GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

1. Le basi giuridiche del trattamento

Il trattamento di dati sulla salute da parte di soggetti che perseguono compiti di interesse pubblico deve necessariamente fondarsi sul diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. g) del Regolamento; *cfr*. sul punto sentenza della Corte Costituzionale n. 20 del 2019).

Tale disposizione ha trovato attuazione nell'art. 2-*sexies* del Codice, in base al quale i trattamenti delle particolari categorie di dati tra cui rilevano quelli sulla salute sono ammessi solo qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

L'elaborazione di dati sulla salute attraverso tecniche di IA richiama i concetti di profilazione e di decisioni sulla base di processi automatizzati con riferimento ai quali si rappresenta che, nell'ambito dei trattamenti svolti per motivi di interesse pubblico, l'uso di tali strumenti è consentito solo se espressamente previsto dal diritto degli Stati membri, nel rispetto di misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati (considerando 71 e art. 22, par. 4, del Regolamento).

Pertanto, in base al combinato disposto delle disposizioni sopra richiamate, operata una preliminare valutazione in ordine alla necessità di tali trattamenti[1], è necessario che gli stessi siano previsti da uno specifico quadro normativo avente le caratteristiche sopra richiamate.

A tale riguardo, si ricorda che in base all'art. 36, par. 4 del Regolamento, gli Stati membri consultano l'Autorità di controllo durante l'elaborazione di un atto legislativo o di misura regolamentare che prevede il trattamento di dati personali. Ciò, anche la fine di supportare gli stessi nella predisposizione di una base giuridica del trattamento chiara e precisa e prevedibile per le persone che vi sono sottoposte, in conformità alla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo (considerando 41 del Regolamento).

[1] cfr. EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 aprile 2017.

In tale contesto, si segnala come, in relazione all'utilizzo di strumenti di IA in altri settori, che tra l'altro non prevedono il trattamento di dati sulla salute, il legislatore, conformemente al quadro normativo sopra evidenziato, abbia allo stato già previsto la predisposizione di specifiche disposizioni volte a disciplinare tali trattamenti[2].

Sul punto, si evidenzia che la proposta di Regolamento del Parlamento europeo e del Consiglio, il cui testo non è ancora consolidato, che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale del 21 aprile 2021) e modifica alcuni atti legislativi dell'Unione, e le successive proposte emendative (posizione negoziale del Parlamento UE del 14 giugno 2023), **individua tra i sistemi di IA ad alto rischio quelli che incidono -tra l'altro- sulla salute**, sul diritto alle cure e sulla fruizione di servizi sanitari, di assistenza medica, nonché sui sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza, auspicando che siano stabilite norme legislative comuni per tutti i sistemi di IA ad alto rischio[3].

2. I principi di *accountability* e di *privacy by design* e *by default*

Il titolare del trattamento deve conformarsi ed essere in grado di comprovare il rispetto dei principi e degli adempienti previsti dal Regolamento e di aver effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione e per impostazione predefinita (artt. 5, par. 2, 24 e 25, par. 1, del Regolamento).

Il rinnovato quadro normativo in materia di protezione dei dati personali richiede, infatti, una preliminare e ponderata valutazione di tutte le scelte connesse ai trattamenti di dati personali, dimostrabile sul piano logico attraverso specifiche motivazioni, volte all'individuazione di misure necessarie e proporzionate rispetto alla concreta efficacia del principio di volta in volta tutelato.

In base al principio della "*protezione dei dati fin dalla progettazione*" (art. 25, par. 1, del Regolamento), nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario devono essere adottate misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e integrate nel trattamento le garanzie necessarie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati.

---

[2] cfr. parere all'Agenzia delle entrate del 30 luglio 2022, doc. *web* n. 9808839; disegno di legge Delega al Governo recante per la riforma fiscale (A.C. 1038-A), nel quale si rinviene la disposizione in materia di semplificazione del procedimento accertativo, anche mediante l'utilizzo delle tecnologie digitali e l'impiego di sistemi di intelligenza artificiale (AS 797). Cfr. legge del 9 agosto 2023, n. 111 (artt. 3, 4 e 17).

