UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

INNOVAZIONE TECNOLOGICA E TUTELA DEI DIRITTI

L'impiego degli Smart Assistant nella Sanità

Sofia Carrino

0351299

Anno accademico 2023/2024

Sommario

Abstract

L'espansione delle tecnologie digitali nella vita quotidiana ha portato, negli ultimi anni, a una vasta diffusione degli assistenti intelligenti, noti come *smart assistant*. Questi software, basati sul *machine learning*, ossia sistemi di apprendimento che utilizzano algoritmi di intelligenza artificiale, possono comprendere il linguaggio naturale umano e interagire con le persone di conseguenza. In questo contesto, l'attenzione particolare riservata agli assistenti vocali "intelligenti" deriva da una duplice ragione: lo stretto legame che il loro funzionamento ha inevitabilmente con i dati personali e il loro elevato grado di pervasività nella vita degli utenti. In particolare, preoccupazioni riguardanti l'ingente quantitativo di dati personali raccolti ed elaborati da questi dispositivi, e le relative perplessità, sono state sollevate con riferimento agli home speaker, collocati nell'ambiente domestico, luogo in cui si svolge la vita privata e familiare. Gli assistenti vocali, però, non sono solo questo. Gruppi di ricerca sparsi in tutto il mondo, spinti dalla possibilità di fornire supporti medico-curativi a determinate categorie di pazienti, che potrebbero beneficiare ampiamente di strumenti tecnologicamente avanzati, si apprestano a valutare e testare auspicabili interazioni positive che gli smart assistant possono determinare in contesti di sanità digitale. Lo sfruttamento dell'IA in campo sanitario ha subito un'evoluzione da un approccio ritenuto futuristico ad una fiorente realtà. Dal punto di vista giuridico, questi scenari innovativi, pur promettendo risultati straordinari in termini di supporto ai processi curativi, presentano notevoli criticità, specialmente in relazione alla disciplina in materia di protezione dei dati personali contenuta nel GDPR. Tecnologia e diritto interagiscono strettamente, influenzandosi reciprocamente. Il giurista è chiamato a un'attività creativa, volta a trovare regole applicative partendo da principi generali, in un contesto dove il legislatore può solo rincorrere le innovazioni tecnologiche con regole destinate a rapida obsolescenza.

Introduzione

Nel contesto contemporaneo, caratterizzato da una crescente digitalizzazione, l'emergere degli smart assistant ha segnato una svolta significativa nelle modalità di interazione tra l'uomo e la tecnologia. Questi assistenti intelligenti, basati su algoritmi di intelligenza artificiale e machine learning, sono progettati per comprendere il linguaggio naturale umano, rispondere a comandi vocali e svolgere una vasta gamma di attività.

L'applicazione degli smart assistant in ambito sanitario rappresenta una delle aree di maggiore interesse e potenzialità, offrendo soluzioni innovative per la gestione della salute personale e il supporto a pazienti con ridotta autonomia. Tuttavia, l'utilizzo di queste tecnologie solleva una serie di questioni giuridiche ed etiche, in particolare riguardo alla protezione dei dati personali e alla privacy degli utenti. Gli assistenti vocali raccolgono e trattano costantemente un'importante mole di dati personali, non solo degli utenti diretti, ma anche di chiunque si trovi nell'ambiente circostante, ampliando così le possibilità di raccolta e incrocio dei dati e la diffusione delle informazioni personali.

In questo contesto, il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea rappresenta un quadro normativo fondamentale per garantire la protezione dei dati personali e la privacy degli individui. Il GDPR stabilisce principi chiave come la liceità, correttezza, trasparenza, che devono essere rigorosamente rispettati nel trattamento dei dati personali raccolti dagli smart assistant. Tuttavia, l'applicazione di questi principi a scenari tecnologicamente avanzati pone sfide significative, in particolare per quanto riguarda la minimizzazione dei dati trattati, la limitazione della loro conservazione e la finalità del trattamento.

La presente tesina si propone di esplorare in dettaglio le implicazioni giuridiche dell'uso degli smart assistant, con un focus sul settore sanitario, analizzando i rischi associati alla raccolta e al trattamento dei dati personali, le misure di protezione della privacy consigliate dal Garante, e le prospettive future in termini di regolamentazione e sviluppo etico dell'intelligenza artificiale. Attraverso un'analisi critica e approfondita, si intende comprendere le complesse dinamiche tra innovazione tecnologica e tutela dei diritti fondamentali degli individui in un'era digitale sempre più pervasiva.

Capitolo 1
General Data Protection Regulation

Il regolamento UE 679/2016, noto come General Data Protection Regulation (GDPR), è stato il primo regolamento ad affrontare in maniera ampia, sistemica e moderna il corretto trattamento e la libera circolazione dei dati personali a livello europeo [1]. Il GDPR, entrato in vigore nel maggio 2018, è un regolamento comunitario, ossia una norma immediatamente applicabile su tutto il territorio dell'Unione Europea. La normativa che lo ha preceduto era il d.lgs. 196/2003, noto come Codice della Privacy, che non è stato completamente abrogato ma armonizzato con il GDPR tramite il d.lgs. 101/2018. In particolare, sono stati abrogati gli articoli del Codice della Privacy riguardanti questioni disciplinate dal nuovo GDPR, e quindi non più necessari, mentre sono rimaste alcune norme che l'Unione Europea aveva lasciato alla discrezionalità dei singoli stati membri.

