«Il diritto dell'economia» issn 1123-3036, anno 71, n. 117 (2-3 2025) pp. 417-457

Articoli e saggi

L'intelligenza artificiale nell'amministrazione sanitaria. Riflessioni a margine della recentissima Legge n. 132/2025

Silia Gardini

1. *L'intelligenza artificiale come nuova frontiera del diritto amministrativo sanitario*

Ogni epoca storica delinea le sue soglie giuridiche[1]: varchi oltre i quali il diritto è chiamato a interrogare sé stesso, alla luce di nuove forze che irrompono nel tessuto ordinamentale e ne mettono alla prova le categorie fondamentali.

[1] Nel XIX secolo la nascita della burocrazia moderna offrì alla giovane statualità europea una nuova architettura e impose al diritto di interrogarsi sul rapporto tra poteri e regole, tra discrezionalità e controllo, inaugurando il primo capitolo della legalità amministrativa. Il Novecento aprì un'altra stagione: lo Stato sociale non si accontentava più di governare e mantenere l'ordine, ma puntava a garantire istruzione, salute, previdenza. L'amministrazione diventò progressivamente veicolo di inclusione e motore di politiche sociali, assumendo una "responsabilità" verso la collettività. L'ultimo scorcio di secolo e l'inizio del nuovo millennio hanno consegnato all'amministrazione altre prove. La globalizzazione e l'integrazione europea hanno imposto coordinamento e apertura verso ordinamenti sovranazionali, mentre la digitalizzazione ha cominciato a ridefinire intrinsecamente il linguaggio degli apparati pubblici.

L'avvento dell'intelligenza artificiale (di seguito anche IA) rappresenta, senza ombra di dubbio, il nuovo grande "salto di fase" nell'evoluzione dell'amministrazione contemporanea[2].

Non siamo dinnanzi ad ausili informatici che velocizzano le procedure: l'intelligenza artificiale[3] è destinata a operare come una vera e propria infrastruttura cognitiva del potere pubblico[4], capace di apprendere, selezionare, classificare e soprattutto di orientare – fino a co-determinare – le decisioni amministrative.

[2] In dottrina si discute di nuova «società algoritmica». Cfr. M. Bassini, L. Liguori, O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Torino, 2018, 333 ss. Sul tema, si vedano anche L. Casini, *Il futuro dello stato (digitale)*, in *Riv. trim. dir. pub*., 2024, 2; A. Pajno, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2019, 206-207; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, a cura di A. D'Aloia, Milano, 2020, 170 ss.; L. Torchia, *Lo Stato digitale. Una introduzione*, Bologna, 2023.

[3] Non è agevole fornire una definizione univoca di "intelligenza artificiale", che richiama e ricomprende meccanismi anche molto diversi tra loro (cfr. G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Diritto dell'informazione e dell'informatica*, 2021, 2, 431 ss.). La versione in lingua italiana dell'art. 3 dell'AI Act definisce un sistema di IA come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Alla base del suo funzionamento potrebbe esserci, dunque, sia un approccio di tipo logico-deduttivo, sia un approccio di tipo induttivo, quale è il *machine learning*. In questa sede, non si può ricostruire il ricco dibattito letterario e scientifico sull'inquadramento generale del fenomeno. Ai nostri fini – in ragione dell'avanzamento del processo di digitalizzazione della p.a. – si può dare per acquisito il fatto che oggi le pubbliche amministrazioni utilizzano strumenti digitali dotati di intelligenza artificiale, più o meno complessa. Si può, dunque, legittimamente parlare di "amministrazione algoritmica" e di "atto amministrativo algoritmico" ogni qual volta la volontà procedimentale si formi (anche) attraverso connettori automatici e "i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione", richiamati dall'art. 3 della l. n. 241/1990 vengano (anche in parte) acquisiti, valutati e riversati nella decisione dalla macchina. Cfr. P. Forte, *Diritto amministrativo e data science. Appunti di intelligenza amministrativa Artificiale (AAI)*, in *P.A. Persona e Amministrazione*, 2020, 1, 265.

[4] Non è possibile approfondire in maniera adeguata il tema dei rapporti tra esercizio del pubblico potere e intelligenza artificiale, rispetto al quale la dottrina ha ampiamente discusso. Per un inquadramento del tema, si vedano, *ex multis*, il volume di M. Protto (a cura di), *Pubblica amministrazione e tecnologie emergenti*, in *Giurisprudenza Italiana*, 2022, 6; G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019; M. Macchia, A. Mascolo, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, 2022, 4, 556 ss.; V. Neri, *Diritto amministrativo e intelligenza artificiale: un amore possibile,* in *Urbanistica e Appalti,* 2021, 5; F. Laviola, *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *Biodiritto*, 2020, 3; L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Federalismi*, 2018, 21; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl*., 2019; M. Timo, *Algoritmo e potere amministrativo*, in *Il diritto dell'economia*, 2020, 1, 753 ss.; D.U. Galetta, J. Ziller (a cura di) *Information and Communication Technologies Challenging Public Law, beyond Data Protection*, Nomos Verlagsgesellschaft, 2018; J. Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, Cambridge, 2019; E. Picozza, *Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence*, in *Giur. it.,* 2019, 7, 1657 ss.; B. Raganelli, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenza diverse nell'assunzione di decisioni amministrative*, in *Federalismi*, 2020, 22; M. Corradino, *Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*, in *www.giustizia-amministrativa.it*, settembre 2021; P. Otranto, *Riflessioni in tema*

Le questioni che discendono da tale innovazione abbracciano inevitabilmente profili generali di governo e di legittimazione del sistema. Quando la logica del potere si intreccia con quella dell'algoritmo, occorre, dunque, individuare un punto di equilibrio che scongiuri distorsioni patologiche nelle decisioni pubbliche e chiarire quali siano gli elementi essenziali per garantire legalità e buon andamento dell'agire amministrativo. In questa prospettiva, l'amministrazione è chiamata ad assicurare la resilienza dei propri processi organizzativi e decisionali: la capacità di adattarsi, correggersi e mantenere continuità di tutela di fronte ai rapidi mutamenti tecnologici. Come ha osservato il Consiglio di Stato, i rischi connessi all'uso sempre più diffuso di strumenti algoritmici non possono essere neutralizzati mediante la rigida applicazione delle regole procedimentali della legge n. 241 del 1990, ma richiedono un impegno ulteriore, in primo luogo sul versante della trasparenza[5].

È in questa traiettoria di analisi che, con il presente lavoro, si intende circoscrivere l'attenzione sull'amministrazione sanitaria[6], laddove l'innovazione algo-

di decisione amministrativa, intelligenza artificiale e legalità, in *Federalismi*, 2021, 7; R. Giordano, A. Panzarola, A. Police, S. Preziosi e M. Protto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022; E. Chiti, B. Marchetti, N. Rangone, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in *BioLaw Journal*, 2022, 2; G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; G. Sgueo, *L'uso dell'IA nelle pubbliche amministrazioni: mitologia informatica?*, in *Irpa.eu*, 2024; G. Gardini, *Dall'amministrazione analogica all'amministrazione per algoritmi. varianti e invarianti di un processo evolutivo*, in *Dir. amm.*, 2025, 3.

[5] Cfr. Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472. Il Consiglio di Stato ha costruito negli ultimi anni un nucleo solido di principi a presidio dell'uso degli algoritmi nella pubblica amministrazione, incentrato su legalità, trasparenza e non discriminazione. In primo luogo, l'algoritmo è considerato una regola tecnica amministrativa soggetta al principio di legalità e ai principi generali dell'azione amministrativa, tra cui imparzialità e trasparenza (Cons. Stato, sez. VI, 8 aprile 2019, n. 2270, in *www.giustizia-amministrativa.it*). Ne discende il dovere per l'amministrazione di rendere conoscibili i criteri decisionali incorporati nel software, pena l'illegittimità del provvedimento per opacità (Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, in *www.giustizia-amministrativa.it*). La giurisprudenza distingue tra algoritmi decisionali – che richiedono piena trasparenza e supervisione – e strumenti informatici di supporto, per i quali si ammette un margine maggiore di riservatezza tecnica (Cons. Stato, sez. IV, 4 giugno 2025, n. 4857, in *www.giustizia-amministrativa.it*). A ciò si affianca il principio di non discriminazione algoritmica, ispirato al GDPR, secondo cui la PA deve prevenire effetti iniqui o distorsivi, adottando misure idonee a neutralizzare *biases* nei dati o nei criteri di calcolo (Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, in *www.giustizia-amministrativa.it*). Infine, anche nei sistemi completamente automatizzati, l'amministrazione resta tenuta a garantire l'accessibilità, la comprensibilità e la tracciabilità delle decisioni: non è ammessa alcuna deresponsabilizzazione per ragioni tecniche o delegate a terzi (Cons. Stato, sez. VI, 6 giugno 2025, n. 4929, in *www.giustizia-amministrativa.it*). Si tratta di profili che saranno approfonditi e contestualizzati rispetto al settore sanitario nei paragrafi che seguono.

[6] Sul tema dell'applicazione dei sistemi di IA nel settore sanitario, si vedano: E.A. Ferioli, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, in *BioLaw Journal*, 2019, 163 ss.; C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, *ivi*, 711 ss.; A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, *ivi*, 3 ss.; M. Hansen, T. Miron-Shatz, A.Y. Lau, C. Paton, Big *Data in Science and Healthcare: A Review of Recent Literature and Perspectives. Contribution of the IMIA Social Media Working Group*, 2014; A. Biancardo, *Problematiche etico-giuridiche relative all'utilizzo dell'intelligenza artificiale in ambito sanitario*, in *JusOnline*, 3-2021, 102 ss.; V. Zagrebelsky, *Un progetto di ricerca su medici e pazienti nel rapporto con l'intelligenza artificiale*, in *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, III, *Pandemia e tecnologie. L'impatto su processi, scu-*

ritmica assume contorni di particolare complessità e interesse, per almeno due ragioni fondamentali[7].

La prima ragione è di ordine tecnico. La medicina è, per sua natura, terreno privilegiato per lo sviluppo dell'intelligenza artificiale (dispone di grandi quantità di dati, opera attraverso processi in larga parte formalizzabili e richiede un costante aggiornamento scientifico[8]) e la macchina amministrativa che la circonda riflette questa caratteristica.

Sul versante più strettamente amministrativo, gli algoritmi sono utilizzati per programmare e allocare risorse, per gestire i flussi di pazienti, definire priorità di accesso, per monitorare la qualità dei servizi, per rilevare inefficienze ed elaborare modelli epidemiologici utili alla pianificazione sanitaria[9]. Sul versante clinico, invece, i sistemi automatizzati supportano la diagnostica, la valutazione prognostica e i percorsi terapeutici, interagendo con le competenze professionali del personale sanitario e influenzando inevitabilmente l'esercizio dei diritti dei pazienti. La coesistenza di questi due livelli – amministrativo e clinico – conferisce senza dubbio al settore sanitario un ruolo strategico nella definizione di un modello di legalità algoritmica coerente con i principi costituzionali.

La seconda ragione è di carattere giuridico-istituzionale e riguarda la peculiarità della sanità come apparato amministrativo. Nel settore sanitario il potere pubblico si interseca in maniera molto incisiva con la vulnerabilità umana, nella sua forma più radicale: nella malattia, nella cura, nella tutela della salute fisica e psichica. Di conseguenza, un algoritmo che ordina le liste d'attesa, che segnala un'a-

---

ola e medicina, a cura di A. Pajno e L. Violante, Bologna, 2021, 54 ss.; G. Fares, A*rtificial intelligence in social and health services: A new challenge for public authorities in ensuring constitutional rights*, in *The IT revolution and its impact on State, constitutionalism and public law*, a cura di M. Belov, Oxford, 2021, 269 ss.; A. Aliper, R. Kudrin, D. Polykovskiy, P. Kamya, E. Tutubalina, S. Chen, F. Ren, A. Zhavoronkov, *Prediction of Clinical Trials Outcomes Based on Target Choice and Clinical Trial Design with Multi-Modal Artificial Intelligence,* in *Clinical Pharmacology & Therapeutics*, 2023, 972 ss.; P. Phan, S. Mitragotri, Z. Zhao, *Digital therapeutics in the clinic*, in *Bioengineering and translational Medicine*, vol. 8(4), e10536, 2023.

[7] Anche l'Agenzia per l'Italia Digitale (AgID) – nelle *Linee guida per l'adozione, l'acquisto e lo sviluppo di sistemi di intelligenza artificiale nella pubblica amministrazione,* previste dal *Piano Triennale per l'Informatica nella PA 2024-2026* e in corso di pubblicazione (cfr. *infra*) – ha riconosciuto la sanità come uno dei fondamentali settori di applicazione dell'AI, sia in ambito clinico che in tutto il resto della sfera sanitaria, ponendo particolare interesse nello sviluppo di modelli affidabili, responsabili (*Trustworthy AI*) e antropocentrici.

[8] Cfr. A. Petersen, D. Rotolo, L. Leydesdorff, *A Triple Helix Model of Medical Innovation: Supply, Demand, and Technological Capabilities in terms of Medical Subject Headings*, arXiv, 2015; A. Kerr, *Embodied Innovation and Regulation of Medical Technologies*, in *BioSocieties*, 2015; O. Zecchino, *The Medical Art Towards New Paradigms*, in *Springer Nature*, 2024; D.A. Petrie, *Integration as Innovation in Healthcare Systems*, in *Journal of Health Services Research & Policy*, 2024.

[9] In Italia la trasformazione algoritmica dell'amministrazione sanitaria sconta una base digitale ancora incompleta: nel 2024 il nostro paese ha registrato 62 punti nell'*eGovernment Benchmark*, contro una media UE di 76, con ritardi rispetto a Francia, Germania e Spagna. La digitalizzazione, senza una strategia di implementazione e di competenze, non produce di per sé semplificazione; al contrario, nel tempo di transizione può accentuare complessità e diseguaglianze di accesso ai servizi. Cfr. *Digital Decade 2024: eGovernment Benchmark* consultabile alla pagina internet: digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark.

nomalia clinica o che orienta un ente pubblico nella programmazione delle risorse economiche non svolge mai un compito asettico e poco rilevante. Ogni operazione riverbera inevitabilmente su diritti fondamentali della persona, costituzionalmente protetti. A ciò si aggiunga che la sanità è il settore a più alta densità di dati sensibili, il cui trattamento richiede un presidio giuridico e tecnico particolarmente rigoroso. L'intenso valore predittivo di questi dati li rende al tempo stesso risorsa e rischio: risorsa per la medicina personalizzata, la ricerca e la prevenzione; rischio per la *privacy*, la discriminazione algoritmica e la sorveglianza sanitaria.

In definitiva, pare corretto ritenere che in nessun altro settore, come in quello sanitario, la promessa di efficienza tecnologica si intrecci in modo tanto stretto con l'esigenza di preservare la pienezza delle garanzie amministrative e costituzionali. Da ciò discende la necessità di riflettere su almeno tre profili essenziali: 1) la ridefinizione dei procedimenti e le responsabilità pubbliche nell'impiego dell'intelligenza artificiale, chiarendo chi decide, chi controlla e chi risponde; 2) l'introduzione di una disciplina specifica sull'uso degli algoritmi in sanità, capace di assicurare trasparenza, tracciabilità e verificabilità delle decisioni automatizzate; 3) la promozione di una cultura amministrativa digitale in ambito sanitario, fondata sull'integrazione di competenze giuridiche, etiche, mediche e tecnologiche, tale da garantire che l'innovazione rimanga al servizio della tutela della salute e dell'uguaglianza nell'accesso alle cure.

In questa direzione, non stupisce che proprio la sanità occupi una posizione centrale nel recente intervento legislativo in materia di intelligenza artificiale, la legge 23 settembre 2025, n. 132, entrata in vigore il 10 ottobre 2025, di cui meglio si dirà nel prosieguo della trattazione.

2. *Come cambia il diritto alla salute nell'era degli algoritmi*

L'intelligenza artificiale è, a tutti gli effetti, una nuova dimensione del potere amministrativo che incide sui criteri di legittimazione dell'azione pubblica e sulla stessa definizione dell'interesse generale. In sanità, più che altrove, la "macchina" incontra la Costituzione ed è a partire da questo incontro che il diritto amministrativo è chiamato a ridefinire la propria misura.

La Costituzione italiana colloca la salute in un punto nevralgico dell'ordinamento, al crocevia tra l'interesse individuale (come diritto fondamentale della persona) e l'interesse generale (come garanzia di tutela collettiva). Da questa duplice dimensione emerge una tensione giuridica delicata, nella quale il diritto inviolabile del singolo ad accedere a cure efficaci e tempestive si intreccia con la responsabilità pubblica di preservare il bene comune, secondo criteri di universa-

lità, equità e solidarietà[10]. La dimensione pubblicistica della salute, in questa prospettiva, non si esaurisce nella prestazione sanitaria in senso stretto, ma si estende all'organizzazione, alla programmazione e alla regolazione dei processi decisionali, attraverso i quali la tutela viene concretamente realizzata.