[3] Considerando 13 della proposta di Regolamento (in corso in approvazione) versione aprile 2021; cfr. anche il parere congiunto del Comitato europeo per la protezione dei dati e il Garante europeo, n. 5/2021 del 18 giugno 2021 sulla predetta proposta, che in particolare raccomanda che tali trattamenti si fondino su adeguate e solide condizioni di liceità; posizione negoziale del Parlamento UE del 14 giugno 2023, cfr., in particolare, emendamenti all'allegato III.

Tali misure, volte ad assicurare l'effettiva applicazione dei principi in materia di protezione dei dati personali, devono garantire -per impostazione predefinita- la proporzionalità del trattamento rispetto all'interesse pubblico perseguito, ponendosi l'obiettivo di ottenere un reale effetto di tutela[4].

Analogamente a quanto già avvenuto con riferimento ad altri sistemi informativi sanitari nazionali, tali profili possono essere efficacemente individuati nelle disposizioni di attuazione della base giuridica del trattamento (es. piattaforma nazionale sul "*Digital Green Certificate (DGC)*"; Sistema Tessera Sanitaria; Fascicolo sanitario elettronico -FSE; Ecosistema dati sanitari - EDS).

In merito a tali profili recentemente **nell'ambito dei lavori del G7 delle autorità per la protezione dei dati** è stata evidenziata la necessità di costruire un sistema virtuoso secondo cui i principi della protezione dati, a partire dalla "*privacy by design*" e dalla valutazione d'impatto, dovrebbero essere integrati nella progettazione e nel funzionamento delle tecnologie di IA generativa. In particolare, le autorità auspicano un uso virtuoso dell'IA da parte delle autorità pubbliche che tenga conto dei valori e dei principi dello Stato di diritto e del governo democratico.

3. Ruoli

Nell'ambito delle operazioni di trattamento dei dati personali occorre poi individuare correttamente i ruoli di titolare (artt. 4, n. 7 e 24) e, se del caso, di responsabile (artt. 4, n. 8 e 28 del Regolamento).

Il titolare è il soggetto sul quale ricadono le decisioni di fondo relativamente alle finalità e ai mezzi del trattamento dei dati personali, nonché la responsabilità generale (cd. "*accountability*") sui trattamenti posti in essere dallo stesso o da altri "*per* [suo] *conto*", in qualità di responsabili ai sensi dell'art. 28 del Regolamento.

L'attribuzione dei ruoli deve corrispondere alle attività che il soggetto svolge in concreto alla luce dei compiti istituzionalmente demandati allo stesso, in conformità al quadro giuridico di settore.

Ai fini dell'attribuzione della titolarità di un trattamento, anche in base al principio di legalità, è in primo luogo necessario valutare la sussistenza di una idonea base giuridica che conferisca a tale soggetto il compito di svolgere il trattamento, non potendosi questi qualificare automaticamente come titolare sulla base di un mero presupposto fattuale, come, ad esempio, la realizzazione di un progetto che prevede il trattamento dei dati personali.

È necessaria, pertanto, anche in un'ottica di *governance* dei dati, una visione complessiva della titolarità del trattamento che tenga conto che un sistema

[4] cfr. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019 by the EDPB*.

nazionale di IA in ambito sanitario potrebbe essere acceduto per differenti finalità da parte di una molteplicità di soggetti sulla base di diversi presupposti di liceità.

Sotto altro profilo, ferma restando la necessità che il trattamento nel settore in esame sia normativamente attribuito al titolare, ai fini della individuazione in concreto dei ruoli del trattamento che si intendono svolgere, è indispensabile esaminare -sul piano sostanziale- le competenze attribuite ai diversi soggetti e, conseguentemente, le attività in concreto svolte dagli stessi[5].