Le principali figure coinvolte nel trattamento dei dati sono:

- L'interessato ovvero la persona fisica di cui si trattano i dati;
- Il titolare del trattamento è l'entità (persona fisica o giuridica, pubblica o privata) che determina i mezzi e le finalità del trattamento;
- Il responsabile del trattamento è colui che tratta i dati per conto del titolare, esclusivamente per la finalità da quest'ultimo indicata (ad esempio, un'agenzia di comunicazione che si occupa di marketing per un cliente);
- Il contitolare del trattamento è colui che è titolare del trattamento congiuntamente ad un altro titolare, e sono quindi due i soggetti a determinare mezzi e finalità del trattamento (ad esempio, due società che operano nello stesso edificio e condividono l'impianto di videosorveglianza sono entrambe ugualmente legittimate ad utilizzare le immagini riprese);
- L'incaricato del trattamento è colui che agisce sotto l'autorità del titolare o del responsabile del trattamento (ad esempio, un dipendente dell'ufficio risorse umane che tratta i dati di tutti i dipendenti dell'azienda sotto l'autorità dell'azienda in questione);
- Un'altra figura è quella del responsabile della protezione dei dati (RDP/DPO), responsabile del monitoraggio della conformità dell'organizzazione in cui opera. Fornisce consigli e linee guida relativi agli obblighi di protezione dei dati e svolge anche un ruolo di tramite con il Garante. La sua designazione è obbligatoria solo in caso di trattamenti più delicati, indicati nell'art. 37.

I principi generali che governano il trattamento dei personali sono elencati nell'art. 5 del GDPR:

- Liceità: il trattamento deve rispettare le norme che lo riguardano e disciplinano;
- Correttezza: i dati devono essere esatti ed aggiornati;

- Trasparenza: le informazioni relative al trattamento dei dati devono essere facilmente accessibili e comprensibili;
- Finalità: la finalità del trattamento deve essere determinata, esplicita e legittima (principio di limitazione delle finalità);
- Necessità: i dati trattati devono essere solamente quelli strettamente necessari rispetto alla finalità del trattamento (principio di minimizzazione dei dati);
- Proporzionalità: il trattamento deve contemperare i diritti di tutti i soggetti coinvolti, senza sacrificare il diritto di una parte rispetto al diritto di altri;

Il GDPR definisce un trattamento come lecito quando esiste una delle basi giuridiche indicate dall'art. 6. Queste sono:

- Consenso: il dato può essere trattato perché l'interessato ha espresso il consenso a trattarlo per una o più specifiche finalità indicate (ad esempio, il titolare del dato ha flaggato sulla casella di posta elettronica autorizzando al trattamento dei dati per ricevere la newsletter, il catalogo prodotti, le informative promozionali, per fare statistiche). Il consenso deve essere libero, specifico, informato e inequivocabile. Non è ammesso il consenso tacito o presunto (ad esempio, caselle preselezionate). L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento ma la revoca non pregiudica la liceità del trattamento basata sul consenso precedente alla revoca;
- Esecuzione del contratto: il trattamento è lecito quando è necessario all'esecuzione di un contratto di cui l'interessato è parte (ad esempio, l'indirizzo di un cliente è necessario al venditore per spedire un prodotto acquistato online);
- Obbligo di legge: il trattamento è lecito quando è necessario per adempiere a un obbligo di legge al quale è soggetto il titolare del trattamento (ad esempio, i dati fiscali necessari per emettere le fatture);
- Interesse vitale: il trattamento è lecito se avviene per salvaguardare gli interessi vitali dell'interessato (ad esempio, dati sanitari necessari per individuare la terapia corretta);
- Interesse pubblico: il trattamento è lecito quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui il titolare è investito (ad esempio, le scuole pubbliche trattano i dati degli studenti per fornire istruzione pubblica);
- Legittimo interesse: il trattamento è lecito quando è necessario per il perseguimento di un legittimo interesse del titolare del trattamento o di terzi (ad esempio, videosorveglianza di un luogo pubblico a fini di sicurezza, bilanciando comunque il legittimo interesse del titolare e dell'interessato affinché non siano lesi i suoi diritti e libertà fondamentali).

Citando l'art. 7, "*Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali"*. L'informativa, descritta nell'art. 12, è una comunicazione (una mail, una pagina web, un popup, anche una comunicazione verbale) rivolta all'interessato allo scopo di informarlo sulle finalità e modalità dei trattamenti da parte del titolare. Se il titolare fornisce l'informativa e, maggiormente, se lo fa per iscritto, riesce a provare che assicura trasparenza e correttezza nei trattamenti fin dalla progettazione del singolo trattamento. L'informativa ha anche lo scopo di permettere che l'interessato possa rendere un valido consenso, se questo è richiesto come base giuridica del trattamento. In questo caso, l'informativa non è solo dovuta in base al principio di trasparenza e correttezza ma è anche una condizione di legittimità del trattamento, senza la quale quel trattamento sarebbe illecito e quindi sanzionabile. L'informativa è dovuta ogni qualvolta ci sia un trattamento di dati ed è un obbligo che va adempiuto prima o al più tardi nel momento in cui avvia la raccolta dei dati. Se il dato viene trattato su una base giuridica diversa dal consenso, l'informativa è quindi ugualmente dovuta ma non è richiesta la controfirma per manifestare il consenso. L'informativa non è invece necessaria nel caso in cui il trattamento riguardi dati anonimi o di enti o persone giuridiche, in quanto non sono oggetto di tutela da parte del GDPR, o se i dati vengono trattati solo a scopo personale. Il contenuto dell'informativa, indicato negli art. 13 e 14, deve riportare la categoria di dati trattati, la finalità, la base giuridica, la natura del trattamento e le conseguenze nel caso un interessato non voglia rilasciare i propri dati. L'informativa deve essere chiara, comprensibile e facilmente accessibile per l'interessato.