L'intelligenza artificiale influenza questo equilibrio, poiché trasforma lo "spazio" nell'ambito del quale il diritto alla salute si esercita e viene garantito. La decisione amministrativa clinico-sanitaria in forma algoritmica si fonda su una valutazione che non è più esclusivamente espressione del discernimento umano, ma è il prodotto di correlazioni e inferenze, spesso non comprensibili né verificabili dal cittadino e, potenzialmente, dello stesso operatore sanitario. La capacità dei sistemi di IA di processare in tempi rapidissimi enormi volumi di dati sanitari consente, in astratto, di accrescere la qualità e l'efficienza delle prestazioni: si pensi alla possibilità di ottenere diagnosi più precoci, di ridurre i tempi di attesa o di ottimizzare l'allocazione delle risorse. Tuttavia, la medesima logica algoritmica può generare effetti distorsivi, amplificando disuguaglianze preesistenti (quando i dati di addestramento siano incompleti o non rappresentativi) e consolidando discriminazioni strutturali, sotto la parvenza di una neutralità tecnica[11].

In altre aree di azione amministrativa la correttezza dell'algoritmo può essere accertata *ex post*, con parametri di efficienza o legittimità formale. Nel campo della salute, invece, l'errore algoritmico incide immediatamente sulla vita e sull'integrità fisica della persona: il tempo del rimedio giuridico non coincide con il tempo del danno[12]. La tutela può, dunque, diventare fragile ogni qual volta il contenuto della decisione (diagnostica, organizzativa o allocativa) non sia immediatamente riconducibile a un procedimento controllato e guidato.

---

[10] Per una ricostruzione della dottrina sul tema, senza pretese di esaustività, cfr.: S. Lessona, *La tutela della salute pubblica*, in *Commentario sistematico della Costituzione italiana* diretto da P. Calamandrei e A. Levi, I, Firenze, 1950; C. Mortati, *La tutela della salute nella Costituzione italiana*, in *Rivista degli infortuni e delle malattie professionali*, 1961; A. Giannini, *La tutela della salute come principio costituzionale*, in *INADEL*, 1960; L. Carlassare, *L'art. 32 della Costituzione e il suo significato*, in *L'amministrazione sanitaria*, Atti del Congresso Celebrativo del Centenario delle Leggi amministrative di Unificazione, a cura di R. Alessi, Vicenza, 1967-1969; B. Caravita, *La disciplina costituzionale della salute*, in *Diritto e Società*, 1984, 1; D. Morana, *La salute nella Costituzione italiana: profili sistematici*, Milano, 2002; G. Cosmacini, *Storia della medicina e della sanità in Italia*, Roma-Bari, 2005; A. Simoncini, E. Longo, *Art. 32*, in *Commentario alla Costituzione*, a cura di R. Bifulco, A. Celotto, M. Olivetti, Vol. I, Torino, 2006; C. Bottari, *Il diritto alla tutela della salute*, in *I diritti costituzionali*, a cura di R. Nania, P. Ridola, Vol. III, Torino 2006; R. Balduzzi, *Diritto alla salute*, in *Dizionario di diritto pubblico*, a cura di S. Cassese, Milano, 2006, 5393 ss.; Id., *Sistemi costituzionali, diritto alla salute e organizzazione sanitaria*, Bologna, 2009; R. Ferrara, *L'ordinamento della sanità*, Torino, 2007.

[11] Il tema sarà meglio inquadrato *infra*.

[12] La lesione dei diritti fondamentali che può essere provocata da un uso non corretto delle applicazioni di IA «è in alcuni casi talmente grave da non essere in alcun modo riparabile o compensabile *ex post*», anche a causa della «estrema velocità con la quale si muove lo sviluppo delle nuove tecnologie». Così, C. Schepisi, *Diritti fondamentali, principi democratici e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e* regolazione, a cura di A. Pajno, F. Donati, A. Perrucci, Vol. I, Bologna, 2022, 206.

In questo nuovo scenario, l'effettività del precetto costituzionale dell'art. 32 non può misurarsi solo sul *quid* della tutela – la cura, l'autorizzazione, la prestazione – alla cui formazione ha concorso la macchina. L'orizzonte costituzionale del diritto alla salute si deve espandere, fino a ricomprendere necessariamente anche il diritto a un'amministrazione sanitaria "giusta nell'utilizzo della tecnologia": un diritto che – come meglio si vedrà – richiede una particolare attenzione alla gestione dei processi e alla loro piena riferibilità umana.

In sostanza, l'intelligenza artificiale non modifica soltanto l'assetto tecnico delle decisioni sanitarie, ma incide anche sulla struttura relazionale della cura, che rappresenta una componente essenziale del diritto alla salute. Da questo punto di vista, l'IA rappresenta una soglia critica del costituzionalismo sanitario: promette una medicina più precisa e predittiva, ma al tempo stesso rischia di ridurre la cura a un processo impersonale, in cui la valutazione clinica potrebbe essere sempre più sovrastata dalle correlazioni algoritmiche e il medico potrebbe diventare un supervisore di *output* automatizzati. La tutela costituzionale del diritto alla salute non può tollerare una simile deriva, perché l'oggetto della protezione non è solo la funzionalità biologica, ma anche la relazione umana della cura.

Sul piano amministrativo, questa esigenza si traduce in una serie di regole e doveri positivi, che la ricca normativa europea – e ora anche la legge nazionale – hanno in parte delineato. Di certo, è solo entro un chiaro perimetro di applicazione che l'utilizzo dell'intelligenza artificiale può tradursi in un effettivo potenziamento del servizio pubblico di cura, che non sacrifichi la dimensione costituzionale della relativa tutela.

3. *Il punto di partenza: la parabola normativa europea*

La recentissima legge n. 132 del 2025 si presenta come il primo tentativo organico di un ordinamento nazionale di dotarsi di un quadro giuridico dettagliato sull'intelligenza artificiale. La portata innovativa di questo intervento normativo – soprattutto nel settore sanitario – può essere pienamente compresa soltanto se collocata dentro la sequenza di passaggi che, *in primis* a livello sovranazionale, ha progressivamente tracciato i confini giuridici dell'IA.

Il percorso europeo può essere articolato in quattro momenti che, pur diversi per oggetto e ambito, delineano una traiettoria coerente: il GDPR, che ha consacrato la protezione dei dati (anche) sanitari come primo pilastro; i regolamenti MDR e IVDR, che hanno qualificato i *software* a finalità clinica come dispositivi medici, assoggettandoli a standard di sicurezza e di efficacia; l'AI Act del 2024, che ha imposto un regime fondato sulla classificazione per livelli di rischio; lo

Spazio europeo dei dati sanitari (EHDS) del 2025, che ha posto le basi per una gestione integrata e controllata delle informazioni cliniche a livello continentale.

La legge italiana si innesta in questo mosaico con una importante funzione di raccordo: parte dalle coordinate fissate a livello unionale e le innerva dei principi costituzionali interni, assumendo – a tal fine – proprio il settore sanitario come banco di prova privilegiato.

3.1. *GDPR e protezione dei dati sanitari*

Dietro ogni algoritmo, dietro ogni modello predittivo, c'è un meccanismo che analizza, elabora e combina una serie di informazioni eterogenee: dati clinici, immagini, cartelle elettroniche, parametri biometrici, valori di laboratorio, per rimanere nell'ambito del settore sanitario. Se questi dati non vengono trattati con rigore giuridico e adeguate garanzie di sicurezza, l'intero edificio algoritmico rischia di poggiare su fondamenta instabili. Per questo motivo il primo, grande tema che deve essere affrontato con riguardo all'impiego dell'IA è quello del trattamento dei dati – nello specifico, sanitari – definendo quali possano essere messi a disposizione della tecnologia, in che modo possano essere utilizzati e alla luce di quali controlli giuridici.

Il Regolamento (UE) 2016/679, noto come GDPR (*General Data Protection Regulation*) costituisce la chiave di volta nella definizione del rapporto tra intelligenza artificiale, dati e diritti fondamentali. Il GDPR ha riconosciuto che i dati relativi alla salute delle persone[13] appartengono a una categoria particolarmente esposta al rischio di lesione della dignità e dell'integrità della persona, e per questo soggetta a un regime di protezione rafforzato[14]. La disciplina del GDPR, in questa prospettiva, influisce sull'amministrazione sanitaria lungo tre direttrici fondamentali[15].

[13] La definizione di "dato sanitario" rappresenta uno dei nodi più complessi e dinamici del diritto europeo dei dati personali. La nozione non si presta a essere circoscritta in un perimetro stabile, confinata al solo ambito clinico. Essa va, piuttosto, intesa come una categoria funzionale e contestuale, la cui qualificazione dipende non soltanto dal contenuto dell'informazione, ma anche dal modo in cui essa viene utilizzata, dalle finalità perseguite e dal contesto di trattamento. Il legislatore europeo, attraverso il considerando 35 del GDPR, ha inteso abbracciare una visione ampia, includendo tra i dati relativi alla salute "qualsiasi informazione che riveli lo stato di salute fisica o mentale di una persona". Cfr. P. Guarda, *I dati sanitari*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, 2019.

[14] Cfr. F. Di Ciommo, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp*., 2-2002; M.S. Bonomi, *Privacy e dati sanitari: le principali novità introdotte dal GDPR,* in *Federalismi*, 2018; R. Panetta (cur.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. 101/2018*, Milano, 2019; E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm*., 2020.

[15] Chiaramente non è possibile, in questa sede, approfondire in maniera adeguata e completa il tema del trattamento dei dati sanitari, così come delineato dalla ricca normativa europea e interna. Per una ricostru-

La prima riguarda la regola della minimizzazione. I dati possono essere raccolti e trattati soltanto nella misura necessaria agli scopi perseguiti e dichiarati. Ciò implica che le amministrazioni sanitarie e le strutture ospedaliere – a maggior ragione laddove si discuta di sistemi algoritmici – non possono accumulare informazioni in maniera indifferenziata, ma devono disegnare con precisione i confini di ogni trattamento, collegandolo a finalità specifiche e proporzionate. In questo modo il principio di proporzionalità, già radicato nella giurisprudenza costituzionale e amministrativa, si proietta dentro l'universo digitale, influenzando *ex ante* la conformazione stessa delle banche dati e degli algoritmi che su di esse operano[16].

La seconda direttrice si innesta sui principi di *privacy by design* e *by default*. Il primo impone di incorporare le regole in materia di protezione dei dati personali a partire dalla progettazione del processo; il secondo obbliga all'adozione di misure tecniche ed organizzative atte a garantire che siano trattati solamente i dati personali necessari per ogni specifica finalità del trattamento. La protezione dei dati non rappresenta, dunque, un adempimento successivo alla progettazione, ma è un vincolo incorporato nella struttura stessa dei sistemi. Ogni architettura informatica deve, così, essere pensata in modo da garantire condizioni predefinite di trattamento, rispettose della riservatezza e costantemente supervisionate[17].

La terza direttrice, la più importante ai fini della nostra analisi, è cristallizzata nell'art. 22 del GDPR. Questa norma sancisce il diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato (compresa la profilazione) laddove la stessa produca effetti giuridici sulla sfera giuridica personale o incida significativamente sulla persona.

Accanto a queste tre direttrici, il GDPR introduce un altro strumento di particolare rilievo per la sanità pubblica: la valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, DPIA). Si tratta di una procedura obbligatoria per tutti i trattamenti che presentano rischi elevati per i diritti e le libertà delle persone fisiche e che richiede di individuare i rischi, valutarne la probabilità e la gravità, adottare misure di mitigazione e documentare l'intero processo. La DPIA traduce, in chiave operativa, il principio di *accountability*: ciò che

---

zione unitaria del tema e della prevalente dottrina, si veda L. Bolognini, S. Zipponi, *Privacy e diritto dei dati sanitari*, Milano, 2024.

[16] Cfr. M. Sinisi, *Uso dei big data e principio di proporzionalità*, in *Federalismi*, 2020; M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quad. cost*., 2016, 3.

[17] Cfr. A. Principato, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings,* in *Contratto e impresa/Europa*, 2015, 1; cfr. anche A. Cavoukian, *Privacy by design: the definitive workshop - A foreword by Ann Cavoukian, IDIS* 2010, 3; cfr. B.J. Koops, R. Leenes, *Privacy Regulation Cannot Be Hardcoded. A critical comment on the "privacy by design" provision in data protection law,* in *International Review of Law, Computers & Technology,* 2014, 28.

rileva non è soltanto il rispetto delle regole, ma la capacità di governare consapevolmente il rischio tecnologico e organizzativo[18].

La giurisprudenza e le Autorità di controllo hanno già avuto modo di applicare questi principi. Il Garante per la protezione dei dati personali, in più occasioni, ha censurato l'uso di sistemi algoritmici in sanità per carenza di base giuridica o per l'assenza di una DPIA adeguata, ribadendo che l'innovazione non può sottrarsi al vaglio di proporzionalità e necessità[19]. Sul piano amministrativo, la disciplina del GDPR appare coerente con i principi generali dell'azione pubblica: la minimizzazione dei dati rappresenta una forma di legalità sostanziale; la *privacy by design* e *by default* si traducono in un modello di buon andamento nella dimensione digitale; il divieto di decisioni interamente automatizzate costituisce presidio di imparzialità e garanzia di eguaglianza sostanziale.

3.2. *MDR/IVDR: software di AI come dispositivi medici*

Il secondo snodo della parabola normativa europea coincide con l'entrata in vigore, nel maggio 2021, dei Regolamenti (UE) 2017/745 e 2017/746, rispettivamente dedicati ai dispositivi medici (*Medical Device Regulation* - MDR) e ai dispositivi medico-diagnostici in vitro (*In Vitro Diagnostic Medical Device Regulation* - IVDR).

Se nel primo stadio normativo l'attenzione era focalizzata sull'utilizzo e la protezione dei dati personali, con i Regolamenti MDR e IVDR il baricentro si sposta: la priorità diventa la qualità clinica e la sicurezza funzionale delle tecnologie. I due regolamenti stabiliscono una regola chiave: un *software* progettato con una destinazione d'uso medico – sia essa la diagnosi, il *triage*, il monitoraggio cli-

[18] Ai sensi dell'art. 35, par. 1 del GDPR, la DPIA è necessaria «quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche». Sul tema, cfr. A. Montalero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati,* in *Il nuovo Regolamento sulla privacy e sulla protezione dei dati personali,* a cura di G. Finocchiaro, Bologna, 2017, 287; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol. II, Torino, 2016, 297-298.

[19] V. Garante per la protezione dei dati personali, Newsletter 24 gennaio 2023, in relazione ai provvedimenti adottati nei confronti di tre Aziende sanitarie del Friuli-Venezia Giulia per l'utilizzo di sistemi di profilazione algoritmica privi di adeguata base giuridica e di valutazione d'impatto preventiva, doc. web nn. 9844989, 9845156, 9845312; nonché doc. web n. 9845106, relativo all'istruttoria avviata nei confronti della Regione Veneto per l'impiego di un algoritmo di gestione delle liste d'attesa; ancora, Provv. 4 agosto 2025, concernente l'Azienda Ospedaliero-Universitaria Careggi di Firenze, in materia di *dossier* sanitario elettronico e misure di sicurezza, doc. web n. 10166336, in Newsletter 25 settembre 2025.

nico o il supporto terapeutico – non è qualificabile come mero strumento informatico, ma acquista a pieno titolo la natura giuridica di dispositivo sanitario[20].

Questa qualificazione ha conseguenze di vasta portata.

Anzitutto, comporta l'obbligo della marcatura CE, che è condizione imprescindibile per l'immissione del dispositivo sul mercato europeo e comporta una procedura rigorosa di valutazione di conformità commisurata al rischio clinico[21].

In secondo luogo, diventa necessario dimostrare la sicurezza e la prestazione clinica del *software* sulla base di evidenze scientifiche validate (artt. 61 ss. MDR e Allegato XIV).

Il Regolamento MDR estende, poi, al *software* il regime di vigilanza *post-market* (artt. 83-86), fondato sulla raccolta sistematica di dati d'uso e sulla segnalazione di incidenti o malfunzionamenti. Tale obbligo grava primariamente sul fabbricante[22], ma si riflette anche sugli operatori sanitari e sulle amministrazioni pubbliche che impiegano tali strumenti, chiamati tutti a garantire un controllo costante e documentato delle prestazioni algoritmiche. Si configura una forma di responsabilità amministrativa diffusa, che proietta nel dominio digitale la logica della farmacovigilanza.