Il ruolo del responsabile del trattamento è, invece, caratterizzato dallo svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare uno o più soggetti particolarmente qualificati allo svolgimento delle stesse - in termini di conoscenze specialistiche, di affidabilità, risorse e sicurezza del trattamento (cfr. cons. 81 del Regolamento)- delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare[6].

Nulla osta pertanto a che, nel trattamento di dati personali connesso allo svolgimento dei propri compiti istituzionali, ciascun titolare, anche pubblico, possa avvalersi del contributo di soggetti esterni, affidando a questi determinate attività che restano nella sfera della titolarità dell'amministrazione stessa e che non comportano decisioni di fondo sulle finalità e sui mezzi del trattamento. In questo caso, è necessario che l'amministrazione – in qualità di titolare del trattamento – designi il soggetto esterno, preposto allo svolgimento di determinate attività che comportano il trattamento di dati personali, come "*responsabile del trattamento*" ai sensi dell'art. 28 del Regolamento.

In caso contrario, in mancanza di tale designazione, la messa a disposizione di dati personali a soggetti esterni si configura come una comunicazione di dati personali da effettuarsi conformemente al quadro normativo sopra richiamato (artt. 9 del Regolamento e 2-*sexies* del Codice).

In ogni caso, le persone fisiche che, anche presso il soggetto esterno materialmente trattano i dati personali, devono essere autorizzate al trattamento e opportunamente istruite ai sensi degli artt. 29 del Regolamento e 2-*quaterdecies* del Codice.

[5] cfr., a titolo esemplificativo, provvedimenti del 16 febbraio 2006, punto 6, doc. *web* n. 1242592; 4 ottobre 2011, punto 5, doc. *web* 1850581; del 19 luglio 2018, doc. *web* 9039945; 14 gennaio 2021, doc. *web* n. 9542136, doc. *web* n. 9542113; 7 luglio 2022, doc. web 9809998; del 20 ottobre 2022, n. 342, doc. web n. 9832507; 10 novembre 2022, n. 368, doc. *web* n. 9843319, Linee guida per il trattamento di dati dei dipendenti privati del 23 novembre 2006, doc. *web* n. 1364099.

[6] cfr. Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0, Adottate il 7 luglio 2021.

4. I principi di conoscibilità, non esclusività e non discriminazione algoritmica

Sulla base delle disposizioni del Regolamento e alla luce della recente giurisprudenza del Consiglio di Stato[7], è possibile enucleare i **tre principi cardine** che devono governare l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico:

1. il principio di conoscibilità, in base al quale l'interessato ha il diritto di conoscere l'esistenza di processi decisionali basati su trattamenti automatizzati e, in tal caso, di ricevere informazioni significative sulla logica utilizzata, sì da poterla comprendere;

2. il principio di non esclusività della decisione algoritmica, secondo cui deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica (c.d. *human in the loop*);

3. il principio di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi sistemi di IA affidabili che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l'efficacia anche alla luce della rapida evoluzione delle tecnologie impiegate, delle procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate. Ciò, anche al fine di garantire, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, visti i potenziali effetti discriminatori che un trattamento inesatto di dati sullo stato di salute può determinare nei confronti di persone fisiche (cfr. considerando n. 71 del Regolamento).

5. Valutazione d'impatto sulla protezione dei dati (VIP)

Il Regolamento introduce poi l'obbligo per i titolari di svolgere una preventiva valutazione di impatto sul trattamento che "*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*" (art. 35), e di consultare l´Autorità di controllo qualora le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento sui diritti e le libertà degli interessati non siano ritenute sufficienti, ovvero quando il rischio residuale per i diritti e le libertà degli interessati resti elevato (art. 36).