Il GDPR indica i diritti degli interessati in relazione ai loro dati. Distinguiamo i seguenti:

- Diritto di accesso (art. 15): l'interessato ha diritto a sapere quali dati personali sono oggetto di trattamento e ad avere l'accesso ad essi;
- Diritto di rettifica (art. 16): se i dati dell'interessato sono errati, egli ha diritto di ottenere dal titolare la rettifica dei dati inesatti;
- Diritto di cancellazione o diritto all'oblio (art. 17): esistono una serie di ipotesi per cui, se l'interessato lo chiede, i suoi dati vanno cancellati. Se i dati sono stati resi pubblici, bisogna informare anche gli altri titolari che li trattano affinché li cancellino;
- Diritto alla limitazione del trattamento (art. 18): consiste nella riduzione dell'ampiezza del trattamento dei dati in alcune circostanze (ad esempio, nel tempo che intercorre tra la contestazione della correttezza dei dati e la loro correzione, l'unico trattamento possibile è la conservazione);
- Diritto alla portabilità dei dati (art. 20): il titolare deve garantire di poter trasferire i dati indicati dall'interessato ad un altro titolare, quando tecnicamente possibile.

Qualora l'interessato faccia valere uno dei diritti descritti, il titolare deve fornire riscontro entro un mese dalla richiesta, anche in caso di diniego, in forma scritta e in modo chiaro, trasparente ed accessibile. Il titolare del trattamento deve infatti agevolare l'esercizio dei diritti da parte dell'interessato con ogni misura tecnica e organizzativa a sua disposizione utile allo scopo. L'esercizio dei diritti è tendenzialmente gratuito per l'interessato, anche se possono esserci delle eccezioni.

Tra le novità introdotte dal GDPR, il principio di accountability, ossia la responsabilizzazione del titolare. Cambiando prospettiva rispetto al vecchio Codice della Privacy, non si comunica più al titolare tutto ciò che deve fare per essere conforme alla normativa, ma è lui che deve adottare comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. In altri termini, il titolare deve decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e anche alla luce di alcuni criteri specifici indicati nel regolamento. Uno di questi è il Data Protection by default/design, ossia il titolare deve configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto in cui si colloca il trattamento stesso. Un altro approccio, basato sul rischio, prevede che il titolare analizzi gli impatti negativi dell'eventuale perdita o diffusione del dato sulla libertà e i diritti degli interessati attraverso l'apposito processo di valutazione di impatto (art. 35), tenendo conto delle misure tecniche di protezione del sistema [2]. Non essendoci più una lista delle misure di protezione minime che il titolare deve adottare, non è possibile individuare delle misure standard uguali per tutti perché la valutazione è rimessa di volta in volta al titolare e al responsabile del trattamento, in relazione ai rischi specificamente individuati per il caso in questione.
Un'altra novità è l'obbligo di notifica delle relazioni dei dati personali di cui si viene a conoscenza all'autorità di controllo, entro 72 ore o comunque senza ingiustificato ritardo.

Capitolo 2
Smart assistant e dati personali

L'espansione delle tecnologie digitali nella vita quotidiana ha portato, negli ultimi anni, a una vasta diffusione degli assistenti intelligenti, noti come *smart assistant*. Questi software, basati sul *machine learning*, ossia sistemi di apprendimento che utilizzano algoritmi di intelligenza artificiale, possono comprendere il linguaggio naturale umano e interagire con le persone di conseguenza. Le loro capacità spaziano dalla gestione delle richieste più varie (fissare appuntamenti, impostare sveglie, timer e promemoria, riproduzione di musica e notizie, fornire previsioni meteorologiche e di traffico) allo svolgimento di azioni come l'accensione di luci, l'attivazione di elettrodomestici o la regolazione della temperatura domestica.
Il basso costo, la frequente preinstallazione sui dispositivi e la facilità d'uso hanno favorito la diffusione e l'utilizzo degli smart assistant. Essi possono infatti essere integrati in una vasta gamma di dispositivi: dagli smart speaker nelle abitazioni e in altri ambienti, come uffici e automobili, ai dispositivi indossabili (*wearable*), fino ai comuni smartphone, computer e tablet. Particolarmente utile è il loro impiego per facilitare le attività quotidiane delle persone con ridotta autonomia.

Per fornire tali servizi, gli assistenti vocali raccolgono costantemente dati personali non solo degli utenti diretti ma anche di chiunque si trovi nell'ambiente circostante. Inoltre, gli smart assistant sfruttano le potenzialità dell'*Internet of Things* (IoT), integrando vari oggetti intelligenti per raccogliere informazioni e migliorare i servizi offerti, come smartwatch, smart TV, e sistemi di controllo e videosorveglianza remoti, ampliando così le possibilità di raccolta e incrocio dei dati e la diffusione delle informazioni personali.
Diventa quindi fondamentale considerare non solo l'interconnessione ma anche l'interoperabilità tra i sistemi informatici. La tendenza attuale è lo sviluppo di multipiattaforme che consentono il controllo di dispositivi intelligenti di diversi fornitori da un unico punto di gestione. Un esempio significativo è l'accordo tra Amazon, Apple e Google per creare un protocollo unificato, che permette di controllare tutti i dispositivi tramite Alexa, Siri e Google Assistant[1]. Non è banale notare come ogni Big Player della Rete abbia sviluppato un proprio smart assistant, strumento diretto per la profilazione degli utenti.

L'adozione di assistenti vocali è strettamente collegata ai progressi nell'intelligenza artificiale, sollevando questioni giuridiche e etiche.

