prospettiva, la tecnologia diventa una leva di empowerment che consente alla persona di essere parte attiva del proprio progetto di vita, in linea con quanto stabilito dal d.lgs. 3 maggio 2024, n. 62 (di cui nel prosieguo della trattazione), in modo da promuovere l'uso dell'IA per migliorare accessibilità, autonomia e inclusione delle persone con disabilità.

L'art. 10 della legge n. 132, inoltre, incide direttamente sulla sanità digitale, introducendo l'art. 12-bis nel decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e istituendo una piattaforma nazionale di intelligenza artificiale affidata ad AGENAS, con funzioni di supporto alla cura e implementazione dell'assistenza territoriale.

Un secondo pilastro da segnalare è rappresentato, appunto, dal decreto legislativo 3 maggio 2024, n. 62, recante "Definizione della condizione di disabilità, della valutazione di base, di accomodamento ragionevole, della valutazione multidimensionale per l'elaborazione e attuazione del progetto di vita individuale personalizzato e partecipato".

Nel d.lgs. n. 62 del 2024 le tecnologie svolgono un ruolo fortemente abilitante rispetto alla disabilità. Non sono trattate come semplice supporto accessorio, ma come fattore strutturale delle nuove nozioni di disabilità e di progetto di vita. È possibile sintetizzare il posizionamento del decreto legislativo rispetto a questo tema seguendo alcuni passaggi fondamentali. Le tecnologie vengono identificate come "risorse" del budget di progetto là dove il decreto colloca espressamente le tecnologie dentro la struttura dei sostegni attivabili per l'inclusione (art. 2, comma 1, lett. p)[73]. Le tecnologie sono, quindi, riconosciute come risorse attivabili al pari di competenze professionali o sostegni economici, e come elementi essenziali per rendere esigibili i diritti e per attuare il progetto di vita.

AI Act: AI Office, AI Board, Scientific Panel, and National Authorities, in *European journal of risk regulation*, 2024; D. LEWIS, M. LASEK-MARKEY, D. GOLPAYEGANI, H.J. PANDIT, *Mapping the regulatory learning space for the EU AI Act*, in *ArXiv*, 2025.

[71] Cfr. art. 1, comma 1, della legge n. 132 del 2025.

[72] Occorre ricordare che la legge n. 132 del 2025 presenta i caratteri di una legge quadro in materia di intelligenza artificiale: essa definisce principi e indirizzi generali per lo sviluppo e l'utilizzo dell'IA in una prospettiva antropocentrica e di tutela dei diritti fondamentali, rinviando tuttavia l'attuazione concreta a successivi decreti legislativi e atti regolatori.

[73] L'art. 2 del d.lgs. n. 62 stabilisce che «1. Ai fini del presente decreto, si applicano le seguenti definizioni: a) condizione di disabilità: una duratura compromissione fisica, mentale, intellettiva, del neurosviluppo o sensoriale che, in interazione con barriere di diversa natura, può ostacolare la piena ed effettiva partecipazione nei diversi contesti di vita su base di uguaglianza con gli altri […]; p) budget di progetto: insieme delle risorse umane, professionali, tecnologiche, strumentali ed economiche, pubbliche e private, attivabili anche in seno alla comunità territoriale e al sistema dei supporti informali, da destinare al progetto di vita».

Le tecnologie, inoltre, possono essere inquadrate come "facilitatori" nella valutazione multidimensionale là dove il decreto con una clausola generale menziona i fattori ostacolanti e facilitatori che, all'interno del contesto di vita della persona con disabilità, possono determinare il profilo di funzionamento della persona (art. 2, comma 1, lett. m)[74].

Fra questi fattori facilitatori possono rientrare, a titolo di esempio, alcune fra le principali infrastrutture tecnologiche, quali i dispositivi digitali, la comunicazione aumentativa, gli strumenti informatici, e le tecnologie per l'accessibilità.

In aggiunta, le tecnologie possono rappresentare strumenti di supporto all'autodeterminazione e partecipazione dove il d.lgs. valorizza la capacità della persona con disabilità di adottare decisioni, «anche mediante l'utilizzo di strumenti, finalizzati a facilitare la comprensione delle fasi del procedimento e di quanto proposto per supportare l'adozione di decisioni e la manifestazione dei desideri, aspettative e scelte, anche attraverso la migliore interpretazione possibile degli stessi» (art. 21, comma 1).