A tale riguardo, si segnalano le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "*possa presentare un rischio elevato*"[8]. In tale ambito il Gruppo articolo 29 indica -in particolare- quando una valutazione di impatto sia obbligatoria, chi debba condurla

[7] cfr., in particolare, sentenze VI sez., nn. 2270/2019, 8472/2019, 8473/2019, 8474/2019, 881/2020, e 1206/2021.
[8] WP248rev.01, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

(il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di considerarla non solo un adempimento statico e *una tantum* ma come un processo soggetto a revisione continua.

La previsione di un sistema centralizzato a livello nazionale attraverso il quale **realizzare servizi sanitari con strumenti di IA, determinando un trattamento sistematico, su larga scala, di particolari categorie di dati personali di cui all'art. 9 del Regolamento di soggetti vulnerabili**, attraverso l'uso di nuove tecnologie e presentando un rischio elevato per i diritti e le libertà degli interessati, deve essere **preceduta da una valutazione di impatto** ai sensi dell'art. 35 del Regolamento.

Tali trattamenti rientrano infatti, senza dubbio, tra quelli ad "*alto rischio*" per i quali è necessaria una preventiva valutazione di impatto, strumento fondamentale per l'individuazione delle misure idonee a tutelare i diritti e le libertà fondamentali degli interessati e a garantire il rispetto dei principi generali del Regolamento, nonché per consentire l'analisi della proporzionalità dei trattamenti effettuati.

L'adeguatezza di tali misure, da assicurare in modo omogeneo e uniforme sull'intero territorio nazionale, è valutabile solo alla luce della preventiva valutazione di impatto sui trattamenti effettuati attraverso sistemi nazionali di IA che vedono coinvolti molteplici soggetti.

L'assenza di tale valutazione d'impatto svolta a livello nazionale non consentirebbe di effettuare un esame complessivo e preventivo sull'adeguatezza e sulla proporzionalità delle misure che si intendono implementare. Circostanza questa non ammissibile con riguardo ad un sistema informativo destinato a trattare ed elaborare i dati sanitari di tutti i soggetti assistiti nel territorio nazionale per i quali è necessario che vengano predisposte misure tecniche e organizzative omogenee atte ad assicurare un'effettiva e uniforme tutela dei diritti e delle libertà fondamentali degli interessati correlati al trattamento dei loro dati personali[9].

La valutazione d'impatto dovrebbe inoltre tener conto dei rischi propri di una banca dati contenente le informazioni sanitarie di tutta la popolazione assistita sul territorio nazionale, quali ad esempio quelli relativi alla perdita dei requisiti di qualità dei dati (es. mancato o errato allineamento e aggiornamento), alla revoca del consenso, ove lo stesso costituisca la base giuridica del trattamento originario, alla re-identificazione dell'interessato in considerazione delle possibili interconnessioni con molteplici sistemi informativi e banche dati e all'utilizzo dei dati per finalità non compatibili.

[9] sul punto, si richiama anche il recente intervento della Corte Costituzionale, cfr. sentenza n. 164 del 2022, punto 10.

6. Qualità dei dati

Il titolare del trattamento deve garantire che i dati siano esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati non corretti rispetto alle finalità per le quali sono trattati (principio di «*esattezza*», di cui all'art. 5, par. 1, lett. d), del Regolamento).

La realizzazione di un sistema nazionale di IA destinato ad elaborare i dati sanitari di tutta la popolazione assistita impone il rigoroso rispetto di specifiche misure volte a garantire in concreto l'esattezza e l'aggiornamento dei dati e soprattutto la tutela degli interessi e dei diritti fondamentali degli interessati.

Al riguardo, il **Consiglio superiore di sanità - già nel 2021** - ha evidenziato come uno sviluppo incontrollato e non governato dell'IA non sia scevro da potenziali rischi, derivanti, ad esempio, dall'uso di sistemi privi di una rigorosa validazione scientifica, dalla mancanza di controllo sui dati processati, senza dimenticare le aspettative illusorie e fuorvianti per professionisti sanitari e pazienti derivanti da un utilizzo improprio dei sistemi di IA[10].