[1] L'accordo risale al dicembre 2019. Oltre ai citati Google, Amazon ed Apple, hanno aderito all'accordo in questione i produttori della ZigBee Alliance (associazione di aziende tecnologiche che cura lo standard di comunicazione wireless), fra cui Ikea, Samsung SmartThings e Schneider Electric, a conferma del grande interesse che il mercato della domotica suscita. Il relativo protocollo è open source così che tutti possano realizzare prodotti compatibili con i tre assistenti vocali.

L'idea che una macchina "intelligente" possa prendere decisioni autonome con impatti sui diritti fondamentali degli individui suscita preoccupazioni e richiede una riflessione approfondita.
A riguardo, la Commissione Europea ha emanato delle Linee Guida per uno sviluppo etico dell'intelligenza artificiale, contenute nel "Libro bianco sull'intelligenza artificiale — Un approccio europeo all'eccellenza e alla fiducia" del 19 febbraio 2020, che forniscono indicazioni per uno sviluppo di IA a misura d'uomo, "*etica, sicura e all'avanguardia, realizzata in Europa*" [3]. A livello nazionale, va ricordato il documento "Proposte per una strategia italiana per l'intelligenza artificiale" del Gruppo di esperti del MISE, rilasciato nel 2019, che suggerisce un percorso verso un'IA complementare, e non meramente sostitutiva, all'intelligenza umana, in grado di rispettare i valori e i principi fondamentali. [4]

2.1 I rischi per gli utenti

In questo contesto, l'attenzione particolare riservata agli assistenti vocali "intelligenti" deriva da una duplice ragione: lo stretto legame che il loro funzionamento ha inevitabilmente con i dati personali e il loro elevato grado di pervasività nella vita degli utenti. In particolare, preoccupazioni riguardanti l'ingente quantitativo di dati personali raccolti ed elaborati da questi dispositivi, e le relative perplessità, sono state sollevate con riferimento agli home speaker, collocati nell'ambiente domestico, luogo in cui si svolge la vita privata e familiare. Inoltre, gli assistenti vocali sono costantemente in attività grazie agli altri dispositivi a cui sono connessi. Ciò significa che, anche quando l'assistente non è in uso, esso può trasmettere continuamente ogni accadimento o variazione dell'ambiente percepito, realizzando così un'operazione continua di monitoraggio dei comportamenti e di profilazione degli individui. D'altronde, questi dispositivi hanno dimostrato di registrare indiscriminatamente tutte le conversazioni all'interno dell'ambiente domestico, comprese quelle che coinvolgono terzi ignari della loro presenza o funzionamento. Gli utenti, così come i terzi inconsapevoli, potrebbero persino attivare l'assistente inavvertitamente, con comandi vocali impartiti involontariamente: alcuni studi hanno infatti rivelato che molti speaker si accendono non solo per effetto della pronuncia delle parole convenzionali, ma rispondono anche a una serie di ulteriori stimoli vocali. La diffusa inconsapevolezza degli utenti risulta particolarmente problematica per quei soggetti che potrebbero trarre i maggiori vantaggi da tali soluzioni, ossia i soggetti più vulnerabili.

Alcuni principi sanciti dal regolamento si adattano con difficoltà a scenari tecnologicamente evoluti, come quello in esame, specialmente laddove il trattamento dei dati raccolti dagli assistenti vocali si traduca in un'attività di Big Data Analytics, ossia nella raccolta e analisi di grandi volumi di dati. Tra questi principi, si evidenziano i tre strettamente connessi della minimizzazione dei dati trattati (art. 5, par. 1, lett. c GDPR), della limitazione della loro conservazione (art. 5, par. 1, lett. e GDPR) e della limitazione delle finalità del trattamento (art. 5, par. 1, lett. b GDPR).

In tale contesto, neppure l'anonimizzazione, prevista dal regolamento come misura di protezione dei dati personali e coerente con il principio di minimizzazione, dimostra particolare efficacia, poiché l'incrocio di dati consente comunque un'alta probabilità di re-identificazione dell'interessato.

Va inoltre considerato che gli speaker intelligenti sono idonei a raccogliere e trattare non solo dati che costituiscono caratteristiche personali dell'utilizzatore (sesso, età, ecc.), ma anche informazioni rientranti tra le categorie particolari ex art. 9 GDPR, come i dati sanitari (ad esempio, uno smart assistant istruito per ricordare l'orario di assunzione dei farmaci) e soprattutto i dati biometrici. Questi ultimi rappresentano una tipologia di dati personali con caratteristiche intrinseche peculiari, in cui si verifica una sostanziale coincidenza fra persona e dato, rendendo il corpo del soggetto strumento per la sua identificazione, con possibili incidenze sull'identità stessa della persona. I dati biometrici, inoltre, sono idonei a rivelare caratteristiche uniche del soggetto, tanto da essere i soli dati personali a consentire un'identificazione univoca della persona. L'attivazione e l'operatività dello speaker dipendono infatti dal comando vocale; se poi lo smart assistant è dotato anche di videocamera, esso raccoglierà dati quali la conformazione dell'iride e le espressioni del volto, dalle quali ricavare persino stati emozionali, e sarà comunque capace di geolocalizzare l'utente. Sebbene le tecnologie biometriche apportino consistenti vantaggi pratici, consentendo il riconoscimento automatizzato dei soggetti e semplificando una pluralità di procedure nelle attività quotidiane, i rischi per l'interessato, connessi a un uso illegittimo o inappropriato dei dati biometrici, sono particolarmente rilevanti, come il furto di identità.