Ciò significa che le nuove tecnologie nella forma delle tecnologie comunicative, delle interfacce semplificate, degli strumenti per la comunicazione aumentativa e alternativa, delle tecnologie vocali e visive, possono essere riconosciute come mezzi per comunicare la volontà, partecipare attivamente, sostenere l'autodeterminazione, superare barriere comunicative e/o cognitive.

Un ultimo passaggio è rintracciabile all'art. 28 del decreto legislativo in parola dove viene confermato che l'attuazione del progetto di vita è sostenuta da un budget di progetto configurato in maniera integrata, quale insieme coordinato di risorse umane, professionali, tecnologiche, strumentali ed economiche, di natura sia pubblica sia privata. Tale budget comprende anche le risorse attivabili all'interno della comunità territoriale e del sistema dei supporti informali, così da garantire un sostegno personalizzato e multidimensionale, capace di valorizzare le capacità della persona e di promuoverne la piena partecipazione alla vita sociale.

Un ultimo pilastro è costituito dal d.lgs. 15 marzo 2024, n. 29, ss.mm.ii., recante "Disposizioni in materia di politiche in favore delle persone anziane, in attuazione della delega di cui agli articoli 3, 4 e 5 della legge 23 marzo 2023, n. 33"[75], che prevede il recepimento del Piano nazionale di non autosufficienza e introduce il concetto di valutazione multidimensionale unificata che, in prospettiva potrebbe essere qualificata in maniera più appropriata come "digitale", ossia coordinata attraverso piattaforme interoperabili che integrino efficacemente i diversi settori di tutela della persona vulnerabile.

[74] L'art. 2 del d.lgs. n. 62 definisce al comma 1, lett. m), la valutazione multidimensionale come «procedimento volto a delineare con la persona con disabilità il suo profilo di funzionamento all'interno dei suoi contesti di vita, anche rispetto agli ostacoli e ai facilitatori in essi presenti, e a definire, anche in base ai suoi desideri e alle sue aspettative e preferenze, gli obiettivi a cui deve essere diretto il progetto di vita».

[75] Il d.lgs. 15 marzo 2024, n. 29, *Disposizioni in materia di politiche in favore delle persone anziane*, rappresenta un passo importante nel riconoscimento dei diritti, della dignità e dell'autonomia della popolazione anziana, in attuazione della legge delega del 23 marzo 2023, n. 33. Questo d.lgs., come specificato dall'art. 1, «reca disposizioni volte a promuovere la dignità e l'autonomia, l'inclusione sociale, l'invecchiamento attivo e la prevenzione della fragilità della popolazione anziana, anche attraverso l'accesso alla valutazione multidimensionale unificata, a strumenti di sanità preventiva e di telemedicina a domicilio, il contrasto all'isolamento e alla deprivazione relazionale e affettiva, la coabitazione solidale domiciliare per le persone anziane (senior cohousing) e la coabitazione intergenerazionale (cohousing intergenerazionale), lo sviluppo di forme di turismo del benessere e di turismo lento, nonché volte a riordinare, semplificare, coordinare e rendere più efficaci le attività di assistenza sociale, sanitaria e sociosanitaria per le persone anziane non autosufficienti».

Come evidenziato, l'approccio alla vulnerabilità, nell'ambito della valutazione multidimensionale unificata, prevista dal d.lgs. n. 29 del 2024 in materia di politiche per le persone anziane[76], è finalizzato a integrare dimensioni sanitarie, sociali, psicologiche e ambientali in un sistema che, *pro futuro*, si svilupperà sempre più come informatizzato e interoperabile[77].

Gli esiti della valutazione multidimensionale saranno finalizzati progressivamente a essere condivisi attraverso piattaforme digitali in modo da collegare il Fascicolo Sanitario Elettronico, le banche dati INPS e le cartelle sociali comunali, consentendo una presa in carico personalizzata e partecipata.

Al Capo V del Titolo I, il decreto legislativo n. 29 dedica ampio spazio alla facilitazione e all'alfabetizzazione digitale, istituendo una rete nazionale di servizi di supporto e formazione, con l'obiettivo di ridurre le disuguaglianze tecnologiche e territoriali[78].