In ordine alla realizzazione di sistemi nazionali di IA in ambito sanitario, i requisiti di esattezza, correttezza e aggiornamento del dato appaiono di particolare rilievo considerati i rischi di elaborazione di dati raccolti per finalità di cura che potrebbero essere stati, successivamente alla raccolta, modificati, rettificati o integrati dal personale sanitario che nel tempo è intervenuto nel percorso di cura dell'interessato. **Il dato non aggiornato o inesatto influenzerebbe inoltre anche l'efficacia e la correttezza dei servizi che i suddetti sistemi di IA, che si basano infatti sulla rielaborazione di tali dati, intendono realizzare.**

In tale contesto, se si considera che la realizzazione di un sistema di IA per l'erogazione di servizi digitali è volto a supportare, in modo innovativo, il servizio sanitario nazionale, eventualmente anche allo scopo di farne discendere idonei interventi da parte dei decisori pubblici, assume particolare rilievo la circostanza che ogni qualità riferita al singolo interessato, nonché ogni diversa categoria di interessati sia rappresentata allo stesso modo in cui essa è presente nella popolazione.

Pertanto la VIP dovrebbe tener conto anche degli specifici rischi (quali ad esempio la discriminazione) legati sia all'elaborazione dei dati attraverso logiche algoritmiche che integrano espressioni matematiche, volte a trovare associazioni, identificare tendenze ed individuare regolarità all'interno di un insieme di dati, alla base dei comportamenti umani, sia a quelli connessi alla profilazione finalizzata all'adozione di decisioni automatizzate che possano incidere sull'aspetto sanitario individuale.

[10] cfr., "*I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*" Consiglio superiore di sanità, Sez. V, 9 novembre 2021.

7. Integrità e riservatezza

Ai sensi del Regolamento, i dati personali devono essere "*trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)"* (art. 5, par. 1, lett. f), del Regolamento).

Al riguardo, occorre evidenziare che, in ossequio a quanto previsto dai richiamati artt. 5, 25 e 35 del Regolamento, i rischi per i diritti e le libertà degli interessati derivanti dai trattamenti in esame e, di conseguenza, le misure da adottare per gestirli, escludendoli o mitigandoli, devono essere valutati in concreto, vale a dire tenendo in considerazione le caratteristiche delle banche dati di volta in volta utilizzate e i modelli di analisi impiegati (es. quelli di analisi deterministica o stocastica, oppure una combinazione di essi).

Ciò, tenuto conto anche del fatto che, tra i principali rischi connessi all'utilizzo di modelli di analisi deterministica e, soprattutto, stocastica con tecniche di *machine learning*, vi sono quelli relativi a potenziali opacità nella fase di sviluppo dell'algoritmo, errori e distorsioni di diversa natura (cc.dd. *bias*), che possono verificarsi nell'elaborazione o nell'utilizzo di tali modelli ovvero correlati alla qualità e/o al volume dei dati di volta in volta utilizzati e che, se non correttamente identificati e mitigati, possono produrre conseguenze pregiudizievoli o risultati discriminatori per gli interessati.

A tal fine, è necessario che, nella descrizione dei trattamenti, siano puntualmente **indicate le logiche algoritmiche utilizzate al fine di "generare" i dati e i servizi attraverso i suddetti sistemi di IA**, le metriche utilizzate per addestrare il modello e valutare la qualità del modello di analisi adottato, le verifiche svolte per rilevare la presenza di eventuali *bias*, le misure correttive eventualmente adottate, le misure idonee a verificare, anche a posteriori, le operazioni eseguite da ciascun soggetto autorizzato e i rischi insiti nelle analisi deterministiche e stocastiche.