Quando l'obiettivo prioritario degli smart assistant è la profilazione dell'utente a fini commerciali, per l'invio di pubblicità comportamentale, il trattamento dei dati sanitari e biometrici apre scenari molto più delicati. Il rischio è legato alla presenza di bias, ossia quelle distorsioni che gravano sulle decisioni dei sistemi informatici automatizzati e che discriminano sistematicamente e ingiustamente certi individui o gruppi di individui a favore di altri, negando opportunità o generando risultati indesiderati per motivi irragionevoli o inappropriati. La profilazione è espressamente definita dall'art. 4 (4) e regolata dall'art. 22 del GDPR, mentre il principio di non discriminazione non è sancito esplicitamente dal GDPR. Il problema di fondo si traduce nella programmazione e nel design dei modelli algoritmici e delle soluzioni tecnologiche che li applicano.

Di fronte alle criticità evidenziate, una soluzione di natura progettuale potrebbe essere l'approccio migliore per risolvere le problematiche a monte, mediante opportune scelte di design del programma di assistenza vocale. Questo dovrebbe, ad esempio, essere concepito per minimizzare la raccolta dei dati, impiegare tecniche di crittografia e/o pseudonimizzazione durante la trasmissione delle informazioni all'Internet Service Provider e attivarsi esclusivamente al riconoscimento del comando vocale dell'utente principale, evitando così la raccolta e il trattamento di dati relativi ad altri soggetti.

Inoltre, dovrebbe permettere all'utente di configurare modalità di funzionamento specifiche.

Tale approccio realizzerebbe appieno il principio della privacy by design previsto dal GDPR (art. 25), attribuendo alla protezione dei dati un ruolo centrale nel processo di progettazione. Questa strategia favorirebbe inoltre i produttori nell'adozione di criteri proattivi piuttosto che reattivi, con l'obiettivo di prevenire potenziali violazioni dei diritti degli interessati.

La privacy by design è un principio strettamente legato all'analisi del rischio, che costituisce un caposaldo del GDPR. Poiché spesso né i titolari né i responsabili del trattamento dispongono degli strumenti adeguati a condurre tale analisi, sarebbe opportuno trasferire l'obbligo di effettuare l'analisi stessa a terzi, che potrebbero essere le Autorità garanti stesse. In questo modo, la valutazione del rischio si sposterebbe, almeno parzialmente e indirettamente, anche a carico del produttore o fornitore del servizio/prodotto smart, il quale sarebbe ad esempio tenuto a procurarsi idonea certificazione. Accredia, a tal proposito, è incaricata di attestare la competenza degli organismi secondo la norma UNI CEI EN ISO/IEC 17065 per la certificazione dei prodotti e servizi, basandosi sui requisiti aggiuntivi individuati dal Garante, a partire dalle Linee guida comuni elaborate dal Comitato europeo per la protezione dei dati personali. In questa prospettiva, la nozione di sicurezza del servizio o prodotto da prendere a riferimento non si limiterebbe più alla mera sicurezza informatica o alla sicurezza del solo processo di trattamento dei dati ma, in un'ottica più ampia, alla sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali della persona.

2.2 I consigli del Garante per un uso a prova di privacy

Come visto e approfondito nei paragrafi precedenti, gli assistenti digitali possono raccogliere e memorizzare una grande quantità di dati personali, non solo relativi all'utilizzatore diretto, ma a chiunque si trovi nello stesso ambiente, riguardanti:

- Scelte, preferenze e abitudini relative a stili di vita, consumi, interessi;
- Caratteristiche biometriche;
- Geolocalizzazione (posizione, percorsi abituali o frequenti, domicilio, indirizzo del posto di lavoro);
- Caratteristiche delle persone che si trovano nell'ambiente in cui operano;
- Stati emotivi.

È quindi opportuno cercare di fare un uso informato e consapevole di questi strumenti, per tutelare in modo adeguato i nostri dati personali e quelli di tutte le persone che entrano, volontariamente o meno, nel campo di azione degli assistenti digitali.

A tale scopo, il Garante propone i seguenti consigli per un uso più sicuro degli assistenti digitali [5]:

1) Informarsi su come vengono trattati i propri dati

   Se per attivare l'assistente digitale o le relative app di gestione è richiesta una registrazione con il conferimento di dati personali, è fondamentale leggere attentamente l'informativa sul trattamento dei dati personali, la quale deve essere sempre disponibile, ad esempio sul sito dell'azienda che fornisce il servizio o nella confezione del dispositivo che include lo smart assistant. In particolare, è cruciale comprendere:

   - Quali e quante informazioni verranno raccolte direttamente dall'assistente digitale tramite microfono e videocamera;
   - In che modo i dati raccolti potrebbero essere utilizzati o trasferiti a terzi, in particolare se esclusivamente per il funzionamento dello strumento o anche per altre finalità;
   - Chi potrebbe ricevere i dati raccolti e come, nonché se sono previsti, per qualsiasi motivo, accessi diretti al microfono e alla videocamera dello smart assistant da parte di operatori dell'azienda produttrice o della società che gestisce i servizi offerti;
   - Dove sono conservati questi dati e per quanto tempo.

2) Non dire troppe cose allo smart assistant

   Quando si attiva per la prima volta lo smart assistant, è preferibile fornire solo le informazioni strettamente necessarie per la registrazione e l'attivazione dei servizi, utilizzando eventualmente pseudonimi per gli account, soprattutto se riguardano minori. In generale, si potrebbe optare per impedire l'uso dello smart assistant ai minori, configurando password o impronte vocali che limitino l'accesso al servizio esclusivamente agli adulti autorizzati.

   È preferibile non utilizzare l'assistente digitale per memorizzare informazioni sensibili, come password o numeri di carte di credito.
   È necessario inoltre valutare attentamente i rischi e i benefici dell'eventuale accesso dello smart assistant ai dati conservati sul dispositivo su cui è installato, come l'archivio fotografico, la rubrica e il calendario.