In definitiva, le nuove tecnologie stanno diventando sempre più strumenti di cura personalizzata e partecipata, in cui il soggetto vulnerabile è parte attiva del proprio progetto di vita, istituzionalizzando un

[76] Il d.lgs. 29 del 2024 rappresenta un tentativo organico di ridefinire le politiche per l'invecchiamento in Italia, spostando il focus dalla mera assistenza alla partecipazione attiva e integrata della persona anziana nella società. Nell'ambito del d.lgs. n. 29 del 2024, l'art. 9 riguarda proprio la promozione di strumenti di sanità preventiva e di telemedicina presso il domicilio delle persone anziane, mentre l'art. 10 concerne la valutazione multidimensionale unificata per cui «Nell'ambito dei punti unici di accesso (PUA), di cui all'articolo 1, comma 163, della legge 30 dicembre 2021, n. 234, sono assicurati alle persone anziane, l'erogazione dell'orientamento e del sostegno informativo per favorire il pieno accesso agli interventi e ai servizi sociali e sociosanitari e la possibilità di ottenere, ove occorra, una valutazione multidimensionale unificata secondo i criteri e le modalità di cui all'articolo 27, in funzione della individuazione dei fabbisogni di assistenza».

[77] L'art. 28, rubricato "Attività dei punti unici di accesso e piattaforma digitale", al comma 4 prevede l'istituzione dello strumento della valutazione multidimensionale unificata di cui all'articolo 27, scientificamente validato, informatizzato e digitale, al fine di promuovere la semplificazione e l'integrazione delle procedure di accertamento e valutazione della condizione di persona anziana non autosufficiente, i cui risultati sono resi disponibili su piattaforme interoperabili secondo le indicazioni di cui all'articolo 2, comma 2, lettera l), e all'articolo 2, comma 3, lettera c), della legge n. 33 del 2023. Viene previsto che tale strumento deve essere in linea con gli standard tecnologici definiti dalla vigente disciplina in materia di telemedicina e fascicolo sanitario elettronico, attraverso la condivisione delle seguenti informazioni: a) relative alla documentazione sanitaria per l'accesso del PUA; b) contenute nel fascicolo sanitario elettronico (FSE); c) relative alla posizione del cittadino nella piattaforma INPS; d) relative alle eventuali cartelle sociali presso gli enti locali secondo quanto previsto dall'articolo 23, comma 3. Invero, gli strumenti digitali vengono menzionati più volte nel decreto come strumenti di semplificazione e facilitazione dell'accesso ai servizi. Oltre al comma 4 dell'art. 28 si può fare riferimento al comma 3 e 4 dell'art. 29. Al comma 3 dell'art. 29 del d.lgs. n. 29 viene stabilito che «Con il decreto del Ministro della salute, di concerto con i Ministri del lavoro e delle politiche sociali e per le disabilità, su proposta congiunta dell'Agenzia nazionale per i servizi sanitari regionali (Agenas) e della componente tecnica della Rete della protezione e dell'inclusione sociale, sono, altresì, definite le linee di indirizzo nazionali per l'integrazione operativa degli interventi sociali e sanitari previsti nei servizi di cura e assistenza domiciliari e per l'adozione di un approccio continuativo e multidimensionale della presa in carico della persona anziana non autosufficiente e della sua famiglia, anche attraverso strumenti digitali, di telemedicina e di supporto tecnologico alla cura, in coerenza con la normativa vigente e con la "Proposta di requisiti strutturali, tecnologici e organizzativi minimi per l'autorizzazione all'esercizio e requisiti ulteriori per l'accreditamento delle cure domiciliari di base e integrate, in attuazione dell'articolo 1, comma 406, della legge 30 dicembre 2020, n. 178", approvata con l'intesa sancita in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nella seduta del 4 agosto 2021, nei limiti delle risorse disponibili a legislazione vigente».

[78] Il Capo V del Titolo I del decreto legislativo n. 29 prevede una serie di misure in materia di alfabetizzazione informatica e di facilitazione digitale, fra cui la rete dei servizi di facilitazione digitale, il percorso per le competenze trasversali e per l'orientamento per ridurre il divario digitale.