Ai sensi del richiamato quadro giuridico, pertanto, la base giuridica del trattamento dei dati effettuati attraverso sistemi nazionali di IA deve indicare misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, tra le quali devono essere indicate (anche in un allegato documento tecnico) quelle **misure adeguate a mitigare i rischi correlati all'uso di tecniche di IA su dati sanitari, trattati su larga scala, di soggetti vulnerabili** che possono portare all'adozione di decisioni automatizzate.

8. Correttezza e trasparenza

In linea con i documenti internazionali[11] e la giurisprudenza amministrativa[12], la trasparenza e la correttezza nei processi decisionali fondati su trattamenti automatizzati costituiscono uno dei pilastri fondamentali da porre alla base dello sviluppo e utilizzo di sistemi di IA alla luce, nell'ambito dell'azione amministrativa, dei correlati rischi, anche discriminatori, che possono derivare dall'uso di tali strumenti.

Nei richiamati documenti internazionali si fa riferimento, per una *trustworthy* IA, alla necessità di assicurare una quanto più ampia "consapevolezza" nelle collettività di riferimento (nel caso di specie la totalità degli assistiti del Sistema Sanitario Nazionale) in relazione all'impiego dei sistemi di intelligenza artificiale e comprensione in relazione al loro funzionamento[13], garantendo, inoltre, la partecipazione dei differenti *stakeholder* in relazione al ciclo di vita dei sistemi di intelligenza artificiale per uno sviluppo sostenibile e una *governance* rispettosa dei diritti degli interessati.

In termini pratici sono svariate le misure e gli adempimenti che nella predisposizione dei sistemi di IA in sanità devono essere implementate, tra le quali quelle volte a:

assicurare che la base giuridica del trattamento sia chiara, prevedibile e resa conoscibile agli interessati anche attraverso specifiche campagne di informazione[14];

consultare gli *stakeholder* e gli interessati nell'ambito dello svolgimento della valutazione d'impatto (art. 35, par. 9, del Regolamento);

pubblicare, anche solo per estratto, la valutazione d'impatto[15];

predisporre le informazioni da rendere agli interessati, con gli elementi di cui agli artt. 13 e 14 del Regolamento in termini chiari, concisi e comprensibili;

informare non solo in merito agli elementi di cui ai richiamati artt. 13 e 14 del Regolamento ma anche evidenziando:

[11] OECD *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449) adottata il 22 maggio 2019, ed in particolare tenere conto dell'approccio antropocentrico in ogni fase del ciclo vitale (*lifecycle*) dei sistemi di intelligenza artificiale e dei principi di correttezza (fairness) e non discriminazione; dei principi di trasparenza (*transparency*) e di comprensibilità (*explainability*); dei principi di robustezza (*robustness*) e (*ciber*)sicurezza informatica (security); ancora, del principio di responsabilizzazione (accountability) di quanti, a vario titolo, svolgono un ruolo attivo nella fase del design, dello sviluppo e dell'impiego dei sistemi di intelligenza artificiale; UNESCO Recommendation on the Ethics of Artificial Intelligence, adottata il 23 novembre 2021.
[12] Sent. Consiglio di Stato, VI sez., nn. 2270/2019, 8472/2019, 8473/2019, 8474/2019, 881/2020, e 1206/2021.
[13] cfr., in particolare, punti 44 e 47 del UNESCO *Recommendation*, citata.
[14] cfr. parere sul FSE dell'8 giugno 2023, doc. *web* n. 9900433.
[15] Provvedimento del 30 luglio 2022, doc. *web* n. 9808839).

se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, nell'ambito dei servizi sanitari, rappresentando le logiche e le caratteristiche di elaborazione dei dati;

se sussistono eventuali obblighi e responsabilità dei professionisti sanitari, a cui si rivolge l'interessato, ad utilizzare servizi sanitari basati sull'IA;

i vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo di tali nuove tecnologie;

assicurare modalità efficaci di esercizio dei diritti degli interessati previsti dal Regolamento e dalle specifiche discipline di settore, tenuto anche conto dei diversi ruoli rivestiti dai soggetti coinvolti nel trattamento;

nel caso di perseguimento di finalità di cura, garantire che i servizi di elaborazione dei dati basati su sistemi di IA, siano realizzati solo a seguito di una espressa richiesta di attivazione del professionista sanitario e non in modo automatico;

regolamentare i profili di responsabilità professionale connessi alla scelta del professionista sanitario di affidarsi o meno ai servizi di elaborazione dei dati sanitari dei propri pazienti effettuati sulla base di sistemi di IA.