3) Disattivare l'assistente digitale quando non è utilizzato

   Quando è acceso ma non in uso, l'assistente digitale si trova in uno stato di "passive listening", una sorta di dormiveglia dal quale si attiva non appena rileva la parola di attivazione scelta.

Alcune precauzioni al riguardo comprendono:

- Se possibile, scegliere con attenzione la parola di attivazione, evitando termini di uso frequente (nomi di persona, animali, oggetti di uso quotidiano);
- Ricordare che, durante lo stato di passive listening, l'assistente digitale può potenzialmente ascoltare e, eventualmente, vedere tutto ciò che avviene nell'ambiente circostante. Questi dati possono essere memorizzati, inviati a terzi o conservati su server esterni anziché sul dispositivo stesso.

Per evitare acquisizioni e trasmissioni non desiderate di dati, si consiglia, quando l'assistente digitale non è in uso (ad esempio, di notte o quando si è fuori casa):

- Se possibile, disattivare il microfono o la videocamera, o entrambi, utilizzando i tasti presenti sul dispositivo che ospita l'assistente digitale o le impostazioni delle app di gestione;
- In alternativa, disattivare completamente l'assistente digitale o spegnere il dispositivo che lo ospita. Questa scelta può risultare scomoda poiché richiede la riattivazione del dispositivo quando necessario, ma garantisce una maggiore protezione della propria privacy.

4) Decidere quali funzioni mantenere attive

Se l'assistente digitale è in grado di svolgere particolari azioni, come inviare messaggi ad altre persone tramite SMS o sistemi di messaggistica, pubblicare contenuti sui social o effettuare acquisti online, è possibile:

- Disattivare tali funzioni;
- Inserire una password per autorizzare l'uso solo su specifica richiesta dell'utente.

Gli assistenti digitali, come tutti i dispositivi e servizi dell'IoT, non solo si connettono alla rete, ma possono anche "dialogare" con altri dispositivi IoT. Questa capacità amplia la possibilità di raccolta, incrocio dei dati e diffusione di informazioni personali. Ad esempio, gli assistenti digitali con funzioni domotiche possono essere collegati con vari oggetti e servizi presenti nelle abitazioni, dagli elettrodomestici alle smart TV, dalle luci ai sistemi di sicurezza e videosorveglianza. Queste funzioni semplificano la vita, permettendo di controllare molti oggetti a distanza con la sola voce.

Tuttavia, è sempre opportuno:

- Informarsi con attenzione su come e da chi vengono raccolti, elaborati, conservati e a chi possono essere resi accessibili i dati personali;
- Considerare l'impatto sulla privacy domestica.

È consigliabile anche valutare se disattivare alcune funzioni di controllo domotico e inserire apposite password per controllare l'attivazione o disattivazione dei sistemi, migliorando così la sicurezza dell'uso dello smart assistant. Ad esempio, c'è il rischio che la voce dell'utente venga captata e clonata da malintenzionati per controllare elettrodomestici, ingressi o sistemi di protezione della casa, oppure per spiare l'interno dell'abitazione utilizzando microfono e videocamera.

5) Cancellare periodicamente la cronologia delle informazioni

Per limitare il trattamento dei dati personali raccolti dall'assistente digitale, si può cancellare periodicamente, parzialmente o totalmente, la cronologia delle informazioni in esso registrate. Questa operazione può essere effettuata utilizzando il sito web o l'app dedicata alla gestione dello smart assistant.

6) Prestare attenzione alla sicurezza

È consigliata la scelta di una password di accesso complessa, non solo per l'uso dello smart assistant ma anche per la sua connessione ad Internet. Tra le precauzioni da prendere:

- Verificare che la crittografia della rete Wi-Fi sia impostata preferibilmente sul protocollo di sicurezza WPA 2;
- Cambiare periodicamente la password;
- Verificare se sul dispositivo in cui è installato lo smart assistant siano presenti sistemi di protezione antivirus e tenerli costantemente aggiornati.

7) Non cedere i propri dati insieme allo smart assistant

Quando si decide di vendere, regalare o dismettere un dispositivo su cui è installato un assistente digitale, è fondamentale disattivare eventuali account personali creati per l'attivazione e la connessione online dello stesso. Inoltre, è necessario provvedere alla cancellazione di tutti i dati eventualmente registrati all'interno del dispositivo o nelle app di gestione.
Nel caso in cui i dati raccolti siano stati trasmessi e conservati nei database dell'azienda produttrice o di altri soggetti terzi, è opportuno richiederne la cancellazione.

Capitolo 3
Caso di studio: Impiego degli smart assistant nella sanità

Nei capitoli precedenti, gli assistenti digitali sono stati presentati come un supporto alla gestione dei servizi di domotica nelle abitazioni, così come alla ricerca di informazioni nei vari luoghi in cui si svolge la quotidianità. Gli assistenti vocali, però, non sono solo questo. Gruppi di ricerca sparsi in tutto il mondo, spinti dalla possibilità di fornire supporti medico-curativi a determinate categorie di pazienti, che potrebbero beneficiare ampiamente di strumenti tecnologicamente avanzati, si apprestano a valutare e testare auspicabili interazioni positive che gli smart assistant possono determinare in contesti di sanità digitale. Lo sfruttamento dell'IA in campo sanitario ha subito un'evoluzione da un approccio ritenuto futuristico ad una fiorente realtà [6]. Dal punto di vista giuridico, questi scenari innovativi, pur promettendo risultati straordinari in termini di supporto ai processi curativi, presentano notevoli criticità, specialmente in relazione alla disciplina in materia di protezione dei dati personali contenuta nel GDPR. Tecnologia e diritto interagiscono strettamente, influenzandosi reciprocamente. Al giurista spetta il compito di determinare il corretto equilibrio tra le esigenze dei singoli, in termini di autodeterminazione informativa, e le necessità del sistema sanitario, focalizzandosi sui processi curativi e sulle scelte di appropriatezza. Inoltre, il giurista è chiamato a un'attività creativa, volta a trovare regole applicative partendo da principi generali, in un contesto dove il legislatore può solo rincorrere le innovazioni tecnologiche con regole destinate a rapida obsolescenza [7].