"*welfare* abilitante", dove la tecnologia non sostituisce la relazione ma la amplifica, costruendo ponti di prossimità tra pubblico, Terzo Settore e comunità locali.
Affinché il paradigma del "*welfare* abilitante" non rimanga confinato a una dimensione programmatica o meramente normativa, occorre individuare alcuni strumenti concreti di attuazione capaci di rendere effettivo il ruolo delle tecnologie nella promozione dell'autonomia delle persone con disabilità.
In primo luogo, assume rilievo la costruzione di infrastrutture digitali interoperabili, capaci di integrare le diverse banche dati sanitarie, sociali e previdenziali (Fascicolo sanitario elettronico, banche dati INPS, cartelle sociali comunali), così da consentire, nel rispetto della normativa vigente in materia di protezione dei dati personali, una presa in carico realmente personalizzata e multidimensionale della persona. In assenza di tale integrazione informativa, infatti, il progetto di vita personalizzato rischia di rimanere frammentato tra diversi livelli amministrativi e settoriali.
In secondo luogo, appare necessario promuovere tecnologie assistive e strumenti di comunicazione aumentativa e alternativa, nonché piattaforme digitali di supporto all'autodeterminazione, che permettano alla persona con disabilità di partecipare attivamente ai processi decisionali che riguardano il proprio progetto di vita. In questa prospettiva, la tecnologia non rappresenta soltanto un ausilio tecnico, ma un vero e proprio supporto fondamentale all'esercizio dei diritti fondamentali. Si pensi, ad esempio, ai sistemi di comunicazione aumentativa e alternativa basati su tablet e software dedicati che consentono alle persone con disabilità comunicative di esprimere preferenze e bisogni; ai dispositivi domotici e agli assistenti vocali che permettono la gestione autonoma dell'ambiente domestico; alle piattaforme digitali di teleassistenza e monitoraggio remoto, che favoriscono la permanenza al domicilio in condizioni di sicurezza; nonché alle applicazioni digitali per la pianificazione personalizzata delle attività quotidiane e per la gestione condivisa del progetto di vita tra persona, famiglia e servizi.
Un ulteriore profilo riguarda la dimensione organizzativa e territoriale della governance del welfare digitale. L'effettività delle misure previste dalla normativa richiede, infatti, modelli di cooperazione stabile e strutturata tra pubbliche amministrazioni, servizi sanitari territoriali, enti del Terzo settore e comunità locali, in modo da costruire ecosistemi di cura e assistenza nei quali le tecnologie fungano da fattore di connessione e coordinamento tra i diversi attori coinvolti.
Infine, la realizzazione di un *welfare* realmente abilitante presuppone politiche di alfabetizzazione digitale e accompagnamento all'uso delle tecnologie, rivolte non solo alle persone vulnerabili ma anche alle famiglie e agli operatori dei servizi sociali e sanitari. Senza adeguate competenze digitali diffuse, infatti, il rischio è che le tecnologie destinate a promuovere l'inclusione finiscano per generare nuove forme di esclusione.

4. Considerazioni conclusive

Il contributo ha analizzato il rapporto tra tecnologie e vulnerabilità muovendo dalla distinzione tra lo standard europeo della protezione dai rischi e l'emergente paradigma nazionale della promozione dei diritti. L'analisi del quadro eurounitario ha messo in luce come la regolazione digitale dell'Unione europea – dall'AI Act, sino al *Digital Services Act*, al *Digital Markets Act*, al *Data Governance Act*, *all'European Health Data Space* – sia prevalentemente orientata alla prevenzione e alla gestione dei rischi idiosincratici e sistemici derivanti dall'uso delle tecnologie, attraverso strumenti di classificazione del rischio,

accountability, vigilanza e standardizzazione tecnica. Si tratta di un modello coerente e funzionale alla tutela minima dei diritti fondamentali e alla garanzia di funzionamento del mercato interno, ma che, per sua natura, tende a privilegiare una logica precauzionale più che una prospettiva attivamente promozionale.

A partire da tale quadro, la trattazione ha evidenziato come, nello spazio lasciato alla discrezionalità degli Stati membri, l'ordinamento italiano stia progressivamente sviluppando una propria declinazione dell'identità costituzionale digitale, fondata sui principi personalista, solidaristico, egualitario e partecipativo previsti in Costituzione. In questa prospettiva, la digitalizzazione dei servizi pubblici e dei sistemi di tutela delle persone vulnerabili non viene letta come un mero processo tecnico-amministrativo, ma come fenomeno costituzionalmente rilevante, idoneo a incidere sull'effettività dei diritti fondamentali e sulle modalità di inclusione delle stesse.