Il *Medical Device Coordination Group* (MDCG), istituito dall'art. 103 dello stesso Regolamento, ha progressivamente precisato questa architettura attraverso una serie di linee guida dedicate ai *medical device software* (MDSW). Tra queste, l'MDCG 2018-5 stabilisce i criteri per l'assegnazione dell'*Unique Device Identifier* (UDI) ai *software* medici, assicurando la piena tracciabilità del ciclo di vita dei dati impiegati o generati dal dispositivo. L'MDCG 2019-11 estende la qualifica di dispositivo medico anche ai *software* indipendenti – inclusi i sistemi di intelligenza artificiale – a prescindere dalla loro collocazione (su *cloud* o su dispositivo locale) e dall'utilizzatore (medico o paziente), riconoscendo che la funzione clinica non dipende più dal supporto materiale, ma dall'elaborazione dei dati. L'MDCG 2020-1 impone anche la necessità di prove cliniche adeguate anche per

[20] L'articolo 2, paragrafo 1, del Regolamento MDR definisce infatti dispositivo medico anche il *software* «destinato dal fabbricante a essere impiegato per finalità mediche specifiche», introducendo un criterio teleologico fondato sulla finalità d'uso.

[21] L'art. 51 del regolamento 2017/745 (MDR) classifica i dispositivi medici secondo un approccio basato sul rischio, considerando la sicurezza degli utenti come una priorità e valutando i potenziali rischi associati all'uso del dispositivo. Il *software* che fornisce informazioni utilizzate per decisioni terapeutiche rientra almeno nella classe IIa, mentre quello che può incidere in modo grave o letale sulla salute del paziente è classificato in classe III. Questa graduazione, chiarita dalle Linee guida del *Medical Device Coordination Group* (MDCG 2021-24), introduce un principio di proporzionalità tecnica che impone, per gli algoritmi più complessi, controlli *ex ante* e sorveglianza *ex post* di particolare intensità.

[22] Le responsabilità dei produttori dei dispositivi medici vengono definite, in particolare, dall'art. 10 e dell'Allegato I del Regolamento, che richiama i requisiti di sicurezza e prestazione da rispettare, l'obbligo agli aggiornamenti e gestione della qualità da parte delle aziende sviluppatrici, l'obbligo di garantire che i dispositivi medici continuino a rispettare i requisiti etici durante tutto il ciclo di vita dello strumento e le responsabilità del produttore in caso di danni causati dal dispositivo difettoso.

i *software* basati su algoritmi, affinché la generazione e l'utilizzo dei dati avvengano nel rispetto di criteri di sicurezza, affidabilità e replicabilità scientifica[23].

In definitiva, con la *Medical device regulation* l'attenzione si sposta dalla componente materiale alla funzione clinica del prodotto, accostando l'algoritmo sanitario al regime dei presidi medici tradizionali e proiettandolo nel paradigma del rischio clinico: non basta che il sistema funzioni, ma è necessario che sia scientificamente affidabile, riproducibile e tracciabile. Ogni passaggio – dalla progettazione, all'immissione in uso, fino alla dismissione – deve essere documentato, validato e riconducibile a standard tecnico-clinici validati e verificabili.

A ben vedere, l'elemento realmente innovativo di tale normativa non risiede nella riclassificazione, nei termini esposti, degli strumenti tecnologici di IA medica, ma nella loro prima sostanziale giuridificazione.

3.3. *L'*AI Act

L'adozione del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, meglio noto come AI Act, segna l'ingresso dell'intelligenza artificiale nel diritto positivo dell'Unione[24]. Per la prima volta a livello mondiale una normativa costruisce un quadro giuridico generale della tecnologia algoritmica, istituendo un insieme coerente di regole, principi e procedure che traducono in legalità pubblica la tensione tra innovazione e diritti.

L'AI Act si colloca nel solco tracciato dal Libro Bianco sull'intelligenza artificiale[25] e dalla Strategia europea per i dati[26] del 2020, che individuano due direttrici tuttora centrali nella politica dell'Unione: la fiducia, intesa come sicurezza per i cittadini che i sistemi di IA operino nel rispetto della dignità umana, dell'u-

[23] Cfr. F. Bini, M. Franzò, A. Maccaro, D. Piaggio, L. Pecchia, F. Marinozzi, *Is medical device regulatory compliance growing as fast as extended reality to avoid misunderstandings in the future?*, in *Health and Technology*, 2023, vol. 13, n. 5, 831-842.

[24] Ai sensi dell'art. 1, il dichiarato scopo del Regolamento è «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione»

[25] Commissione Europea, *Libro Bianco sull'intelligenza artificiale: Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final. Il contributo del Libro bianco intende regolamentare e promuovere l'utilizzo dell'intelligenza artificiale attraverso la sensibilizzazione dell'opinione pubblica circa il suo concreto apporto evolutivo nel processo di digitalizzazione dei servizi e della pubblica amministrazione. Proprio alla PA la Commissione indirizza le raccomandazioni del documento, con l'invito a implementare soluzioni digitali intelligenti compatibili con principi, valori europei e diritti fondamentali. Cfr. M. Tresca, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in *Rivista di diritto dei media*, 2018, 3.

[26] Commissione Europea, *Una strategia europea per i dati*, COM(2020) 66 final.

guaglianza e della protezione dei dati personali e l'eccellenza, intesa come sostegno alla ricerca, alla competitività e all'innovazione.

Il Regolamento 2024/1689 costituisce la traduzione normativa di quella visione, la sua incarnazione in regole giuridiche vincolanti. Non nasce, infatti, come regolazione "di settore", ma si pone come quadro orizzontale volto a garantire e disciplinare la circolazione dei sistemi IA negli Stati membri[27]. Come riportato anche nel primo considerando, il Regolamento n. 2024/1689 intende promuovere l'impiego di un'intelligenza artificiale antropocentrica e affidabile, garantendo al contempo un livello elevato di protezione della salute, della sicurezza e dei diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea.

Il tratto metodologico che conferisce all'AI Act la sua originalità è l'approccio fondato sul rischio[28]. Non tutte le intelligenze artificiali sono uguali: un algoritmo che ottimizza il traffico cittadino o organizza la logistica di un magazzino non può essere equiparato a un *software* che stabilisce la priorità di un paziente in pronto soccorso o che segnala una lesione sospetta in una TAC. Per tale ragione, il legislatore europeo si è orientato verso un modello graduato, nel quale l'intensità delle garanzie varia in funzione del livello di rischio che il sistema di IA comporta per i diritti, la sicurezza e la salute delle persone[29]. Tale impostazione traduce sul piano normativo la logica della proporzionalità già propria del diritto amministrativo: la misura dell'intervento pubblico non è uniforme, ma varia in relazione all'intensità del rischio e alla gravità degli interessi coinvolti[30].

---

[27] Gli obiettivi perseguiti dal Regolamento UE sono esplicitamente indicati all'art. 1. Tra questi, il testo del Regolamento fa riferimento anche alla tutela della salute, della sicurezza, dei diritti fondamentali delle persone, della democrazia, dello Stato di diritto e alla protezione dell'ambiente. Cfr. F. Donati, *La protezione dei diritti fondamentali nel regolamento sull'intelligenza artificiale*, in *Rivista AIC*, 2025, 1.

[28] Cfr. E. Longo, *La disciplina del rischio digitale*, in *La regolazione europea della società digitale*, a cura di F. Pizzetti, Torino, 2024; A. Alemanno, *The Past, Present and Future of Risk Regulation*, *European Journal of Risk Regulation,* 2017, 8, 1; C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in *Federalismi*, 2024; L. Magli, *AI Act: i diritti sono tutelati?*, in *Irpa.eu*, 2024; V. D'Antino, *L'approccio basato sul rischio nell'AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *Federalismi*, 2025.

[29] Cfr. A. Di Martino, *Le proposte emendative del Parlamento europeo sull'Artificial Intelligence Act: percorsi di avanzamento o fase di stallo?*, in *Irpa.eu*, 2022; E. Mandarà, *Il Regolamento UE sull'intelligenza artificiale*, in *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di M. Iaselli, Rimini, 2024; O. Pollicino, G. De Gregorio, F. Bavetta, F. Paolucci, *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, in *agendadigitale.eu*, 21 maggio 2021; R. Petruso, G. Smorto, *Il Regolamento europeo sull'Intelligenza Artificiale: una prima lettura*, in *La nuova giurisprudenza civile commentata*, Padova, n. 4, 2024; F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'Intelligenza Artificiale*, in *Il Diritto dell'Unione Europea*, 2021, 3-4; E. Raffiotta, *I profili definitori ed i principi dell'AI Act*, in *Navigare l'European AI Act*, AIRIA Associazione per la Regolazione dell'Intelligenza Artificiale, Milano, 2024; A. Giovene, *AI Act. Tra perfettibilità e compromessi*, in *Federalismi*, 2024; G. Lo Sapio, *L'Artificial Intelligence Act e la prova di resistenza per la legalità algoritmica*, in *Federalismi*, 2024.

[30] A riguardo, L'*High-Level Expert Group* della Commissione europea, all'interno delle raccomandazioni del 2019 aveva elaborato sette principi etici (intervento e sorveglianza umana; robustezza tecnica e sicurezza; vita privata e governance dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale e ambientale; responsabilità) che, benché non vincolanti, vengono richiamati anche all'interno del Regolamento

Il settore sanitario è collocato tra le aree di impiego dell'intelligenza artificiale considerate ad alto rischio, ai sensi dell'articolo 6 e dell'allegato III del Regolamento. I sistemi di IA utilizzati – tra le altre cose – per diagnosi, prognosi, *triage* o gestione delle risorse cliniche sono dunque soggetti ai requisiti previsti dagli articoli 9-15: gestione del rischio, qualità e rappresentatività dei dati, documentazione tecnica, registrazione automatica delle operazioni, trasparenza e supervisione umana.

Il principio di trasparenza è certamente uno dei pilastri del Regolamento, che lo concepisce come strumento trasversale, funzionale alla comprensione, al controllo e alla responsabilità umana del sistema di IA.

La trasparenza serve a rendere l'uso dell'IA "governabile", a tre livelli.

Il primo livello è rivolto a chi impiega professionalmente sistemi di intelligenza artificiale, come ospedali, enti pubblici o imprese. L'articolo 13 del Regolamento stabilisce, infatti, che i fornitori di sistemi di IA ad alto rischio devono fornire agli utilizzatori «istruzioni d'uso chiare, comprensibili e adeguate al contesto»[31]. Il secondo livello di trasparenza riguarda la spiegabilità funzionale dei sistemi, ossia la possibilità per l'essere umano di capire e dominare il comportamento dell'algoritmo. L'articolo 14 dell'AI Act impone, in tal senso, che tutti i sistemi di IA ad alto rischio siano progettati e sviluppati in modo da consentire una supervisione umana efficace[32]. Un terzo livello di trasparenza riguarda il rapporto tra l'IA e la persona che ne è destinataria o interagisce con essa. L'art. 86 introduce, in questa direzione, un vero e proprio "diritto all'esplicazione" per chi è oggetto di una decisione significativamente influenzata da un sistema di IA ad alto rischio[33]. Nel contesto sanitario, tale obbligo si intreccia con il principio

come criteri orientativi per la disciplina dei sistemi di IA. Cfr. M. Cardone, *La Strategia nazionale sull'Intelligenza artificiale e le prossime sfide dell'Italia*, *Irpa.eu*, 2022.

[31] Queste istruzioni devono indicare, tra l'altro: la finalità prevista del sistema e le sue capacità e limitazioni; le prestazioni attese, le condizioni d'uso e i potenziali rischi; i requisiti qualitativi dei dati utilizzati o necessari al funzionamento; le misure di sicurezza e i sistemi di registrazione automatica delle operazioni (*logging*); le modalità con cui deve essere esercitata la supervisione umana. Questa disposizione non si limita a un obbligo documentale: mira a garantire che chi utilizza l'IA possa comprenderne il funzionamento e gli effetti in modo sufficiente per usarla in modo corretto, prevenendo errori o abusi. In questo senso, l'art. 13 si collega agli artt. 11 e 12, che prevedono rispettivamente: la redazione di una documentazione tecnica completa, che consenta alle autorità di controllo di ricostruire come il sistema è stato progettato e testato; la creazione di registri di attività (*logs*) che documentano il comportamento del sistema, permettendo un controllo ex post sulla sua affidabilità e correttezza.

[32] Il Regolamento specifica che anche l'interfaccia e il *design* del sistema devono permettere all'operatore umano di: comprendere le capacità e i limiti del sistema, anche in relazione al contesto d'uso; interpretare correttamente le uscite (*output*) generate; individuare anomalie, errori o *biases*; interrompere o annullare l'esecuzione del sistema quando necessario; prevenire l'*automation bias*, cioè l'eccessiva fiducia passiva nelle decisioni automatizzate.

[33] «Ogni persona interessata, oggetto di una decisione che incide in modo significativo sui suoi diritti o interessi e che è stata adottata mediante o con il contributo di un sistema di IA ad alto rischio, ha diritto a otte-

del consenso informato, estendendolo alla conoscenza dell'uso di strumenti di IA nella diagnosi, nella terapia o nella gestione dei dati clinici[34].

In questo contesto, il diritto amministrativo ritrova molte delle sue categorie tradizionali. La documentazione tecnica svolge la funzione del fascicolo istruttorio, il controllo umano integra il momento della ragionevolezza della decisione, la trasparenza degli algoritmi diviene strumento di motivazione e di sindacato pubblico. In particolare, l'elemento dell'umanità – in forza della quale l'essere umano deve mantenere un ruolo centrale nel ciclo esplicativo dell'intelligenza artificiale[35] – richiamata dall'articolo 14, rappresenta il cardine di questa impostazione, poiché garantisce che la decisione rimanga imputabile a un soggetto e quindi sia sottoponibile ai regimi ordinari di responsabilità. In tal senso, l'AI Act traduce in regola positiva il principio già affermato dal GDPR all'articolo 22 e conferma la centralità della responsabilità personale come elemento essenziale della legalità algoritmica.

Rilevante è anche il richiamo al principio di *accountability*. L'AI Act obbliga i produttori e gli utilizzatori di sistemi di IA a documentarne la conformità ai requisiti di legge, predisponendo sistemi di gestione e di *audit* continui. Si tratta di un insieme di obblighi che attraversano l'intero ciclo di vita del sistema, dalla progettazione alla dismissione, in coerenza con la *regulation by design* già tracciata dal GDPR.

Il regolamento istituisce un modello di *governance* multilivello, con un *AI Office* europeo incaricato del coordinamento e della vigilanza e autorità nazionali responsabili della notifica e della sorveglianza del mercato. In questa architettura, il potere pubblico recupera un ruolo di direzione e di garanzia nell'ecosistema digitale, assumendo la funzione di custode della correttezza procedurale e dell'affidabilità tecnica dei nuovi strumenti.

L'impianto complessivo dell'*AI Act* non è esente da rilievi critici. Pur configurandosi come il più ambizioso tentativo di regolazione pubblica dell'intelligenza artificiale a livello mondiale, il Regolamento rivela un equilibrio ancora fragile tra promozione dell'innovazione e garanzie sostanziali dei diritti. La centralità del modello *risk-based*, che rappresenta la principale novità metodologica della disciplina, va accolta con una certa cautela: ancorare la tutela dei diritti alla quantificazione del rischio significa, in fondo, assimilare la protezione della persona a

nere dal soggetto utilizzatore una spiegazione chiara e significativa del ruolo svolto dal sistema di IA nella procedura decisionale e dei principali elementi della decisione adottata»: art. 86, Regolamento (UE) 2024/1689.

[34] In tema sarà approfondito *infra*, par. 5.1.

[35] Cfr. B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 2; I.P. Di Ciommo, *La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello Human In The Loop*, in *Federalismi*, 2023; D. Martire, *Human in the loop. L'essere umano come fattore condizionante della – o condizionato dalla– intelligenza artificiale*, in *Rivista italiana di informatica e diritto*, 2024, 2.

una logica di sicurezza del prodotto. Ne deriva il timore che la valutazione del rischio finisca per sostituirsi alla garanzia dei diritti, riducendo la loro inviolabilità a una soglia di "accettabilità", variabile nel tempo e nello spazio applicativo. Come rilevato in dottrina, l'AI Act fissa standard di sicurezza finalizzati a prevenire rischi sistemici generali nella diffusione di applicazioni dell'IA sul mercato europeo, non per garantire il rispetto di regole procedimentali da parte dell'autorità pubblica che fa uso di questa tecnologia. Questa peculiare impostazione lo rende "inadeguato" rispetto alla tutela dei diritti dei cittadini nel rapporto con l'autorità pubblica, se lo si misura con i parametri delle garanzie che devono circondare l'esercizio del potere pubblico[36].

E, in effetti, un recente studio[37] – avviato proprio con l'intento di verificare a livello empirico il livello di efficacia in ambito sanitario delle prescrizioni di trasparenza previste dal diritto dell'Unione nell'utilizzo dei sistemi di IA – ha rilevato l'esistenza di un divario profondo tra trasparenza formale (intesa come adempimento regolatorio, alla luce della normativa europea in materia) e trasparenza sostanziale (intesa come comprensibilità, accessibilità e utilità dell'informazione da parte di tutti i soggetti coinvolti). Questa asimmetria informativa riguarda tutti gli attori del procedimento sanitario algoritmico: i medici esprimono l'esigenza di comprendere il meccanismo di apprendimento e validazione dei dati, per poter esercitare un controllo critico sull'*output* dell'algoritmo; i pazienti, invece, chiedono di sapere "perché" una determinata raccomandazione o diagnosi li riguardi, ossia cercano una spiegazione narrativa più che tecnica; i manager e tecnici si concentrano su affidabilità, robustezza e riferimenti normativi.