Un caso esemplare dell'impiego e delle potenzialità degli assistenti vocali in ambito sanitario è il Boston Children's Hospital, che ha introdotto tecnologie vocali in tre sperimentazioni:

- Nel reparto di terapia intensiva l'assistente vocale supporta i professionisti negli aspetti organizzativi, per facilitare e rendere più rapide le attività burocratiche attraverso l'uso dell'intelligenza artificiale, capace di elaborare il linguaggio naturale per estrarre informazioni mediche da molteplici fonti come fogli di accettazione, note mediche e cartelle cliniche elettroniche;
- Nell'unità di trapianti funge da interfaccia rapida per i controlli preliminari;
- Fuori dall'ospedale, l'assistente vocale aiuta i pazienti con patologie comuni come febbre e raffreddore. Questo utilizzo è stato sperimentato dal National Health Service (NHS) in Europa, attraverso un accordo con Amazon, permettendo agli utenti di ricevere consigli medici da Alexa basati sulle informazioni verificate dal NHS. I destinatari principali di questa iniziativa sono anziani o persone affette da cecità, con l'obiettivo di migliorare l'assistenza a domicilio e alleggerire il carico sulle strutture sanitarie.

L'Agenzia per l'Italia Digitale (AgID) nel "Libro bianco sull'intelligenza artificiale al servizio del cittadino" prospetta un utilizzo proficuo dell'assistente digitale anche come logopedista o psicologo per soggetti dislessici, fornendo monitoraggio costante e tentativi di correzione. L'interesse si estende anche ai pazienti diabetici, che potrebbero utilizzare l'assistente per informazioni sugli zuccheri negli alimenti o per ottenere indicazioni terapeutiche personalizzate, implicando il trattamento di dati sanitari e decisioni algoritmiche. L'assistente vocale può rappresentare uno strumento chiave anche per patologie croniche gravi, che richiedono assistenza continua a domicilio e un costante confronto con il personale sanitario per monitorare i sintomi e garantire un pronto intervento in caso di crisi acute. Le problematiche includono la transizione dall'ospedale al contesto domestico e la difficoltà nel riportare accuratamente e tempestivamente i sintomi al medico curante. Il virtual assistant potrebbe supportare i caregiver o i pazienti stessi, adattandosi alle loro esigenze nel tempo. L'uso del linguaggio naturale per registrare sintomi riduce l'omissione di segnalazioni e migliora la precisione. Oltre a fornire informazioni su richiesta dell'utente, l'assistente vocale può essere impiegato per progetti volti a migliorare lo stile di vita del paziente, supportandolo quotidianamente al fine di incentivare comportamenti che possano ridurre l'impatto della patologia stessa e l'occorrenza di patologie secondarie. Il monitoraggio costante offerto dall'assistente vocale permette di fornire indicazioni tempestive e personalizzate al personale sanitario

La ricerca di un equilibrio tra le prospettive di efficienza e i timori di una spersonalizzazione dell'entità a cui è affidato il giudizio ha spinto il legislatore europeo a redigere l'articolo 22 del GDPR. Questo articolo conferisce all'interessato il diritto di "*non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Per essere soggetta al divieto ex articolo 22, comma 1, la decisione deve essere unicamente basata su un trattamento automatizzato e deve produrre effetti giuridici nella sfera dell'interessato o incidere in modo analogo significativamente sulla sua persona. Tale proibizione è mitigata dal secondo comma, che introduce basi legali che legittimano il processo decisionale automatizzato. Fondamentale per la corretta definizione dell'ambito applicativo di questa norma (e successivamente per lo studio dell'efficacia delle tutele) è l'individuazione del significato di "*decisione unicamente basata su un processo automatizzato*". È da rigettare l'interpretazione che esclude l'applicazione della disciplina ex articolo 22 laddove sia integrato un qualsiasi intervento umano nel processo decisionale. Tale interpretazione, infatti, consentirebbe di eludere le previsioni del GDPR inserendo un intervento umano meramente formale e fittizio nel processo. Al contrario, il fatto che la decisione debba essere unicamente basata su un trattamento automatizzato implica l'applicazione della norma a quelle decisioni i cui presupposti siano interamente frutto di trattamenti automatizzati.

Il punto di riferimento, quindi, è il tipo di coinvolgimento umano, e non la sua sola presenza, il quale deve essere caratterizzato necessariamente dall'autorità e dalla competenza del soggetto chiamato a intervenire affinché possa effettivamente modificare la decisione. Le criticità sorgono nel momento in cui si prendono in considerazione tecnologie più avanzate le cui logiche diventano complesse. Il terzo comma menziona il diritto di esprimere la propria opinione, di contestare la decisione e di ottenere l'intervento umano. L'affidabilità e l'utilità dei risultati dipendono anche dal gold standard scelto dai programmatori, ossia dal test di riferimento rispetto al quale viene misurata l'accuratezza di un secondo test diagnostico che si intende valutare (da cui si dedurrà una maggiore o minore affidabilità dell'algoritmo).