9. Supervisione umana

Nel citato parere congiunto del Garante europeo e del Comitato europeo per la protezione dei dati (EDPS/EDPB)si precisa che generare contenuti, fare previsioni o adottare decisioni in maniera automatica, come fanno i sistemi di IA, per mezzo di tecniche di apprendimento automatico o regole di inferenza logica e probabilistica è cosa ben diversa rispetto alle modalità con cui queste stesse attività sono svolte dagli esseri umani attraverso il ragionamento creativo o teorico, nella piena consapevolezza della responsabilità e delle relative conseguenze.

Se da una parte, quindi, l'IA amplia significativamente la quantità di previsioni che si possono fare in molti ambiti – a cominciare dalle correlazioni tra i dati-, dall'altra, affidare solo alle macchine il compito di prendere decisioni sulla base di dati, elaborati mediante sistemi di IA, comporta rischi per i diritti e le libertà delle persone.

A tale riguardo, il Comitato, il Garante europeo e quello italiano[16] hanno sottolineato la centralità del concetto di supervisione umana contenuto nella proposta di Regolamento, evidenziando che l'effettivo coinvolgimento degli esseri umani dovrebbe fondarsi su una supervisione altamente qualificata e sulla liceità del

[16] cfr. contributi sul tema pubblicati in https://www.gpdp.it/temi/intelligenza-artificiale.

trattamento, al fine di assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato.

Ciò, in particolare, nella fase di addestramento degli algoritmi, in quanto sulla base di questo "addestramento", l'IA è in grado di fare delle previsioni, con diversi gradi di probabilità. La correttezza nella predizione della IA, soprattutto qualora correlata al rischio di sviluppare malattie, è proporzionale al numero, alla qualità e all'accuratezza dei dati inseriti e alle esperienze immagazzinate su un determinato tema. Tuttavia, le predizioni possono essere "sbagliate" per l'imprecisione dei dati forniti, per l'addestramento degli algoritmi (ad es. informazioni inesatte non aggiornate) o per l'uso di assunzioni non fondate o non pertinenti.

Al fine di fornire una concreta evidenza dei "rischi di discriminazione" che possono derivare da una selezione impropria, incompleta e non accurata dei dati utilizzati dai sistemi di IA, occorre evidenziare che negli Stati Uniti un sistema di IA utilizzato per stimare il rischio sanitario di oltre 200 milioni di americani tendeva ad assegnare un livello di rischio inferiore ai pazienti afroamericani a parità di condizioni di salute, con la conseguenza di negargli l'accesso a cure adeguate. I ricercatori che hanno svolto l'analisi del caso[17] hanno stabilito che la causa era da attribuire alla metrica utilizzata per stimare il rischio, basata sulla spesa sanitaria media individuale. In questo caso, quindi, l'appartenenza a un gruppo etnico non è una caratteristica utilizzata direttamente dall'algoritmo, ma influenza indirettamente il risultato in considerazione della struttura economica della società americana; ciò rende evidente come sia indispensabile nell'addestramento e nell'utilizzo dell'algoritmo considerare la qualità dei dati che è spesso fortemente condizionata anche dalle caratteristiche socio-economiche della popolazione di riferimento.

È necessario, dunque, che in tale fase di addestramento degli algoritmi sia mantenuto il ruolo centrale dell'uomo e, nel caso di specie, del professionista sanitario e non rimettere *in toto* la decisione alle macchine.