C'è da dire, però, che il percorso è ancora in una fase iniziale. L'AI Act non è ancora interamente operativo, poiché prevede un'applicazione lenta e progressiva. Gli anni immediatamente prossimi costituiranno una importante fase di adeguamento, in cui le amministrazioni (anche) sanitarie dovranno farsi parte attiva

---

[36] Così, G. Gardini, *L'uso preparatorio dell'AI come limite agli eccessi regolativi. Per una valutazione "in concreto" dell'intelligenza artificiale applicata all'agire pubblico*, in *Istituzioni del Federalismo*, aprile/giugno 2025, *Nuove tecnologie per nuove amministrazioni. L'intelligenza artificiale applicata alla sfera pubblica*, 275

[37] Cfr. A. Spagnolli, C. Tolomini, E. Beretta, C. Sarra, *Transparency in Healthcare AI: Testing European Regulatory Provisions against Users' Transparency Needs*, Università di Padova, 2025, https://arxiv.org/pdf/2505.17105. La ricerca ha analizzato oltre cento *Instructions for Use* (IFU) di dispositivi e *software* medici basati su IA approvati in Europa tra il 2023 e il 2025, incrociando l'analisi documentale con questionari e interviste a oltre ottocento operatori del settore. È emerso che, nella quasi totalità dei casi, le IFU rispettano i requisiti minimi previsti dal MDR – descrizione delle funzioni, limiti d'uso, rischi noti – ma non consentono una reale comprensione della logica decisionale o della provenienza dei dati utilizzati dal sistema. La maggior parte degli utenti non è in grado di individuare con chiarezza in quale parte del documento si trovino le informazioni che cercano, e tende a sovrastimare la propria capacità di orientarsi tra le sezioni tecniche. Il 66% dei bisogni informativi mappati risulta, infatti, "disperso" tra più sezioni o collocato in modo ambiguo. Le IFU – pensate per un destinatario astratto – non riescono a differenziare i livelli e i linguaggi della trasparenza, finendo per essere documenti formalmente completi ma sostanzialmente opachi.

del processo, integrando stabilmente nei propri processi i protocolli, le procedure e i sistemi previsti dal Regolamento.

3.4. *L'*EHDS*: verso un'infrastruttura europea dei dati sanitari*

Il Regolamento (UE) 2025/327, che istituisce lo Spazio europeo dei dati sanitari (*European Health Data Space* - EHDS), costituisce l'ultimo e più recente tassello del quadro normativo europeo che definisce il regime giuridico dell'intelligenza artificiale in sanità. L'EHDS nasce con l'intento di creare un'infrastruttura giuridica e tecnologica capace di disciplinare in modo unitario la raccolta, la circolazione e l'utilizzo dei dati sanitari, superando la frammentazione nazionale e assicurando standard omogenei a livello europeo.

L'Unione ha così inteso affermare una vera e propria sovranità digitale in materia di salute, declinando il dato sanitario come bene collettivo, la cui gestione deve essere conformata a criteri di equità, sicurezza e rappresentatività[38].

Il regolamento opera una distinzione fondamentale tra uso primario e uso secondario dei dati sanitari. Nel primo caso, i dati servono alla cura diretta del paziente, con l'obiettivo di consentire a ogni cittadino europeo di accedere alle proprie informazioni sanitarie e di condividerle in modo sicuro con i professionisti di altri Stati membri. Questa funzione è assicurata da *MyHealth@EU*, la rete che collega i sistemi sanitari nazionali e garantisce l'interoperabilità dei fascicoli sanitari elettronici[39] attraverso direttive comuni (*European Electronic Health Record Exchange Format* - EEHRxF).

---

[38] Cfr. R. Hussein, L. Scherdel, F. Nicolet, F. Martin-Sanchez, *Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios, International Journal of Medical Informatics*, Volume 170, 2023; E. Biasin, *Spazio europeo dei dati sanitari al rush finale: ecco come cambia la Sanità digitale nell'UE*; G. Cucchiarato, S. Zipponi, *EHDS e uso secondario dei dati sanitari: regole, ruoli e implicazioni*; L. Falciai, P. Perri, *Il regolamento European Health Data Space: l'Europa abbatte le frontiere dei dati medici*, tutti in *Agendadigitale.eu*, 2024-2025.

[39] L'interoperabilità non si esaurisce nella sola capacità tecnica di un sistema di inviare un dato da un nodo ad un altro della rete. Come chiarito dallo *European Interoperability Framework* (EIF) – quadro di riferimento elaborato dalla Commissione europea nel 2017 per la costruzione di servizi pubblici europei digitali e interoperabili – l'interoperabilità si articola su quattro livelli: giuridico, organizzativo, semantico e tecnico. Sul piano giuridico, essa implica la capacità degli ordinamenti nazionali di dialogare attraverso regole armonizzate, superando frammentazioni normative e assicurando una base uniforme per i servizi sanitari digitali. Il Regolamento EHDS realizza tale condizione imponendo agli Stati membri l'adozione di un formato europeo comune per le cartelle cliniche elettroniche e standard condivisi per la gestione e l'uso secondario dei dati. L'interoperabilità organizzativa riguarda invece l'allineamento dei processi e delle responsabilità tra le amministrazioni sanitarie, così da garantire coerenza, comprensibilità e cooperazione tra i diversi livelli del sistema pubblico. A queste si aggiunge la dimensione semantica, che assicura la conservazione del significato e della struttura logica dei dati scambiati. Solo in presenza di standard comuni di rappresentazione e codifica l'informazione sanitaria può essere realmente riutilizzata per scopi clinici, amministrativi o di ricerca, preservando la correttezza del dato originario. Infine, l'interoperabilità tecnica – basata su protocolli e specifiche – rappresenta il fondamen-

Nel secondo caso, i dati vengono utilizzati per finalità di interesse pubblico o scientifico – ricerca, innovazione, programmazione sanitaria, definizione delle politiche pubbliche – attraverso l'infrastruttura *HealthData@EU*, che connette le autorità nazionali responsabili dell'autorizzazione e del controllo dei flussi informativi.

La distinzione tra uso primario e secondario esprime due diversi paradigmi di legittimazione del trattamento: il primo fondato sulla continuità della cura e sull'autodeterminazione informata del paziente; il secondo ancorato all'interesse pubblico alla generazione di conoscenza e alle garanzie procedimentali poste a presidio del suo esercizio.

L'uso secondario costituisce il cuore innovativo dell'EHDS[40], sottoposto a tre regole cardine. Il Regolamento richiede, anzitutto, che l'accesso ai dati avvenga in forma ove possibile anonimizzata o, in alternativa, pseudonimizzata, al fine di non consentire l'identificazione[41] (art. 44, par. 4 e art. 50, par. 2). Ogni accesso deve, poi, essere autorizzato da un organismo competente, incaricato di valutare la legittimità e la proporzionalità della richiesta (artt. 36-38). È, infine, vietato in modo tassativo qualsiasi utilizzo per scopi non sanitari o che possa determinare discriminazioni, profilazioni indebite o forme di sfruttamento commerciale (art. 54).

Questo quadro normativo ha un ruolo cruciale per lo sviluppo e l'utilizzo di sistemi di intelligenza artificiale in sanità. L'IA si alimenta di dati e proprio la frammentazione delle informazioni sanitarie ha costituito fino ad ora uno dei principali ostacoli alla progettazione di algoritmi pienamente efficaci e affidabili in campo medico. Con l'EHDS questo limite viene astrattamente superato: l'Unione mira a istituire una infrastruttura europea del dato sanitario e un ambiente tecnico-giuridico che dovrebbe consentire di utilizzare i dati sanitari in modo dif-

---

to operativo dell'intero sistema, ma anche il livello più critico, poiché deve superare l'attuale frammentazione dei sistemi informativi nazionali e regionali. Cfr. *https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf*. Sul concetto giuridico di "interoperabilità", cfr. M. Cardone, *L'interoperabilità nella pubblica amministrazione*, in *Munus*, 2024, 3, 1043 ss.

[40] Il regolamento (art. 71) riconosce agli interessati il diritto di opporsi – *pro futuro* e con effetti reversibili – all'uso secondario dei propri dati (c.d. *opt-out*), ma prevede eccezioni nei casi in cui la ricerca risponda a motivi di rilevante interesse pubblico, quali la sorveglianza epidemiologica, la farmacovigilanza, o la valutazione di politiche sanitarie. Il regolamento demanda agli Stati membri la concreta attuazione procedurale del diritto di opposizione, nonché l'eventuale individuazione di eccezioni all'*opt-out*. Come rilevato, questa ampia discrezionalità nazionale potrebbe sollevare il rischio di una tutela diseguale dei diritti informativi all'interno dell'Unione, con possibili divergenze nella protezione effettiva della riservatezza e, di riflesso, nella qualità e rappresentatività dei dataset sanitari europei. Cfr. N. Foggetti, G. Pesole, F. De Leo, B. Fosso, M.A. Tangaro, A. Cestaro, F. Licciulli, C. Lo Giudice, M. Chiara, G. Cauli, M. D'ambrosio, *EHDS e Data Governance: Verso un'Europa della Condivisione dei Dati Sanitari*, 2025.

[41] L'anonimizzazione elimina stabilmente ogni legame tra dato e identità, sottraendo il trattamento dall'ambito del GDPR; la pseudonimizzazione, invece, conserva una potenzialità identificativa mediata da una chiave separata e rimane pienamente soggetta alla disciplina del GDPR.

fuso, sicuro, trasparente e verificabile[42]. Da un lato, attraverso fascicoli elettronici interoperabili tra tutti i Paesi dell'Unione; dall'altro, mediante il sistema comune *HealthData@EU*.

L'attuazione del Regolamento, ovviamente, non è immediata. Ogni Stato dovrà adeguare i propri sistemi nazionali di fascicolo sanitario elettronico, istituire un'*Health Data Access Body* (HDAB) e connettersi alla piattaforma europea. Si tratta di un processo complesso, ma di certo destinato a ridefinire il rapporto tra informazione, sanità e amministrazione, con il passaggio dalla tutela del dato individuale a una sua legalità istituzionale, in cui la stessa condivisione dell'informazione diventa esercizio di sovranità e strumento di tutela dei diritti.

4. *La Legge n. 132/2025. Prima lettura nella prospettiva della pubblica amministrazione*

L'analisi della trama normativa europea, maturata in meno di un decennio, ha definito principi e strumenti destinati a orientare l'uso dell'intelligenza artificiale nei sistemi sanitari. Dalla protezione dei dati personali alla qualificazione dei *software* come dispositivi medici, dall'approccio *risk-based* dell'AI Act alla costruzione dello Spazio europeo dei dati sanitari, il diritto dell'Unione ha fissato le coordinate essenziali entro cui l'innovazione algoritmica dovrà muoversi nel prossimo futuro.

In continuità con questa base normativa si colloca la recentissima Legge 23 settembre 2025, n. 132, entrata in vigore il 10 ottobre 2025 e rubricata "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" [43]. Si tratta di una legge-quadro, articolata in sette capi e ventotto articoli[44], che – in una

[42] Cfr. S. Corso, *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *Federalismi*, 2022.

[43] La Legge n. 132/2025 definisce l'intelligenza artificiale, rinviando a quanto stabilito all'art. 3 dell'AI Act, come «sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali», comprendendo sostanzialmente nella nozione sia sistemi predittivi, sia quelli cc.dd. generativi.

[44] La bibliografia sulla legge n. 132/2025 è ovviamente al momento ridottissima. Per un primo inquadramento, si vedano F. Manganaro, *IA e attività amministrativa, alla luce della Legge n. 132/2025*, in *Astrid*, 15/2025; M. D'Amico, *Intelligenza artificiale: nella via italiana una strategia di sviluppo*, Il Sole 24Ore, 25 settembre 2025; O. Pollicino, G. Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, in *Media Laws*, 2025, 2; D. Marongiu, *Algoritmi e diritti. Trasparenza, non-discriminazione e proprietà degli output dell'intelligenza artificiale,* Milano, 2025, 66 ss.; G. Terracciano, *I sistemi di intelligenza artificiale, l'attività amministrativa e il sindacato giurisdizionale, in considerazione della legge n. 132 del 2025*, in *Amministrativamente*, 3-2025; M. Cappai, *Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*, in *Federalismi,* 2024, 30.

dimensione strategica di sviluppo[45] – intrecciano i principi del diritto dell'Unione con l'ordinamento nazionale.

L'art. 3 della Legge n. 132/2025 costituisce la clausola di principio dell'intero impianto normativo. Il legislatore vi condensa la proiezione costituzionale del fenomeno tecnologico, delineando una cornice di legalità sostanziale che subordina la ricerca, la sperimentazione e l'impiego dell'IA al rispetto dei diritti fondamentali e della dignità della persona. Il richiamo ai principi di trasparenza, proporzionalità, accuratezza, spiegabilità e prevenzione del danno conferisce alla norma una portata precettiva che configura un dovere di conformazione dell'azione pubblica e privata ai canoni della responsabilità tecnologica[46]. Come meglio si dirà, l'IA viene sottoposta a un vincolo di giuridicità sostanziale[47], in virtù del quale si stabilisce che la tecnologia può incidere sui processi, non sulle fonti della legittimazione.

Il lessico si allinea al quadro europeo e diviene strumento di indirizzo dell'azione amministrativa, predisponendo sistemi di programmazione e di vigilanza e indicando ambiti settoriali in cui l'intelligenza artificiale deve essere governata con particolare attenzione, primo fra tutti il settore sanitario.

L'articolo 14 della Legge n. 132/2025 rappresenta una delle disposizioni di maggior rilievo sistematico nella nostra prospettiva, poiché definisce i principi generali che regolano l'impiego dell'intelligenza artificiale nell'ambito specifico dell'azione pubblica[48]. In dottrina è stata elaborata da tempo la nozione di "intel-

[45] L'articolo 5 della Legge n. 132/2025 rappresenta il punto di convergenza tra la disciplina pubblicistica dell'intelligenza artificiale e la politica industriale nazionale, configurando lo sviluppo tecnologico come interesse pubblico primario. La norma introduce un deciso profilo di sovranità tecnologica, che riafferma il ruolo attivo dello Stato nell'indirizzare, promuovere e garantire i processi di innovazione. Il legislatore riconosce nella valorizzazione produttiva dell'intelligenza artificiale non solo uno strumento di competitività economica, ma anche un fattore di modernizzazione amministrativa e di rafforzamento dell'autonomia strategica del Paese.

[46] Particolarmente rilevante è la saldatura tra cybersicurezza e tutela della persona vulnerabile, che riflette l'intento di integrare la sicurezza digitale nella più ampia architettura dei diritti umani. L'obbligo di garantire l'accesso alle tecnologie per le persone con disabilità, in conformità alla Convenzione ONU del 2006, segna l'ingresso del principio di inclusività algoritmica nel diritto positivo italiano.

[47] Prima dell'approvazione della Legge n. 132/2025, l'Agenzia per l'Italia Digitale (AgID) ha avviato e concluso la consultazione pubblica delle *Linee guida per l'adozione, l'acquisto e lo sviluppo di sistemi di intelligenza artificiale nella pubblica amministrazione,* previste dal *Piano Triennale per l'Informatica nella PA 2024-2026*. Aperta a febbraio 2025 e conclusa il 20 marzo 2025, la consultazione ha rappresentato il primo confronto strutturato tra amministrazioni, università, imprese e cittadini sull'impiego pubblico dell'IA. Le Linee guida si inseriscono nel percorso di progressiva costruzione di una legalità algoritmica, fornendo alle amministrazioni un quadro operativo di riferimento per la valutazione, l'acquisto e la gestione dei sistemi di IA. Pur in attesa della pubblicazione definitiva ai sensi dell'art. 71 del Codice dell'amministrazione digitale, esse hanno avuto il merito di anticipare i temi poi cristallizzati nella Legge n. 132/2025: la necessità di una trasparenza effettiva dei processi decisionali automatizzati, la tracciabilità delle decisioni e la formazione del personale come condizione di responsabilità istituzionale nell'uso della tecnologia.

[48] Secondo parte della dottrina, con questa norma il legislatore italiano intende ridimensionare notevolmente il *favor* per la decisione algoritmica, «non solo ribadendo l'imprescindibilità della "sorveglianza umana", ma

ligenza artificiale amministrativa" [49], per descrivere l'insieme delle implicazioni giuridiche, organizzative e procedimentali derivanti dall'introduzione di sistemi intelligenti nei processi decisionali della pubblica amministrazione. Tale concetto s'incardina sulla concezione per la quale la tecnologia non rappresenta un mero strumento tecnico, ma è un fattore strutturale di trasformazione del modo stesso di amministrare.