Un passaggio centrale dell'analisi è stato dedicato al tema delle priorità costituzionali e delle infrastrutture abilitanti, mettendo in evidenza come la giurisprudenza costituzionale e di legittimità stiano progressivamente riconoscendo il valore della tecnologia quale strumento di promozione dei diritti. Le pronunce in materia di spesa costituzionalmente necessaria, di disabilità, di partecipazione democratica e di autonomia personale mostrano come la tecnologia possa essere qualificata, caso per caso, non solo come costo o fattore di rischio, ma come investimento funzionale alla realizzazione dei principi di eguaglianza sostanziale, solidarietà e alla tutela della dignità umana. In tale contesto, emerge una nozione di dignità tecnologicamente mediata, nella quale l'autonomia e la capacità di autodeterminazione della persona dipendono anche dall'accesso a strumenti tecnologici adeguati e dall'assenza di ostacoli giuridici alla attuazione dei diritti.

La riflessione si è poi concentrata sul concetto complesso e plurale di vulnerabilità, inteso non come dato statico o deficit individuale, ma come condizione relazionale, dinamica ed "ecologica", prodotta dall'interazione tra individui, istituzioni e tecnologie. In questa prospettiva, le nuove tecnologie possono tanto aggravare preesistenti situazioni di vulnerabilità quanto costituire potenti strumenti di capacitazione, a seconda delle scelte normative, organizzative e progettuali che ne orientano l'uso. Le riforme nazionali più recenti – in particolare, in materia di disabilità, politiche per la non autosufficienza e intelligenza artificiale – delineano un modello di tutela abilitante, nel quale le tecnologie sono integrate nei progetti di vita individuale come risorse strutturali per l'inclusione, la partecipazione e l'autonomia.

Nel complesso, la trattazione consente di individuare un possibile paradigma nazionale della promozione dei diritti, destinato ad affiancare e integrare lo standard europeo della protezione dai rischi. Tale paradigma non si esaurisce nella neutralità delle regole o nella mera sicurezza dei sistemi, ma richiede una governance dei diritti orientata alla progettazione inclusiva degli ambienti tecnologici unitamente alla valorizzazione delle capacità residue e potenziabili delle persone.

Nel quadro considerato, il rapporto tra regolazione europea delle tecnologie e ordinamenti nazionali non può essere interpretato esclusivamente in termini di attuazione o recepimento delle discipline eurounitarie. Piuttosto, esso sembra configurarsi come una relazione di complementarietà funzionale tra un modello europeo prevalentemente orientato alla gestione dei rischi tecnologici e un livello nazionale chiamato a sviluppare strumenti istituzionali e organizzativi capaci di tradurre l'innovazione digitale in effettive opportunità di inclusione e promozione dei diritti fondamentali, in particolare nei confronti delle persone vulnerabili.

La vulnerabilità non è più concepita come eccezione alla normalità o come deficit individuale, ma come dimensione costitutiva della condizione umana all'interno di sistemi complessi e tecnologicamente mediati. Essa può diventare, quindi, un indice di qualità costituzionale nella sua declinazione di misura della capacità dell'ordinamento di includere, accogliere e abilitare tutte le persone, indipendentemente dalle loro condizioni fisiche, cognitive, e socio-economiche.

In tale prospettiva, la tecnologia non rappresenta soltanto una sfida etica o un rischio da contenere, ma si configura come una componente essenziale di un ambiente di giustizia da progettare secondo criteri di accessibilità, trasparenza e responsabilità pubblica. Lo Stato costituzionale non può limitarsi, nell'era digitale, al ruolo di garante della sicurezza dei sistemi: dovrebbe, infatti, assumere la funzione di governatore di ecosistemi tecnologici inclusivi, orientando lo sviluppo e l'uso delle innovazioni verso la promozione dei diritti fondamentali di tutti e la realizzazione della dignità umana.

In questo senso, la Costituzione italiana, attraverso i principi personalista, egualitario e solidaristico, può trovare nell'innovazione tecnologica non solo un eventuale limite da gestire e un rischio da contenere, ma una inedita (e potenziale) frontiera della sua attuazione.