Tuttavia, i fenomeni osservati in medicina hanno una componente di incertezza intrinseca e tendenzialmente ineliminabile, che rende arduo (se non impossibile) trovare un gold standard universale; conseguentemente, il professionista chiamato a intervenire potrebbe giudicare la decisione sulla base di un diverso parametro di riferimento.

Conclusioni

Le tecnologie hanno da sempre supportato e condizionato i processi curativi. Il medico utilizza gli strumenti che gli vengono resi disponibili per assistere al meglio i propri pazienti, secondo scienza e coscienza. Tradizionalmente, ciò ha riguardato oggetti destinati a intervenire direttamente sulla fisicità del paziente. Successivamente, sono emersi strumenti volti alla gestione clinico-amministrativa degli utenti del servizio sanitario e al supporto dei processi decisionali. Il rapporto medico-paziente si è quindi trasformato, le modalità di interazione sono cambiate e la percezione degli attori coinvolti si è evoluta. Questo ha spesso sollevato preoccupazioni riguardo al rischio di disumanizzazione del rapporto empatico che caratterizza il contesto sanitario.

Attualmente, stiamo assistendo a un cambiamento epocale. L'intelligenza artificiale applicata a strumenti che non solo mimano il comportamento umano nella gestione e soluzione di problemi complessi, ma che, sintetizzando la voce, interagiscono direttamente con i pazienti emulando la tradizionale modalità orale di comunicazione, determina relazioni completamente nuove, talvolta del tutto autonome: non più un rapporto uomo a uomo, seppur mediato da una tecnologia, ma un confronto quasi esclusivamente uomo a macchina.

Il nuovo approccio cognitivo del paziente rispetto a un servizio sanitario dotato di questi strumenti può essere riassunto nella convinzione che "la macchina non sbaglia mai". L'errata percezione che un sistema completamente automatizzato debba necessariamente fornire risposte efficaci porta a non contestualizzare l'ambito applicativo di queste "macchine" e a considerare il fallimento di alcuni processi curativi, spesso inevitabile alla luce di un quadro clinico compromesso, come un errore medico, una malpractice che solo l'intervento giudiziario può sanare. Molto si gioca sulla percezione, corretta o distorta, che noi come esseri umani abbiamo dell'intervento della macchina stessa.

Analogamente a qualsiasi strumento, anche gli assistenti vocali di ultima generazione soffrono inevitabilmente di bias legati al tipo di "addestramento" ricevuto (le informazioni utilizzate per educare gli algoritmi a "ragionare"), alla mancanza di "empatia" rispetto al tradizionale rapporto umano (che può determinare diagnosi e cure razionalmente perfette ma inefficaci rispetto all'unicità dell'essere umano), e al contesto socio-culturale in cui vengono utilizzati (divide generazionali, diversità culturali che impattano sugli stili di vita, ecc.). Sarà quindi necessario analizzare questi possibili bias al fine di verificarli, se non risolverli.

Un altro tema centrale in questa discussione è quello dei processi decisionali unicamente basati sul trattamento automatizzato dei dati sanitari, ampiamente trattato sopra. Come già descritto, il legislatore europeo ha previsto all’art. 22 del GDPR una disciplina specifica per tali scenari.

Oltre agli obblighi informativi che enfatizzano l'importanza della trasparenza di questi processi (in contesti fortemente caratterizzati da black-box), una delle garanzie principali è quella di prevedere un possibile intervento umano su richiesta del paziente/utente. L'intermediario umano dovrebbe essere dotato delle conoscenze mediche e informatiche necessarie per valutare con criticità e, eventualmente, modificare la decisione assunta dalla macchina. Tuttavia, questo soggetto dovrebbe essere scevro da condizionamenti e dal tipico processo mentale di ancoraggio alla prima decisione assunta dallo strumento automatizzato, anche a fronte del rischio legale di discostarsene.

Infine, la privacy by design gioca un ruolo essenziale. I processi di trattamento dei dati personali devono essere informati, fin dalla loro progettazione, dai principi e dalle tutele riconosciuti dall'ordinamento giuridico. Questo richiede l'attivazione di tavoli di lavoro interdisciplinari, dove la programmazione dei codici informatici sia supportata da esperti di vari settori, quali la medicina, la sociologia, la psicologia e, per quanto ci riguarda, il diritto. Servirà, pertanto, un giurista in grado di comprendere, almeno negli elementi essenziali, i percorsi di sviluppo delle piattaforme informatiche.

È ora necessario affrontare le criticità insite nelle nuove tecnologie e cercare di influenzarne la progettazione. Questo compito non può più essere demandato ad altri.

Riferimenti

[1] A. Cataleta, A. Longo e R. Natale, «Network Digital 360,» 5 Aprile 2024. [Online]. Available: https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/. [Consultato il giorno 26 Giugno 2024].

[2] B. Saetta, «Protezione dati personali,» 11 Ottobre 2023. [Online]. Available: https://protezionedatipersonali.it/regolamento-generale-protezione-dati. [Consultato il giorno 26 Giugno 2024].

[3] E. Commission, «Artificial Intelligence: Commission outlines a European approach to boost investment and set ethical guidelines,» Brussels, 2018.

[4] L. Vizzoni, «Smart assistant e dati personali: quali rischi per gli utenti?,» *MediaLaws,* 2020.

[5] Garante per la protezione dei dati personali, «Garante per la protezione dei dati personali,» Marzo 2021. [Online]. Available: www.gpdp.it. [Consultato il giorno Giugno 2024].

[6] J. Chung, «What Should We Do About Artificial Intelligence in Health Care?,» *Health Law Journal,* vol. 22, n. 3, pp. 37-40, 2017.

[7] P. Guarda e L. Petrucci, «Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati,» *BioLaw Journal,* 2020.