Il legislatore nazionale, nel delineare questa prospettiva, si colloca in coerenza con il Regolamento (UE) 2024/1689 (AI Act), che individua le pubbliche amministrazioni tra i *deployers*, vale a dire i soggetti che utilizzano «sistemi di intelligenza artificiale sotto la propria autorità» [50]. Tale qualifica comporta una serie di obblighi specifici – di controllo, documentazione, sorveglianza e trasparenza – che rendono l'amministrazione pubblica non solo utilizzatrice di tecnologia, ma anche garante della sua conformità giuridica e del rispetto dei diritti fondamentali [51].

Il legislatore affronta direttamente la questione e colloca l'IA in una prospettiva strumentale rispetto all'efficienza della funzione pubblica: può ampliare la capacità operativa dell'amministrazione, ma non sostituirne la decisione [52]. Il richiamo – centrale – alla conoscibilità del funzionamento e alla tracciabilità dell'impiego dell'IA traduce la tensione, ormai centrale nel diritto amministrativo contemporaneo, tra efficienza algoritmica e controllo democratico. Ed è anche una proiezione interna del principio di *accountability* già sancito dall'AI Act e dal GDPR e qui declinato come forma di legalità procedimentale. L'IA può supportare, ma non sostituire, l'esercizio della discrezionalità amministrativa e la responsabilità giuridica e morale del provvedimento deve rimanere in capo alla persona fisica [53].

---

anche sbarrando la strada all'utilizzo dei sistemi di IA nella fase decisoria del procedimento, per relegarla alla fase istruttoria». Cfr. C. Polidori, *Procedimento amministrativo e algoritmi*, in *www.giustizia-amministrativa.it*, 2025.

[49] Cfr. P. Forte, *Diritto amministrativo e data Science. Appunti di intelligenza amministrativa artificiale (AAI)*, in *PA Persona e Amministrazione*, 2020, 1; G. Terracciano, *I.I.A. (intelligenza artificiale amministrativa) e sindacato giurisdizionale*, in *Amministrativ@mente*, 2022, 2.

[50] Cfr. art. 3, paragrafo 1, n. 4, Regolamento UE 2024/1689.

[51] Come ben sintetizzato da M. Corradino, *Potere pubblico e intelligenza artificiale*, in L*'intelligenza artificiale tra regolazione e esperienze applicative. AI Act (regolamento UE) e disegno di legge governativo*, a cura di. A.F. Uricchio e C. Caldarola, 42 ss., la giurisprudenza amministrativa ha individuato, progressivamente, tre limiti nell'utilizzo dell'intelligenza artificiale da parte della pubblica amministrazione, a garanzia dei diritti fondamentali dei cittadini. Il primo è il limite della "conoscibilità" dell'algoritmo; il secondo è quello della "non esclusività" (*human in the loop*); il terzo è il limite della "non discriminazione". Questi profili sono tutti presi in considerazione dal legislatore, in particolare – come meglio si vedrà – con riferimento al settore sanitario.

[52] In linea con la giurisprudenza amministrativa: cfr., da ultimo, Cons. di Stato, sezione IV, 4 giugno 2025, n. 4857, in *www.giustizia-amministrativa.it*: «occorre distinguere tra decisione amministrativa algoritmica e algoritmo di mero supporto alle decisioni che restano rigorosamente affidate al fattore umano e che, dunque, si inscrivono nella più tradizionale impostazione, che vede nell'informatica un mero ausilio rispetto allo svolgimento dell'attività amministrativa nelle sue classiche modalità operative».

[53] La dottrina, sul punto, è ferma. Cfr. G. Clemente di San Luca, M. Paladino, *Decisione amministrativa e intelligenza artificiale*, in *Federalismi*, 2025, 4, 133, che richiamano il principio di "non esclusività della decisione algoritmica", secondo cui nel processo decisionale deve sempre esistere «un contributo umano capace di controllare, validare ovvero smentire la decisione automatica»; N. Paolantonio, *Il potere discrezionale della pubblica*

Questa clausola di imputazione soggettiva è presidio fondamentale di legittimità, finalizzato a garantire che l'algoritmo non venga mai considerato autonomo soggetto di azione, neppure nei casi di sistemi di apprendimento automatico.

Di particolare rilievo è, nella stessa direzione, l'obbligo di formazione e di competenza digitale degli operatori amministrativi, che segna il passaggio da una logica di mera adozione tecnologica a una di "apprendimento istituzionale". L'efficacia dell'IA nella pubblica amministrazione non può, infatti, dipendere soltanto dalla sofisticazione degli strumenti, ma richiede la capacità dell'apparato di comprenderne i limiti, i rischi e le implicazioni (giuridiche, tecniche, etiche). In tal senso, la disposizione si allinea a un nuovo paradigma culturale, che mette al centro un'amministrazione che apprende, riflette e governa consapevolmente l'innovazione[54].

La Legge n. 132/2025 istituisce un modello organico di *governance* pubblica dell'intelligenza artificiale, superando la frammentarietà degli interventi precedenti.

L'articolo 19 istituisce la Strategia nazionale per l'intelligenza artificiale, che rappresenta il fulcro dell'intero impianto di *policy*. Il documento deve essere ela-

---

automazione. Sconcerto e stilemi (sul controllo giudiziario delle decisioni algoritmiche), in *Dir.Amm*., 2021, 4, 820 ss., secondo cui l'imputabilità della decisione algoritmica deve «restare all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo»; D.U. Galetta, J. Corvalán, *Intelligenza artificiale per una PA 4.0*, in *Riv. it. dir. pub. com*., 2021, 113 ss., che evidenziano come l'automazione dell'azione pubblica possa accrescere l'efficienza amministrativa, ma solo entro un quadro che preservi i principi di imparzialità, trasparenza e responsabilità. Nella stessa direzione: G. Pasceri, *Le incertezze dell'istruttoria nella decisione amministrativa algoritmica*, in *Amministrativamente*, 2023, 120 ss.; G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. informaz. e informatica*, 2021, 436 ss.; M. Botto, *Decisione algoritmica, discrezionalità e sindacato del giudice amministrativo*, in Dir. proc. amm., 2022, 1013 ss.; M. Timo, *Algoritmo e potere amministrativo*, in Questa Rivista, 2020, 1, p. 753 ss.; M. Francaviglia, *L'intelligenza artificiale nell'attività amministrativa: principî e garanzie costituzionali nel passaggio dalla regula agendi alla regola algoritmica*, in Federalismi, n. 17/2024, 121 ss.; E. Carloni, *Algoritmi su carta. Amministrazione digitale e trasparenza algoritmica*, in *Riv. trim. dir. pub*., 2020, 627 ss., che sottolinea come la legalità amministrativa nell'era digitale richieda non solo la tracciabilità tecnica dei processi decisionali automatizzati, ma anche la loro piena intelligibilità giuridica. Come si vedrà *infra*, con specifico riguardo al settore sanitario, la trasparenza algoritmica deve essere intesa, ancor di più, come dovere di motivazione in senso sostanziale, che consente al cittadino e al giudice di comprendere le ragioni della decisione e di esercitare un controllo effettivo sulla stessa.

[54] Le "*Linee guida per l'adozione, l'acquisto e lo sviluppo di sistemi di intelligenza artificiale nella pubblica amministrazione"*, previste dal *Piano Triennale per l'Informatica nella PA 2024-2026 e predisposte dal*l'Agenzia per l'Italia Digitale (in corso di pubblicazione; cfr. *supra* nota 47) prevedono, tra le figure professionali di cui le pubbliche amministrazioni devono dotarsi nello sviluppo e gestione di progetti e soluzioni che si basano sull'IA, quella del *"*giurista informatico*"*, definito come «un esperto in grado di combinare competenze legali e informatiche per fornire consulenze legali relative all'uso delle tecnologie informatiche che possano impattare su temi come la protezione dei dati personali, la sicurezza informatica e la proprietà intellettuale. Una figura professionale in grado anche di redigere e revisionare contratti relativi a *software*, licenze ecc., assicurando che siano conformi alle normative vigenti senza dimenticare le tematiche legate alla compliance, alla gestione delle controversie e all'analisi e la valutazione dei rischi derivanti dall'uso di una tecnologia come l'intelligenza artificiale». Gli ulteriori profili professionali di cui l'amministrazione dovrebbe dotarsi, pure richiamati dalle Linee guida, sono molteplici e altamente specializzati: *data engineer*, *machine learning engineer*, *prompt engineer*, *deep learning engineer*, *data scientist*, *AI engineer*, *AI architect*, *esperto di cybersecurity*, *AI ethicist*.

borato dal Dipartimento per la trasformazione digitale presso Presidenza del Consiglio dei ministri, d'intesa con le Autorità nazionali per l'intelligenza artificiale e deve essere approvata dal Comitato interministeriale per la transizione digitale, con cadenza almeno biennale. La Strategia definisce le priorità di intervento e costituisce il quadro di riferimento vincolante per le amministrazioni pubbliche, con la funzione di orientare la ricerca pubblica e privata, coordinare i programmi di investimento, orientare la collaborazione tra p.a. e soggetti privati[55].

L'articolo 20 individua le due Autorità nazionali per l'intelligenza artificiale, in linea con l'art. 59 dell'AI Act europeo: l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN). All'AgID spettano compiti di promozione, standardizzazione, registrazione e notifica dei sistemi di IA, nonché il raccordo tecnico con la Commissione europea e con l'AI Office istituito a Bruxelles. All'ACN sono invece attribuite le funzioni di vigilanza sui sistemi di IA ad alto rischio, di verifica della sicurezza informatica e di coordinamento con le reti europee di cybersicurezza.

Presso la Presidenza del Consiglio è istituito un Comitato di coordinamento interistituzionale, composto dai direttori generali di AgID e ACN e dal Capo del Dipartimento per la trasformazione digitale, con il compito di assicurare l'uniformità di indirizzo, l'interoperabilità delle piattaforme pubbliche e la circolarità delle informazioni tra le autorità coinvolte. Il Comitato svolge una funzione di cabina di regia del sistema nazionale dell'intelligenza artificiale, evitando duplicazioni e garantendo un raccordo operativo tra i livelli tecnico, politico e amministrativo.

Rimangono ferme, in questo quadro, le competenze del Garante per la protezione dei dati personali, che mantiene la propria autonomia funzionale, costituendo il presidio indipendente della tutela dei diritti nel trattamento dei dati.

La *governance* dell'IA viene, così, formalmente inscritta in un sistema ordinato di azione. La realtà applicativa rischia, però, di essere molto meno lineare ed efficace rispetto alla prospettazione legislativa. Da una parte, come rilevato in dottrina, vista l'attitudine dell'IA a "fondersi" con il decisore umano (se non tendenzialmente a sostituirlo)[56], le enunciazioni della Legge n. 132/2025 potrebbero essere del tutto insufficienti se non accompagnate – in tempi rapidi – dall'elaborazione di protocolli procedimentali *ad hoc* e regole di buona amministrazione algoritmica[57].

---

[55] La stessa norma istituisce un Comitato di coordinamento con composizione interministeriale e funzioni rivolte al raccordo delle attività di indirizzo esercitate sugli enti e sulle fondazioni, pubbliche o private, che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale e che sono sottoposti a vigilanza o finanziamento pubblico.

[56] Cfr. G. Terracciano, *I sistemi di intelligenza artificiale, l'attività amministrativa e il sindacato giurisdizionale, in considerazione della legge n. 132 del 2025*, cit., 823.

[57] Cfr. E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, *in Dir. Amm.*, 2020, 2, 271 ss.; D. Ponte, G. Pernice, *L'intelligenza artificiale e l'algoritmo a contatto col diritto amministrativo: rischi e speranze*, in *www.giustizia-amministrativa.it*, 2021.

Dall'altra, la stessa legge sembra talvolta confidare eccessivamente nella capacità autoregolativa dell'apparato pubblico. L'architettura enunciata è ambiziosa, ma i meccanismi di attuazione rimangono incerti e affidati a una "*governance* per principi" che rischia di tradursi in una diluizione di responsabilità. Ad esempio, l'obbligo di formazione e competenza digitale, seppur cruciale, è privo di una reale strategia di implementazione e il rinvio alle risorse presenti "a legislazione vigente" (art. 14, comma 4) segnala il limite materiale di una riforma che pretende di trasformare l'amministrazione senza dotarla di mezzi adeguati. Anche l'ampiezza del mandato affidato alla Presidenza del Consiglio e alle agenzie tecniche rischia di concentrare in un unico polo decisionale poteri eterogenei – normativi, tecnici e di controllo – senza ancora un chiaro bilanciamento istituzionale. La piena effettività della *governance* delineata dipenderà in ampia parte anche dalla capacità di coordinamento verticale tra ministeri, regioni e autorità indipendenti, che restano titolari di competenze settoriali rilevanti.

Nel complesso, la Legge n. 132/2025 introduce un paradigma potenzialmente evolutivo, ma ancora sospeso tra l'enunciazione di principi e la costruzione di strumenti effettivi di attuazione.

5. *I tre capisaldi della Legge n. 132/2025 per l'utilizzo dell'intelligenza artificiale nel settore sanitario*

Nel disegno della Legge n. 132/2025 la sanità rappresenta il banco di prova più significativo per la nuova regolazione dell'intelligenza artificiale.

L'impianto normativo si articola lungo tre direttrici complementari, che delineano un quadro organico di regole: la tutela dei percorsi di cura, con la riaffermazione della centralità del giudizio umano nel processo decisionale sanitario (art. 7); la regolazione del trattamento dei dati sanitari anche per finalità di ricerca, sperimentazione e sviluppo di sistemi di intelligenza artificiale (art. 8); la creazione di un'infrastruttura pubblica nazionale per l'utilizzo dell'IA in sanità, integrata con il Fascicolo Sanitario Elettronico e con le piattaforme digitali del Servizio Sanitario Nazionale (art. 10). Queste tre componenti delineano un modello di IA che ambisce a coniugare l'innovazione tecnologica con la responsabilità istituzionale, secondo criteri di affidabilità, equità e controllo.

5.1. *L'intelligenza artificiale nei percorsi di cura*

La garanzia dei percorsi di cura, innanzitutto, viene ancorata al principio dell'imputazione personale e umana della decisione. Il giudizio clinico e la determinazione terapeutica devono rimanere riferibili a un soggetto umano, perché solo la persona può assumerne la responsabilità giuridica, scientifica e morale (art. 7, comma 5, l. n. 132/2025). L'algoritmo deve rimanere strumentale rispetto ai processi di prevenzione, diagnosi, cura e scelta terapeutica e lasciare impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica. Tale clausola interna – già prevista in termini generali dalla legge – riflette il divieto di decisioni unicamente automatizzate previsto dall'art. 22 del GDPR e il presidio di controllo umano imposto dall'art. 14 dell'AI Act per i sistemi ad alto rischio.

La riaffermazione dell'imputazione personale segna solo il primo livello di garanzia. Il secondo, di natura sostanziale, riguarda la posizione soggettiva del paziente, poiché l'impiego dell'intelligenza artificiale nei percorsi di cura influisce direttamente sul suo diritto all'autodeterminazione terapeutica[58]. Ne deriva che l'obbligo di informare l'interessato circa l'utilizzo e il funzionamento dei sistemi algoritmici impiegati (art. 7, comma 3, l. n. 132/2025) deve essere interpretato come nuovo corollario imprescindibile del consenso informato[59]. L'informazione deve essere effettiva e comprensibile e riguardare, ragionevolmente, almeno quattro profili: (i) la presenza dell'IA nel percorso; (ii) la natura di supporto dell'*output*; (iii) le principali logiche dell'elaborazione, espresse in un linguaggio accessibile; (iv) le limitazioni note (ambito di validità clinica, rischio di errore, necessità di verifica).

---

[58] Cfr. C. De Menech, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in *BioLaw Journal*, 2022, 193 ss.; D. Morana, T. Balduzzi, F. Morganti, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione*, in *Federalismi*, 2022, 34, 27 ss.; A.G. Grasso, *Diagnosi algoritmica errata e responsabilità medica*, in *Riv. dir. civ*., 2023, 353 ss.

[59] Come rileva V. Viti, *Consenso al trattamento terapeutico e intelligenza artificiale*, in *Giureta, Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, XXIII, 2025, 665, la maggior parte degli autori che si sono occupati della questione si è espressa in favore dell'inclusione dell'informazione sull'utilizzo di sistemi intelligenti nell'obbligo comunicativo dell'operatore sanitario. Cfr. R. Messinetti, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr*., 2019, 861 ss.; C. Casonato e L. Violante, *Forum: AI and Law*, in *BioLaw Journal*, 2020, 463 ss.; G. Muto, L. Tosco, *Forum: AI and Law*, ivi, 507; A.E. Tozzi, G. Cinelli, *Informed consent and artificial intelligence*, *ivi*, *Special Issue*, 2021, 2, 106 ss.; D. Morana, T. Balduzzi, F. Morganti, *La salute "intelligente"*, cit., 141 ss.; A.G. Grasso, *Diagnosi algoritmica errata e responsabilità medica*, cit., 354 ss.; P. Zuddas, *Intelligenza artificiale in medicina: alcune risposte – significative, ma parziali – offerte dal codice di deontologia medica (in materia di non discriminazione, consenso informato e relazione di cura)*, in *Riv. it. inf. dir*., 2024, 2, 28 ss. In questa stessa direzione si pongono anche sia la Legge n. 219/2017 ("Norme in materia di consenso informato e di disposizioni anticipate di trattamento"), il cui art. 1, comma 3 impone un'informazione al paziente completa e comprensibile su diagnosi, prognosi, benefici e rischi dei trattamenti, sia l'art. 78 del Codice di deontologia medica, che prevede l'obbligo del medico di acquisire il consenso del paziente «nell'uso degli strumenti informatici» e di assicurare la consapevole partecipazione dell'assistito.