Tale processo richiede di essere accuratamente descritto nella valutazione d'impatto al fine di ridurre i rischi per i diritti e le libertà degli interessati, con particolare riferimento al rischio di discriminazione, che potrebbe verificarsi relativamente all'accesso alle cure, alla quota di partecipazione al costo in carico all'assistito e addirittura all'appropriatezza dei percorsi diagnostici e terapeutici. Nel settore in esame, infatti, i rischi di discriminazione algoritmica possono incidere sull'equità e sull'inclusività alle cure, potendo potenzialmente aumentare il divario e le disuguaglianze socio sanitarie.

[17] https://pubmed.ncbi.nlm.nih.gov/31649194/ *Dissecting racial bias in an algorithm used to manage the health of populations*.

10. Ulteriori profili rispetto alla disciplina sulla protezione dei dati personali connessi alla dignità e all'identità personale

Il dibattito internazionale richiama con sempre maggiore attenzione la necessità che lo sviluppo dell'IA sia accompagnato da una costante attenzione ai profili etici del trattamento dei dati personali. Ciò, si rende ancor più necessario se attraverso gli strumenti di IA si intendono trattare informazioni sulla salute di un'intera popolazione con l'obiettivo di fornire servizi ai professionisti sanitari che prenderanno in cura l'interessato[18].

Tenuto quindi conto che l'etica ha già influenzato la genesi del quadro normativo nazionale e comunitario a tutela dei diritti e delle libertà fondamentali degli interessati, così come adesso sta contribuendo alla formazione di quello specificamente dedicato all'IA, ad essa deve attribuirsi una puntuale funzione interpretativa che porti ad escludere scelte che, ancorché apparentemente lecite e materialmente possibili, dal punto di vista sostanziale possano produrre effetti discriminatori e lesivi della dignità umana e identità personale anche nei confronti di soggetti vulnerabili (minori, anziani, malati).

In tale quadro, in termini più pratici – per un atteggiamento eticamente corretto, sicuro e trasparente della tecnologia IA - sarebbe ad esempio opportuno preferire fornitori che sin da subito si preoccupano di svolgere una valutazione di impatto sulla protezione dei dati prima della commercializzazione dei propri prodotti (e fermo l'obbligo in capo al titolare del trattamento di svolgerne una specifica), nonché che abbiano eventualmente anche condotto una specifica valutazione di impatto per l'IA, sicura, trasparente e affidabile[19].

Si rappresenta inoltre che restano infatti fermi gli specifici obblighi deontologici cui è tenuto il professionista sanitario nell'elaborazione delle informazioni sulla salute del paziente, nella scelta del percorso terapeutico appropriato e proporzionato e nell'astensione dalle eventuali condizioni di conflitto di interessi che potrebbero ingenerarsi nel caso in cui, dall'utilizzo o dal mancato utilizzo dei servizi di IA da parte del professionista, lo stesso possa subire incentivi o conseguenze di tipo amministrativo.

La validazione degli algoritmi dovrebbe garantire che l'introduzione delle varie forme di IA migliori la qualità delle prestazioni del Servizio Sanitario Nazionale senza ripercussioni negative in termini sociali, deontologici, etici per l'interessato e sugli aspetti legati alla responsabilità professionale. Al riguardo, nell'ambito dei citati lavori dell'ultimo G7 delle autorità per la protezione dei dati e la privacy, il Garante italiano ha proposto che le Autorità, dei sette sistemi socio-economici più importanti

[18] cfr., in particolare, CNB – Cnbbvs intelligenza artificiale e medicina: aspetti etici del 29 maggio 2020; Gruppo di esperti ad alto livello sull'intelligenza artificiale https://digital strategy.ec.europa.eu/en/policies/expert-group-ai

[19] HLEGAI: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

al mondo, elaborino un modello etico distintivo per la governance dell'intelligenza artificiale.