In tal modo, la conoscibilità delle procedure e delle logiche algoritmiche – benché non possa essere intesa come piena "*comprensibilità",* nel senso tradizionalmente attribuito al principio di trasparenza amministrativa[60] – assume la forma di un "diritto di spiegazione ragionevole"[61]. Si tratta di un livello di trasparenza funzionale e proporzionata, che non pretende la divulgazione integrale del codice o dei modelli computazionali, ma garantisce al paziente la possibilità di capire in che modo l'algoritmo ha inciso sul percorso di cura e di esercitare consapevolmente i propri diritti di contestazione, verifica e riesame umano[62].

Il secondo comma dell'articolo 7 focalizza un altro profilo molto importante, ovvero il rischio che dall'utilizzo dell'intelligenza artificiale possano derivare, anche in modo indiretto, condizionamenti negativi nell'erogazione delle prestazioni sanitarie.

L'intelligenza artificiale, in particolare nei sistemi basati sul *machine learning*[63], non è mai intrinsecamente neutrale: nutrendosi dei dati inseriti nel sistema, riflette la loro qualità, rappresentatività e coerenza. Ogni sua applicazione in sanità agisce come un prisma che può rifrangere il principio di uguaglianza in diverse direzioni: rafforza l'equità e la qualità dei servizi quando è governata con criteri di trasparenza e inclusività; la compromette quando opera attraverso logiche indecifrabili o su basi informative non rappresentative. La correttezza del sistema non dipende, dunque, soltanto dalla qualità del *software* che viene impie-

[60] Cfr. M. Ramajoli, *L'amministrazione pubblica deve cercare di sfruttare tutte le potenzialità insite nell'Intelligenza artificiale, senza però abbandonare l'aspirazione a essere aperta e adattabile alle circostanze concrete*, in *Il Mulino*, 2024.

[61] Come già rilevato, nel lessico giuridico internazionale, il principio della *explainability* – riconosciuto, in forma implicita, dal combinato disposto dell'art. 22 GDPR, dell'art. 13 dell'AI Act e dal Consiglio d'Europa nel 2023 (*Recommendation CM/Rec[2023]2 on the Ethics of AI in Healthcare)* – indica la necessità che l'algoritmo resti, almeno nei suoi tratti essenziali, intellegibile all'uomo. Cfr., *supra*, par. 3.3. La spiegabilità essenziale rappresenta una soglia invalicabile, al di là della quale l'algoritmo si riduce a una delega cieca, incompatibile con la responsabilità che caratterizza l'agire pubblico. Cfr. M. Zalnieriute, L. Bennet Moses, G. Williams*, The Rule of Law and Automation of Government Decision-Making*, in *The modern Law Review*, 2019, 435; U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 1, 2020, 96 ss.; M. Palmirani, *Big Data e conoscenza*, in *Rivista di filosofia del diritto*, 1, 2020, 74 ss.; Per alcune considerazioni sulla conoscibilità dell'algoritmo, si vedano M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi*, 2019; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Rivista di Bio Diritto*, n. 1, 2019; F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

[62] Il Consiglio di Stato ha chiaramente affermato che l'utilizzo di sistemi algoritmici e procedure automatizzate non può essere invocato dalla pubblica amministrazione per limitare o negare il diritto di accesso agli atti. Le difficoltà tecniche connesse alla gestione dell'intelligenza artificiale, al funzionamento di piattaforme esterne o alla necessità di coinvolgere soggetti terzi non costituiscono un valido motivo di diniego del diritto di accesso agli atti. Cfr., da ultimo, Cons. di Stato, sez. VI, 6 giugno 2025, n. 4929, in *www.giustizia-amministrativa.it*.

[63] In questi casi il dispositivo agisce sulla base di algoritmi di autoapprendimento, in grado di attribuire ad esso una spiccata autonomia che si manifesta nella capacità dello strumento di autoprogrammarsi e di operare scelte elaborando notevoli volumi di dati attraverso complessi percorsi che tendono a rimanere in parte ignoti agli stessi programmatori. Il fenomeno viene sinteticamente qualificato con la formula della *black box*: cfr. F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, 2015.

gato, ma anche dall'integrità del patrimonio informativo su cui esso opera. Un *dataset* incompleto o distorto (come nei casi in cui manchino dati relativi alle specificità sintomatologiche femminili, predicate dalla c.d. medicina di genere) produce decisioni cliniche parziali e, in ultima analisi, discriminatorie.

Si produce, dunque, quello che nel linguaggio tecnico viene identificato come *bias*.

Nel contesto dell'IA applicata alla sanità, il *bias* può essere definito come qualsiasi differenza sistematica e non giustificata nelle previsioni riferite a diversi gruppi di pazienti, tale da produrre trattamenti diseguali nell'erogazione delle cure. Attraverso questi meccanismi, l'algoritmo può generare o amplificare disparità nei benefici o nei rischi attribuiti a specifici individui o categorie, indebolendo la capacità del sistema sanitario di garantire prestazioni eque, imparziali e realmente adeguate ai bisogni di tutti[64]. Nella nostra prospettiva, i *biases* dei sistemi di intelligenza artificiale valgono come veri e propri "vizi di giuridicità", che alterano la parità di trattamento e incidono sull'eguaglianza sostanziale nell'esercizio del diritto alla salute, ponendo in discussione la conformità stessa dell'azione amministrativa sanitaria ai principi costituzionali che la governano.

Anche alla luce di tale rischio, il requisito di affidabilità dei sistemi di intelligenza artificiale, previsto dall' art. 7, comma 6, assume un rilievo decisivo. La norma proietta il controllo tecnico sulle tecnologie algoritmiche tra le garanzie intrinseche del buon andamento. Ciò si traduce, sul piano pratico, in un insieme articolato di obblighi a carico delle strutture sanitarie, tenute ad assicurare la validazione iniziale dei sistemi, la verifica periodica delle loro prestazioni, l'individuazione di soglie di allerta e di procedure per la disattivazione o la ricalibrazione in presenza di deviazioni significative. Il controllo e l'aggiornamento dei sistemi

[64] Cfr. M. DeCamp, C. Lindvall, *Latent bias and the implementation of artificial intelligence in medicine*, in *J. Am. Med. Inform. Assoc*., 2020, 27; L.H. Nazer et al., *Bias in artificial intelligence algorithms and recommendations for mitigation*, in *PLOS Digital Health*, 2023. I *biases* possono essere suddivisi in quattro macrocategorie: *human biases*; *data biases*, *algorithmic biases* e *model deployment biases*. Appartengono alla prima categoria: il *bias implicito*, cioè l'influenza di stereotipi inconsci nelle decisioni cliniche; il *bias sistemico*, legato a norme e pratiche istituzionali che generano disuguaglianze strutturali; il *bias di conferma*, che porta a privilegiare dati o interpretazioni coerenti con convinzioni preesistenti; il *training–serving skew*, cioè la divergenza tra i dati utilizzati in fase di addestramento e quelli incontrati nella pratica corrente; il *concept shift*, che riguarda i cambiamenti nel significato clinico di diagnosi o variabili nel tempo. I *data biases* includono il *bias di rappresentazione*, dovuto alla sotto o sovra rappresentazione di alcuni gruppi di pazienti; il *bias di selezione*, quando il campione incluso non riflette la popolazione reale; il *bias di campionamento*, derivante da raccolta non casuale dei dati; il *bias di misurazione*, introdotto da differenze tecniche nelle modalità di acquisizione o processamento delle informazioni. Gli *algorithmic biases* comprendono l'*aggregation bias*, legato all'uniformazione dei dati che cancella le specificità dei sottogruppi, e il *feature selection bias*, cioè la scelta inappropriata di variabili o proxy che distorce le previsioni. Infine, i *model deployment biases* includono l'*automation bias*, ossia un'eccessiva fiducia nelle raccomandazioni dell'IA; il *feedback loop bias*, in cui gli errori dell'IA vengono rinforzati attraverso cicli di riaddestramento; e il *dismissal bias* o *alert fatigue*, che porta gli utenti a ignorare segnalazioni e avvisi a causa della loro frequenza o scarsa accuratezza. Cfr. F. Hasanzadeh, C.B. Josephson, G. Waters *et al. Bias recognition and mitigation strategies in artificial intelligence healthcare applications*, in *npj Digit. Med.,* 2025, 8, https://doi.org/10.1038/s41746-025-01503-7.

basati su IA deve sempre avvenire in maniera controllata e documentata, così da poter ricostruire anche a distanza di tempo le modifiche apportate e garantire una piena trasparenza e responsabilità nell'utilizzo della tecnologia[65].

Il controllo di affidabilità diventa, così, uno strumento di giustizia sostanziale, volto a garantire che l'efficienza della tecnologia non si traduca in diseguaglianza delle cure. In questa stessa direzione si colloca la clausola di accessibilità e inclusione prevista dal medesimo comma 6 dell'art. 7, che impone la progettazione di interfacce comprensibili e canali alternativi di informazione e consenso, in coerenza con i requisiti di progettazione dei sistemi ad alto rischio previsti dall'AI Act e con la Convenzione ONU sui diritti delle persone con disabilità (ratificata con Legge n. 18/2009).

L'innovazione tecnologica non è neutra né fine a sé stessa: nel paradigma delineato dal legislatore, essa deve essere orientata alla rimozione delle barriere e non alla loro proliferazione, facendo dell'affidabilità algoritmica una componente imprescindibile della tutela della salute e della realizzazione dell'eguaglianza effettiva tra i cittadini. In definitiva, con il nuovo sistema normativo della legge n. 132/2025, vengono interiorizzati dall'ordinamento nazionale tre presidi fondamentali di legalità applicabili ai percorsi di cura integrati dall'uso di IA: la decisione clinica umana effettiva, con responsabilità imputabile e controllo sostanziale sull'*output* algoritmico (c.d. *human in the loop*); l'informazione qualificata all'assistito e tracciabilità dell'uso dell'IA nel fascicolo clinico, a tutela di consenso, contestabilità e riesame; la verificabilità e l'aggiornamento dei sistemi secondo standard europei di qualità del dato, sicurezza, equità e sorveglianza continua, con integrazione – ove applicabile – dei regimi MDR/IVDR.

5.2. *Intelligenza artificiale, ricerca e sperimentazione scientifica in ambito medico*

L'articolo 8 della Legge n. 132/2025 disciplina in modo organico il trattamento dei dati personali utilizzati per la ricerca e la sperimentazione scientifica nella creazione di sistemi di intelligenza artificiale in ambito sanitario[66]. La dispo-

[65] Al fine di prevenire i *biases*, a ciò si aggiunge l'esigenza di verificare periodicamente come il sistema si comporta nei confronti dei diversi gruppi di pazienti – distinti, ad esempio, per età, sesso o condizioni cliniche – così da rilevare con tempestività eventuali distorsioni sistematiche nelle sue valutazioni. È inoltre necessario annotare gli eventi avversi e gli episodi che avrebbero potuto degenerare in errore (*near miss*), in modo da disporre di un quadro informativo utile al miglioramento continuo dello strumento. Quando i sistemi di IA rientrano nel perimetro dei dispositivi medici (MDS), tali obblighi devono integrarsi con le procedure previste dal Regolamento (UE) 2017/745 (MDR), in particolare in materia di marcatura CE, sorveglianza *post-market*, vigilanza e gestione del rischio. Cfr., *supra*, par. 3.2.

[66] Al comma 1 dell'art. 8, il legislatore delimita tassativamente l'area di applicazione della norma, individuando un ambito oggettivo costituito dai «trattamenti di dati anche personali e di quelli particolari/sensibili,

sizione mira a comporre un equilibrio fra due poli tradizionalmente in tensione: da un lato, la tutela dei diritti fondamentali di protezione dei dati e riservatezza; dall'altro, la promozione della ricerca e dell'innovazione biomedica come espressione dell'interesse pubblico alla salute e al progresso scientifico.

Il comma 1 della norma stabilisce, innanzitutto, chi sono i soggetti legittimati a trattare i dati. Sono sempre ammessi i soggetti pubblici (università, enti di ricerca, aziende sanitarie locali, ospedali pubblici) e i soggetti privati senza scopo di lucro (fondazioni, associazioni di ricerca, istituti scientifici riconosciuti). Anche i soggetti privati a fini di lucro possono operare, ma esclusivamente se inseriti in progetti di ricerca congiunti con enti pubblici, Istituti di ricovero e cura a carattere scientifico (IRCCS) o organizzazioni non *profit*. La collaborazione pubblico-privata, dunque, è ammessa quando la finalità del progetto sia chiaramente di interesse pubblico e quando la *governance* dei dati sia garantita da un ente amministrativo o da un organismo indipendente.

Lo stesso comma qualifica "di *rilevante interesse pubblico"* i trattamenti di dati effettuati per la sperimentazione e la realizzazione di sistemi di IA destinati a prevenzione, diagnosi, cura e riabilitazione, allo sviluppo di farmaci, dispositivi medici e tecnologie sanitarie[67]. Tale espressione rinvia direttamente all'articolo 9, paragrafo 2, lettera g) del Regolamento (UE) 2016/679 (GDPR), che consente il trattamento di categorie particolari di dati personali senza il consenso dell'interessato quando il legislatore nazionale individui un motivo di interesse pubblico rilevante e stabilisca garanzie adeguate[68]. Ne consegue che, per i trattamenti contemplati dall'art. 8, la base giuridica non è il consenso, ma la qualificazione normativa dell'attività di ricerca come interesse pubblico primario. Ciò non comporta una riduzione delle tutele, poiché il trattamento resta comunque subordinato

rivolti a ricerca, sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale finalizzati alla prevenzione, diagnosi, cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, salute pubblica, incolumità della persona; nonché a quei trattamenti rivolti alla: ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale finalizzati allo studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario in quanto necessari alla realizzazione e all'utilizzazione di banche dati e modelli di base».

[67] La formulazione adottata dal legislatore è particolarmente ampia e ricomprende anche lo sviluppo di apparati medicali, protesi e interfacce uomo-macchina, fino a includere lo studio della fisiologia, della biomeccanica e della biologia umana, anche quando tali attività si svolgano in ambito non sanitario. L'elencazione normativa, pur dettagliata, deve ritenersi non tassativa: ciò che rileva è che il trattamento sia necessario per la realizzazione o l'utilizzazione di banche dati, modelli di base o sistemi algoritmici destinati a finalità di salute pubblica, sicurezza sanitaria o avanzamento della conoscenza biomedica e biotecnologica.

[68] In base a tale disposizione, il trattamento delle categorie particolari di dati personali – tra cui rientrano i dati sanitari – è in linea di principio vietato, salvo che sia "necessario per motivi di rilevante interesse pubblico", sia fondato su una norma di diritto nazionale e accompagnato da misure adeguate a tutelare i diritti dell'interessato. L'articolo 8 risponde precisamente a questa logica, costituendo la base giuridica interna che abilita il trattamento dei dati sanitari senza il consenso individuale, quando sia diretto alla tutela della salute pubblica o al progresso della conoscenza scientifica.

al rispetto delle misure tecniche e organizzative richieste dal GDPR, che operano come contrappeso essenziale[69].

Il comma 2 della norma si occupa, poi, del riutilizzo degli stessi dati sanitari per scopi di ricerca ulteriori o diversi da quelli per cui erano stati originariamente raccolti. Questa disposizione è di grande importanza pratica: consente ai soggetti indicati nel comma 1 di impiegare dati già disponibili – anche appartenenti alle categorie particolari – senza acquisire un nuovo consenso, a condizione che tali dati siano privi di elementi identificativi diretti. L'accesso all'identità dell'interessato rimane possibile solo in casi eccezionali, quando ciò sia inevitabile o necessario per garantire la tutela della sua salute, ad esempio per comunicare un risultato clinicamente significativo o un rischio emerso durante l'attività di ricerca.

Questa previsione recepisce, a livello nazionale, la logica del *secondary use* dei dati sanitari delineata dal Regolamento (UE) 2025/327 sullo Spazio europeo dei dati sanitari (EHDS), secondo cui i dati raccolti per finalità di cura (uso primario possono essere riutilizzati per scopi di interesse pubblico o scientifico, quali ricerca, innovazione, programmazione sanitaria o sviluppo di modelli algoritmici, purché siano adeguatamente anonimizzati o pseudonimizzati e il loro accesso sia sottoposto alla verifica dell'*Health Data Access Body* nazionale[70].

Il terzo comma dello stesso art. 8 consente, infine, il trattamento dei dati personali sanitari, anche appartenenti a categorie particolari, per finalità diretta di anonimizzazione, pseudonimizzazione o creazione di dati sintetici. Queste operazioni costituiscono un prerequisito essenziale per lo sviluppo di modelli di *machine learning* e per la validazione degli algoritmi, poiché consentono di disporre di *dataset* ampi e statisticamente rappresentativi, senza compromettere la riservatezza individuale[71]. L'anonimizzazione e la pseudonimizzazione, già previste dal Regolamento (UE) 2016/679 (GDPR), rappresentano due diverse modalità di riduzione del rischio di re-identificazione: la prima elimina in modo irreversibile ogni legame con la persona; la seconda conserva una chiave di corrispondenza, utilizzabile solo da soggetti autorizzati. A queste si aggiunge la più recente pratica della generazione di dati sintetici, contemplata anche dal Regolamento (UE) 2025/327 (EHDS), che

[69] In particolare: la pseudonimizzazione, la limitazione delle finalità, la minimizzazione dei dati e la valutazione d'impatto (DPIA). Chiaramente, resta obbligatoria – in tutti i casi contemplati dalla norma – anche la previa informativa all'interessato, che può essere fornita anche in forma generale, ad esempio pubblicata sul sito *web* del titolare del trattamento. Questa soluzione semplifica la gestione di progetti di ricerca complessi, che coinvolgono grandi quantità di dati, senza sacrificare la trasparenza nei confronti delle persone.

[70] Cfr., *supra*, par. 3.4.

[71] La norma aggiunge che sono ammessi analoghi trattamenti anche per lo studio dei gesti atletici e delle prestazioni sportive, purché vengano rispettati i principi della legge e i diritti economici di chi organizza le competizioni sportive. Si tratta di un'estensione interessante: il legislatore riconosce che la ricerca sul movimento umano, pur non essendo strettamente sanitaria, può contribuire allo sviluppo di tecnologie di riabilitazione e dispositivi assistivi.

riproducono, mediante modelli statistici o di apprendimento automatico, le caratteristiche aggregate dei dati reali, senza riferirsi a individui specifici.

In sintesi: il comma 1 riguarda i trattamenti effettuati per svolgere attività di ricerca e sperimentazione qualificati dal legislatore come "di rilevante interesse pubblico"; il comma 2 disciplina il riutilizzo degli stessi dati per attività di ricerca ulteriori rispetto alle finalità originarie; il comma 3 ha invece natura tecnica e consente il trattamento volto a anonimizzare, pseudonimizzare o generare dati sintetici.

In questa prospettiva complessiva, il dato personale sanitario, tradizionalmente concepito come oggetto di tutela diretta, viene reinterpretato come bene funzionale all'interesse collettivo. La disposizione definisce un modello di "legalità proporzionata", in cui il consenso individuale viene sostanzialmente traslato su un piano sistemico, dove la legittimazione deriva dalla finalità pubblica del trattamento e dal rispetto di una serie di garanzie oggettive.

La tutela del dato si trasfigura in requisito procedimentale dell'innovazione.

All'Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS) è attribuito il compito di definire, con il parere del Garante per la protezione dei dati personali, delle linee guida in materia di anonimizzazione, pseudonimizzazione e produzione di dati sintetici, per garantire l'omogeneità degli standard tecnici e giuridici sull'intero territorio nazionale. Particolarmente significativa è la disciplina del meccanismo di comunicazione preventiva al Garante (art. 8, comma 5), che impone a qualunque soggetto intenzionato a effettuare i trattamenti previsti dalla norma di informare l'Autorità circa: le misure tecniche e organizzative adottate; le valutazioni d'impatto sulla protezione dei dati (DPIA); l'eventuale designazione dei responsabili del trattamento[72]. I trattamenti possono avere inizio trascorsi trenta giorni dalla comunicazione, salvo che il Garante disponga, entro tale termine, il blocco motivato dell'attività. Non si tratta, dunque, di un sistema autorizzatorio in senso stretto, ma di un modello di vigilanza preventiva che consente all'Autorità di esercitare controllo e di intervenire prima che il trattamento produca effetti potenzialmente lesivi. In astratto, ciò aumenta la capacità di intercettare rischi prima che si traducano in danno; nella pratica, tuttavia, potrebbe generare un flusso massivo di comunicazioni standardizzate, difficilmente gestibile dall'Autorità senza risorse aggiuntive.

Il successivo art. 9 demanda a un decreto del Ministro della Salute la definizione delle *modalità operative* dei trattamenti di dati destinati alla ricerca e alla sperimentazione di sistemi di IA in sanità. Il decreto ministeriale sarà chiamato a colmare una lacuna regolativa significativa. La legge definisce l'ambito applicati-

[72] Opportuna è stata la scelta, operata dal legislatore, di sopprimere l'obbligo di preventiva approvazione da parte dei comitati etici, emerso nel corso dell'*iter* parlamentare di discussione del progetto di legge. In tal modo è stato alleggerito l'onere procedurale senza tuttavia pregiudicare i poteri ispettivi, interdittivi e sanzionatori del Garante della Privacy. Cfr. www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?did=59313.

vo, ma non ne disciplina alcuni punti chiave, tra cui i criteri per valutare la necessità del trattamento senza consenso, il coordinamento con la DPIA, le misure tecniche di prevenzione dei *biases* algoritmici, le condizioni per l'eventuale riidentificazione nei casi eccezionali[73]. Regolazione che difficilmente potrà avvenire nel termine di 120 giorni. Il ritardo (altamente probabile) nell'emanazione del decreto non sospenderà l'efficacia della norma primaria, ma scaricherà sui titolari del trattamento un onere interpretativo elevato, con il rischio di generare comportamenti difensivi, applicazioni eterogenee sul territorio e potenziali frizioni con il Garante.

5.3. *La nuova infrastruttura pubblica*

L'articolo 10 della legge n. 132/2025 interviene sul decreto-legge 18 ottobre 2012, n. 179, (convertito con modificazioni nella legge 17 dicembre 2012, n. 221), che costituisce il quadro normativo del Fascicolo Sanitario Elettronico (FSE)[74]. La disposizione introduce il nuovo articolo 12-*bis*, rubricato «Intelligenza artificiale nel settore sanitario», con l'obiettivo di integrare in modo sistematico l'uso di tecnologie di IA nella gestione del FSE e affida a uno o più decreti del Ministro della Salute il compito di definire sia le caratteristiche tecniche e funzionali dei sistemi di IA, sia le categorie di soggetti abilitati ad accedervi.

Per il supporto alle finalità di cura, in particolare dell'assistenza territoriale, il nuovo art. 12-*bis* istituisce una "Piattaforma di intelligenza artificiale". La progettazione, la realizzazione, la messa in esercizio e la gestione della piattaforma sono attribuite all'AGENAS (Agenzia Nazionale per i Servizi Sanitari Regiona-

[73] Sul piano sistematico, il decreto costituirà la cerniera tecnico-giuridica tra il quadro normativo nazionale e quello europeo. Il documento dovrebbe ragionevolmente disciplinare anche: la standardizzazione dei protocolli di anonimizzazione, pseudonimizzazione e generazione di dati sintetici, in coerenza con le linee guida AGENAS (art. 8, co. 4); la predisposizione di modelli di DPIA rafforzata, con metriche di rischio, accuratezza e distorsione, nonché soglie di riesame periodico; la fissazione di moduli uniformi di comunicazione preventiva al Garante (art. 8, co. 5); l'individuazione di tempi di conservazione, *logging* e *audit trail*, per garantire la tracciabilità e la responsabilità delle operazioni; il raccordo con lo Spazio europeo dei dati sanitari (EHDS), per assicurare interoperabilità e compatibilità con il sistema *MyHealth@EU* per l'uso primario e con il futuro *Health Data Access Bodies* per l'uso secondario.

[74] L'art. 12 del decreto-legge n. 179 del 2012 definisce il FSE come l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario conseguenti ad eventi clinici attuali o passati con riferimento al singolo assistito. Il D.P.C.M. 29 settembre 2015, n. 178 ha, poi, qualificato il *nucleo minimo* dei dati che compongono il Fascicolo Sanitario Elettronico, comprendente *dati identificativi e amministrativi dell'assistito, referti, prescrizioni, dati relativi all'assistenza domiciliare e specialistica, diagnosi, piani terapeutici, verbali di pronto soccorso e consenso alla donazione di organi e tessuti*. Cfr. S. Corso, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, a cura di A. Thiene, S. Corso, Napoli, 2023. Questa struttura costituisce il substrato informativo di base su cui si innestano oggi i servizi di intelligenza artificiale previsti dalla legge n. 132/2025, in una prospettiva di integrazione funzionale e di interoperabilità nazionale ed europea (cfr. D.P.C.M. 29 settembre 2015, n. 178, art. 2, comma 2).

li), che assume espressamente la funzione (supplementare) di Agenzia nazionale per la sanità digitale.

La piattaforma dovrà erogare servizi di supporto rivolti a tre categorie di destinatari.

In primo luogo, ai professionisti sanitari, per migliorare la presa in carico della popolazione assistita. In secondo luogo, ai medici, per l'attività clinica quotidiana, attraverso sistemi che forniscano suggerimenti diagnostici e terapeutici non vincolanti[75]. Infine, ai cittadini, per agevolare l'accesso ai servizi sanitari, in particolare nelle Case della Comunità[76].

Per la definizione operativa dei servizi, la norma prevede che AGENAS adotti un provvedimento, da emanarsi previa intesa in sede di Conferenza Stato-Regioni, che specifichi nel dettaglio le funzionalità della piattaforma e garantisca il raccordo con i sistemi informativi regionali.

La disciplina ribadisce la centralità della protezione dei dati sanitari e della sicurezza informatica. AGENAS è individuata come titolare del trattamento dei dati raccolti e generati all'interno della piattaforma, assumendo piena responsabilità sulla loro gestione, nel rispetto del Regolamento (UE) 2016/679. Il nuovo articolo 12-*bis* impone ad AGENAS anche l'obbligo di adottare – previo parere del Ministero della Salute, del Garante per la protezione dei dati personali e dell'Agenzia per la Cybersicurezza Nazionale – un provvedimento che descriva in modo puntuale le tipologie di dati trattati, le operazioni di trattamento e le misure tecniche e organizzative destinate a garantirne la sicurezza.

La nuova disciplina, pur innovativa, presenta alcune criticità applicative.

In primo luogo, la clausola di invarianza finanziaria (art. 10, comma 2, l. n. 132/2025), che esclude nuovi oneri per la finanza pubblica. L'assenza di fondi dedicati rischia di rallentare lo sviluppo della piattaforma e di limitarne la portata innovativa, salvo attingere a risorse già stanziate in altri programmi nazionali o europei in materia di sanità digitale (quali PNRR, *EU4Health* o *Digital Europe*).

Un secondo profilo critico riguarda l'integrazione della piattaforma con i sistemi regionali e con il Fascicolo Sanitario Elettronico (FSE), ancora caratterizzati da eterogeneità strutturale e semantica. Il Fascicolo Sanitario Elettronico, disciplinato dall'art. 12 del d.l. 179/2012 e dal D.P.C.M. 29 settembre 2015, n. 178, costituisce già un archivio digitale unitario dei dati clinici e amministrativi dell'assistito, istituito a livello regionale ma interoperabile in ambito nazionale. L'interoperabilità è assicurata dall'Infrastruttura nazionale per l'interoperabilità (INI), istituita ai sensi dello stesso art. 12 del d.l. n. 179/2012 e regolata dal

[75] Si pensi, ad esempio, ad allerte su interazioni farmacologiche o anomalie cliniche e a raccomandazioni basate su dati epidemiologici e predittivi.

[76] Obiettivo da perseguire, ad esempio, tramite servizi digitali intelligenti come assistenti virtuali, *triage* automatizzato o percorsi guidati di prenotazione e orientamento.

D.P.C.M. n. 178/2015, poi potenziata dall'art. 11 del d.l. 19 maggio 2020, n. 34, che ne ha esteso funzioni e flussi informativi[77]. In questo quadro, l'introduzione dell'art. 12-bis fa sì che l'INI assuma, in via sistemica, il ruolo di naturale punto di interfaccia tra i fascicoli regionali e la piattaforma AGENAS, anche al fine di consentire la circolazione standardizzata dei dati e il loro riutilizzo per finalità di analisi predittiva e supporto clinico, nel rispetto dei requisiti previsti dal Regolamento (UE) 2025/327 sullo Spazio europeo dei dati sanitari (EHDS)[78]. La piattaforma di intelligenza artificiale attribuita ad AGENAS si colloca dunque in una cornice multilivello già stratificata, fungendo da diaframma funzionale nazionale incaricato di elaborare i flussi informativi provenienti dai fascicoli regionali e dai sistemi di telemedicina, secondo i principi europei di minimizzazione, sicurezza e supervisione pubblica.

La piena attuazione della disciplina richiederà, evidentemente, un complesso lavoro di armonizzazione tecnica e giuridica, in buona parte delegato ai decreti attuativi e ai provvedimenti di AGENAS. In assenza di un disegno tecnico e semantico realmente efficace, il rischio è che la piattaforma AGENAS si sovrapponga – più che innestarsi – sull'ecosistema esistente, trasformando l'INI da motore di interoperabilità a mero collettore di complessità.

Un terzo aspetto critico riguarda la formazione del personale sanitario. L'utilizzo dei sistemi di IA richiede competenze altamente qualificate, che le amministrazioni sanitarie in buona parte non possiedono. La legge n. 132/2025 dedica alla formazione un riferimento solo indiretto (art. 14), rinviando a futuri programmi, ma non prevede obblighi minimi né una strategia nazionale legata all'introduzione della piattaforma AGENAS. Sarebbe, dunque, auspicabile che AGENAS, il Ministero della Salute e le Regioni[79] – in raccordo con università e ordi-

[77] Cfr. E. Sorrentino, A.F. Spagnuolo, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico,* in *Federalismi*, 2020; N. Posteraro, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi*, 2021.

[78] L'EHDS, come già ricordato, impone infatti agli Stati membri di assicurare l'interoperabilità dei fascicoli sanitari nazionali mediante *MyHealth@EU* e l'adozione di formati comuni europei per le categorie di dati clinici. Cfr., *supra*, par. 3.4. L'INI costituisce, a ben vedere, la condizione tecnica necessaria per la portabilità transfrontaliera dei dati e la mutua leggibilità dei documenti clinici. Il decreto del Ministero della salute del 31 dicembre 2024, pubblicato il 5 marzo 2025 ha istituito, in attuazione dell'art. 12, comma 15-*quater*, del d.l. n. 179/2012, anche l'Ecosistema dei dati sanitari (EDS). Si tratta di un'infrastruttura tecnologica progettata per ricomprendere i dati trasmessi al Fascicolo sanitario elettronico (FSE) dalle strutture sanitarie e sociosanitarie e dagli enti del Servizio sanitario nazionale (SSN), nonché i dati resi disponibili tramite il sistema Tessera sanitaria. Il sistema dovrebbe entrare in funzione entro il 31 marzo 2026.

[79] Come rileva M. De Donno, *Le Regioni e l'intelligenza artificiale*, in *Istituzioni del Federalismo*, aprile/giugno 2025, *Nuove tecnologie per nuove amministrazioni. L'intelligenza artificiale applicata alla sfera pubblica*, 253 ss., anche il recente Regolamento UE 2024/903, *Interoperable Europe Act* prevede – e raccomanda agli Stati membri – un coinvolgimento diretto di Regioni ed enti locali per la sua attuazione. Secondo i Considerando 9, 10 e 12, ad enti regionali e locali va riconosciuto «un ruolo attivo» tanto «nello sviluppo delle soluzioni di interoperabilità» quanto nel coinvolgimento di «PMI, istituti di ricerca e istruzione e [della società civile».

ni professionali – avviassero fin da ora programmi formativi obbligatori e linee guida nazionali, affinché l'evoluzione normativa non resti disallineata rispetto alle reali capacità operative del sistema sanitario.

5.4. *La gestione del rischio algoritmico nell'amministrazione sanitaria. Qualche indicazione operativa*

L'impiego di sistemi di intelligenza artificiale introduce una morfologia del rischio profondamente diversa da quella che l'amministrazione ha finora conosciuto. L'analisi delle pagine precedenti consente di isolare almeno sei aree di rischio particolarmente rilevanti per il settore sanitario che, tradotte in chiave giuridico-amministrativa, delineano altrettante sfere di adempimenti per le strutture pubbliche.

Un primo profilo riguarda il rischio di *bias* e di discriminazione, connesso alla possibilità che gli algoritmi, se addestrati su dati non rappresentativi o incompleti, generino decisioni distorte e discriminatorie. In coerenza con l'art. 10 dell'AI Act, con l'art. 7 della l. n. 132/2025 e con il principio di non discriminazione algoritmica elaborato dal Consiglio di Stato[80], le strutture sanitarie sono chiamate a introdurre meccanismi di validazione dei *dataset*, *audit* periodici sulla qualità dei dati e procedure di tracciabilità delle fonti (c.d. *data lineage*), così da garantire imparzialità e coerenza nelle basi informative.

Un secondo ambito è costituito dal rischio di errore clinico o decisionale, che si manifesta quando l'algoritmo produce raccomandazioni errate o non aggiornate, intrecciato con quello dell'imputabilità delle decisioni automatizzate. Da ciò deriva l'obbligo di assicurare una supervisione umana effettiva (*human-in-the-loop*), prevista dagli artt. 3, 7 e 14 della legge n. 132/2025, in forza della quale ogni decisione automatizzata deve essere validata da un operatore qualificato. Le strutture sanitarie dovrebbero pertanto designare, per ogni processo in cui interviene un sistema algoritmico, un referente clinico-amministrativo responsabile della validazione, dotato della possibilità di sospendere, correggere o disattendere l'*output* dell'algoritmo quando necessario. Contestualmente, è necessario documentare nel fascicolo procedimentale – o nel fascicolo sanitario elettronico,

[80] Il Consiglio di Stato ha stabilito che l'utilizzo di sistemi di intelligenza artificiale, dagli algoritmi al c.d. *machine learning*, va inteso quale modulo procedimentale per lo svolgimento dell'attività autoritativa in modalità più efficienti ed è regolato dai principi di conoscibilità e comprensibilità, non esclusività della decisione algoritmica, non discriminazione algoritmica. In questa direzione, l'amministrazione non può mai trincerarsi dietro la non conoscibilità o l'opacità dei meccanismi informatici di gestione. Cfr. Cons. di Stato, Sez. VI, 13 dicembre 2019, n. 8472, nonché, da ultimo, Cons. di Stato, Sez. VI, 6 giugno 2025, n. 4929, tutte in *www.giustizia-amministrativa.it*.

a seconda dei casi – l'utilizzo del sistema, la persona fisica incaricata della supervisione e le motivazioni della decisione finale.

Vi è poi il rischio di uso improprio, che si verifica quando un algoritmo viene riutilizzato al di fuori del contesto per il quale era stato progettato. In base al principio di limitazione della finalità (art. 5 GDPR), l'amministrazione sanitaria, per agire nella piena legalità, dovrebbe istituire registri dei sistemi di IA con l'indicazione delle finalità autorizzate, dei responsabili di progetto e delle eventuali riutilizzazioni.

Particolarmente delicato è poi il rischio per la *privacy* e la sicurezza dei dati, atteso che i sistemi di IA sanitaria si fondano sull'elaborazione massiva di dati sensibili. Ne derivano precisi e imprescindibili adempimenti: condurre DPIA preventive (art. 35 GDPR), adottare adeguate misure di sicurezza *by design* e *by default* (art. 25 GDPR), mantenere un registro dei trattamenti (art. 30 GDPR) e coinvolgere attivamente il *Data Protection Officer* (DPO) nelle fasi di progettazione e monitoraggio.

Un quinto rischio riguarda la mancata trasparenza e spiegabilità (*explainability*) dei processi algoritmici. L'art. 13 dell'AI Act, l'art. 7 della l. n. 132/2025 e il principio di legalità algoritmica impongono che le decisioni automatizzate siano comprensibili e verificabili. Di conseguenza, le strutture sanitarie dovrebbero conservare *log* e documentazione tecnica delle decisioni automatizzate, garantire la comunicabilità della logica del sistema ai medici e ai pazienti e predisporre *report* di trasparenza algoritmica accessibili alle autorità di controllo[81].

Infine, va considerato il rischio di obsolescenza e mancato aggiornamento. Gli algoritmi clinici, se non sottoposti a revisione periodica, possono perdere affidabilità tecnica. Ai sensi degli artt. 83 e ss. del Regolamento (UE) 2017/745 (MDR), le strutture devono pretendere dai produttori un programma di sorveglianza *post-market*, con controlli periodici di accuratezza, revisione annuale dei modelli e nuova validazione clinica in caso di modifiche sostanziali. Il mancato aggiornamento potrebbe integrare una forma di *culpa in vigilando* e violare il principio di buon andamento di cui all'art. 97 Cost.

[81] L'art. 30, comma 2, lett. a) del Codice dei contratti pubblici, D.lgs. n. 36/2023 richiede che, nell'acquisire soluzioni informatiche fondate su procedure automatizzate, l'amministrazione disponga del codice sorgente, della documentazione tecnica e degli elementi necessari a comprenderne le logiche di funzionamento. Come rilevato da M. Corradino, in *Potere pubblico e intelligenza artificiale*, in L*'intelligenza artificiale tra regolazione e esperienze applicative*, cit., 52, la natura opaca dei modelli di intelligenza artificiale e la tutela del segreto industriale rendono spesso difficile verificare realmente ciò che la norma pretende, esponendo la P.A. al rischio di un controllo solo apparente e a una dipendenza informativa dal fornitore. In questo scenario, secondo l'A., acquistano rilievo i contratti innovativi previsti dall'art. 70 dello stesso Codice dei contratti pubblici, che permettono all'amministrazione di "dialogare" con il mercato e di partecipare alla definizione della soluzione tecnologica. Attraverso tali procedure, già diffuse in altri ordinamenti europei, la P.A. potrebbe contribuire alla costruzione dell'algoritmo sin dalla fase progettuale, assicurando trasparenza, verificabilità e un effettivo presidio umano sul processo decisionale.

5.5. **Time-line *attuativa***

L'attuazione della Legge 132/2025 si estrinsecherà in un contesto normativo europeo molto complesso e in rapido movimento[82]. La piena operatività delle misure nazionali dipenderà in buona parte dal progressivo allineamento, in particolare, con due regolamenti chiave dell'Unione: l'AI Act e il Regolamento sullo Spazio europeo dei dati sanitari (EHDS). Entrambi i testi fissano scadenze e obblighi che incidono e si intersecano con l'architettura italiana dell'intelligenza artificiale in sanità. Altri adempimenti, seppur non espressamente circoscritti temporalmente dalla legge, dovrebbero effettuarsi di pari passo.

Entro centoventi giorni dall'entrata in vigore della legge (11 ottobre 2025), dovrà essere emanato il decreto del Ministro della Salute previsto dall'articolo 9, volto a precisare le modalità operative del trattamento dei dati sanitari per finalità di ricerca e sperimentazione scientifica. Questa prima tappa è fondamentale per rendere applicabili gli articoli 8 e 10 della legge, che disciplinano rispettivamente la ricerca basata su intelligenza artificiale e la piattaforma nazionale AGENAS.

Nel primo semestre del 2026 potrebbero vedere la luce le prime linee guida dell'AGENAS sulle tecniche di anonimizzazione e sulla generazione di dati sintetici (art. 8, comma 4, l. 132/2025). Nello stesso periodo, l'Agenzia dovrebbe avviare la progettazione della piattaforma di intelligenza artificiale in sanità, da sottoporre all'intesa della Conferenza Stato-Regioni (art. 10, comma 3, l. 132/2025). Questi atti, di natura tecnico-operativa, rappresentano la prima condizione per la costruzione della nuova infrastruttura nazionale che dovrà interagire con il Fascicolo Sanitario Elettronico 2.0 e con l'Infrastruttura Nazionale per l'Interoperabilità (INI).

Sempre nel 2026, sul piano europeo, il Regolamento sullo Spazio europeo dei dati sanitari (EHDS) – che impone agli Stati membri di garantire l'interoperabilità dei fascicoli sanitari e di istituire un organismo nazionale di accesso ai dati *Health Data Access Body* (artt. 7-10 e 33-38 EHDS) – inizierà a essere concretamente attuato, in vista delle prime scadenze applicative. Parallelamente, anche l'AI Act avvierà la sua fase di piena applicazione. Entro il 2026 la Commissione europea metterà a regime l'*AI Office*, incaricato di coordinare le autorità nazionali e di gestire il registro dei sistemi di intelligenza artificiale ad alto rischio (artt. 56-57 AI Act). L'Italia dovrà quindi completare la designazione formale di AgID e ACN come Autorità nazionali per l'IA, in conformità con l'articolo 59 dell'AI Act e predisporre i relativi regolamenti interni.

[82] Come rilevato da G. Gardini, *L'uso preparatorio dell'AI come limite agli eccessi regolativi*, cit., 263, da più parti sono state espresse preoccupazioni per la *overregulation* dei sistemi di AI.

Il 2027 costituirà l'anno di consolidamento. È in questa fase che dovrebbe avvenire la pubblicazione della prima Strategia nazionale per l'intelligenza artificiale, adottata dalla Presidenza del Consiglio tramite il Dipartimento per la Trasformazione Digitale e approvata dal Comitato interministeriale per la transizione digitale (art. 19, commi 1-3, l. 132/2025). Il documento dovrà definire gli obiettivi generali, i piani di investimento e i meccanismi di coordinamento con le politiche europee in materia di ricerca e salute digitale. Contestualmente, AGENAS dovrebbe completare la valutazione d'impatto (DPIA) sul trattamento dei dati della piattaforma, acquisire i pareri del Ministero della Salute, del Garante e dell'Agenzia per la Cybersicurezza Nazionale e adottare il provvedimento attuativo che disciplina le operazioni e le misure di sicurezza interne (art. 10, comma 5, l. 132/2025).

Il 2028 rappresenterà la tappa di piena integrazione. Entro tale anno dovrebbero trovare applicazione le principali previsioni del Regolamento EHDS, con l'interconnessione dei sistemi nazionali alla rete europea *MyHealth@EU* (artt. 12-15 e 49-52 EHDS) e dovrebbe dunque essere messa a regime la piattaforma AGENAS, interoperabile con i fascicoli sanitari regionali (art. 10, commi 2-3, l. 132/2025). Nello stesso arco temporale, le autorità nazionali per l'IA (AgID e ACN) saranno probabilmente tenute a pubblicare le prime relazioni annuali sull'attività di vigilanza e sull'allineamento con gli standard europei di sicurezza e conformità (art. 20, comma 5, l. 132/2025, in raccordo con art. 59 AI Act).

Nel complesso, l'Italia dovrà procedere su due piani paralleli: da un lato, la costruzione interna di infrastrutture e procedure; dall'altro, l'integrazione di tali strumenti nel più ampio quadro europeo di *governance* dei dati e dell'intelligenza artificiale. La sfida principale sarà mantenere sincronismo tra le tappe nazionali e quelle europee, evitando che ritardi nei decreti o nelle linee guida compromettano la partecipazione del Paese alle reti e ai registri comuni. Se il calendario verrà rispettato, entro la fine del 2028 la Legge n. 132/2025 potrà dirsi pienamente avviata, segnando il completamento della prima infrastruttura pubblica di intelligenza artificiale sanitaria a livello europeo.

6. *Conclusioni*

Dall'analisi condotta sono emerse alcune indicazioni utili per rispondere alle questioni poste in apertura. I tre profili individuati – la ridefinizione dei procedimenti e delle responsabilità pubbliche, la necessità di una disciplina specifica per l'uso degli algoritmi sanitari e la costruzione di una cultura amministrativa digitale – appaiono strettamente interconnessi e reciprocamente dipendenti. In questa prospettiva, la Legge n. 132/2025 rappresenta un punto di equilibrio

dinamico, che prefigura una nuova legalità algoritmica sanitaria, in cui la decisione deve rimanere umana, motivata, trasparente e contestabile e l'algoritmo si pone come uno strumento sottoposto a regole specifiche. Specularmente, ne deriva un'immagine di "IA pubblica" trasparente nei presupposti, giustificata nei processi, contestabile negli esiti.

La ricerca condotta suggerisce che il diritto alla salute, nell'era algoritmica, si espande fino a includere come suo fondamentale corollario un nuovo "diritto alla trasparenza delle tecnologie" che lo mediano. L'accesso alle cure non può essere separato dall'accesso alla conoscenza dei processi che le generano. Per il giurista pubblicista ciò significa che la trasparenza non è più soltanto un dovere dell'amministrazione, ma anche un elemento costitutivo della stessa legalità sanitaria digitale.

L'efficacia della riforma si giocherà probabilmente su tre fronti.

Primo, l'attuazione. I provvedimenti secondari previsti dalla legge dovranno trasformare i principi in procedure verificabili. Senza standard chiari e pubblici, l'innovazione rischia di frammentarsi in sperimentazioni diversificate.

Secondo, la tutela giurisdizionale. L'ingresso dell'algoritmo nei procedimenti sanitari sposterà il fuoco del sindacato sulla qualità del processo tecnico-amministrativo di gestione della tecnologia. Ciò implica doveri di tracciabilità e motivazione idonei a consentire accesso, contraddittorio e verifica, inclusa la spendibilità processuale degli elementi essenziali del funzionamento del sistema, quando rilevanti ai fini del giudizio[83].

Terzo, la cultura istituzionale. La supervisione umana non può ridursi a convalida formale. Richiede alfabetizzazione tecnica e giuridica del personale sanitario e amministrativo, protocolli di uso clinico responsabile dei suggerimenti non vincolanti, capacità di interpretazione e di giustificazione delle scelte assistite dall'algoritmo[84].

Ogni trasformazione amministrativa porta con sé nuove regole, ma anche nuove immagini del potere. L'intelligenza artificiale ha aggiunto, in questa direzione, un ulteriore strato simbolico, quello della decisione pubblica integrata da

[83] La giurisprudenza del Consiglio di Stato – dalle c.d. sentenze gemelle n. 8472, 8473 e 8474 del 2019 (in ordine alla possibilità di utilizzare sistemi di IA anche nella formazione di decisioni che costituiscono espressione di un potere discrezionale), fino alle più recenti pronunce – ha già tracciato un percorso, affermando che l'amministrazione algoritmica deve restare conoscibile, motivata e contestabile. Ma l'applicazione di questi principi al campo sanitario, dove l'automazione incide su diritti fondamentali e dati sensibili, richiederà un salto di competenza e di metodo.

[84] Pienamente condivisibili sono le riflessioni di G. Montedoro, *Intelligenza artificiale e digitalizzazione fra Costituzione, amministrazione e giustizia*, in *www.giustizia-amministrativa.it*, 2024, secondo cui: «si dovrebbe tentare un esercizio di ri-scrittura dell'art. 97 Cost. portando il problema al livello costituzionale che gli spetta in modo che l'amministrazione possa orientare la sua azione nella direttiva del digitale al rispetto della dignità umana ed alla massimizzazione della trasparenza (evitando di squilibrare i poteri a favore dell'esecutivo con un eccesso di concentrazione del dominio sull'AI negli apparati dello Stato…)».

macchine capaci di apprendere e di elaborare. È in questo spazio che il diritto amministrativo deve riaffermare il proprio ruolo: dare forma a un'amministrazione capace di restare fedele ai principi della Costituzione, anche mentre si serve di strumenti che si specchiano in un universo cognitivo inedito.

L'orizzonte da seguire, soprattutto nel settore sanitario, non è quello di un'amministrazione più veloce, ma quello di un'organizzazione pubblica capace di unire il linguaggio della tecnica con quello dei diritti e di restituire al cittadino la fiducia che ogni sistema di cura deve garantire.

Silia Gardini - Abstract

La regolazione giuridica dell'intelligenza artificiale nell'amministrazione sanitaria. Riflessioni a margine della recentissima Legge n. 132/2025

Il lavoro analizza l'impatto dell'intelligenza artificiale sull'amministrazione sanitaria, mostrando come l'innovazione algoritmica incida sulla struttura costituzionale del diritto alla salute e sulla configurazione della decisione pubblica in ambito clinico-assistenziale. La Legge n. 132/2025 è esaminata nella cornice europea costituita da GDPR, MDR/IVDR, AI Act ed EHDS, che delinea un modello di legalità fondato su trasparenza, controllo umano, qualità dei dati e presidio del rischio. La ricerca evidenzia che la riforma non si limita a introdurre nuovi strumenti tecnologici, ma riorganizza la legalità sanitaria: rafforza la responsabilità personale del decisore, impone tracciabilità istruttoria e mantiene la supervisione umana quale elemento strutturale delle decisioni assistite da sistemi algoritmici.

The Legal Framework for Artificial Intelligence in Healthcare Administration: Reflections Following Italy's New Law No. 132/2025

The paper examines the impact of artificial intelligence on healthcare administration, showing how algorithmic innovation affects the constitutional framework of the right to health and the configuration of public decision-making in clinical and care settings. Law No. 132/2025 is analysed within the European framework shaped by the GDPR, MDR/IVDR, the AI Act and the EHDS, which outlines a model of legality grounded in transparency, human oversight, data quality and risk governance. The study demonstrates that the reform does not merely introduce new technological tools, but reorganises the legal architecture of healthcare administration: it reinforces the personal accountability of decision-makers, requires full procedural traceability, and maintains human supervision as a structural element of decisions supported by algorithmic systems.