Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati

Paolo Guarda, Livia Petrucci*

WHEN ARTIFICIAL INTELLIGENCE SPEAKS: VOCAL ASSISTANTS AND E-HEALTH IN THE LIGHT OF THE GENERAL DATA PROTECTION REGULATION

ABSTRACT: The intellect and the speech, faculties commonly used to distinguish humans from other living beings, represent instead the point of contact between man and machine. The vocal assistant combines these qualities and makes use of them to gain a pivotal role in the healthcare system. This scenario has great potential, but shows strong issues too in terms of compliance with the General Data Protection Regulation. The aim of the paper is twofold. Firstly, to critically discuss the implications and the effectiveness of the safeguards provided by Article 22 of the GDPR in case of automated decision making in the healthcare field. Secondly, to analyze the organizational and technical security measures to be enforced, stressing the importance of the data protection by design approach. Further, it will emerge the need for the close collaboration of several professionals and knowledges to solve the riddle.

KEYWORDS: Vocal assistant; artificial intelligence; e-Health; GDPR; data protection

1. Introduzione: macchine che parlano tra futuro e realtà della sanità digitale

«*Giro giro tondo, io giro intorno al mondo*…». Quando pensiamo ad un assistente vocale la memoria va inevitabilmente a questa filastrocca, cantata in modo sinistro dal padre di tutte le "macchine che parlano", ovvero Hal9000 nel famosissimo film "2001: Odissea nello Spazio" di Stanley Kubrick (1968). Di tempo ne è trascorso e quanto appariva allora futuribile ora è divenuto realtà. Gli assistenti vocali fanno oramai parte della nostra quotidianità: ci aiutano a gestire i

**Paolo Guarda, Ricercatore di Diritto privato comparato presso la Facoltà di Giurisprudenza - Università di Trento, paolo.guarda@unitn.it, è autore dei paragrafi 1 e 5. Livia Petrucci, Dottoressa in Giurisprudenza presso l'Università di Trento, consulente in materia di protezione dei dati personali, liviapetrucci1@gmail.com, è autrice dei paragrafi 2, 3 e 4.* *Ultimo accesso ai siti Web citati 11 maggio 2020.* *Un grazie sentito va a tutte le persone con le quali abbiamo avuto la possibilità di confrontarci e discutere durante la redazione di questo contributo. In particolare, ci teniamo a nominare l'unità di ricerca "eHealth" della Fondazione Bruno Kessler ed il Centro di competenza sulla salute digitale "TrentinoSalute4.0".*

servizi di domotica nelle nostre case o, semplicemente, a scegliere la playlist da ascoltare durante una cena con gli amici (vedi Google Home ed Alexa, ad esempio); ci supportano quando siamo in auto, al lavoro o mentre passeggiamo per la strada e ci forniscono indicazioni utili semplicemente attraverso una interrogazione vocale (vedi Siri e Cortana). Questi apparecchi che sintetizzano la voce umana e che sono in grado di interagire con noi si sono via via evoluti fino a prevedere, al loro interno, sistemi basati su forme di intelligenza artificiale e processi di "machine learning": non solo quindi sono sempre più efficaci ed affidabili, ma imparano attraverso l'interazione umana, affinano le loro capacità linguistiche, migliorano i processi di ascolto e risposta[1].

Gli assistenti vocali, però, non sono solo questo. Gruppi di ricerca sparsi in tutto il mondo si apprestano a valutare e testare auspicabili interazioni positive che questi possono determinare in contesti di sanità digitale. La possibilità di fornire supporti medico-curativi a determinate categorie di pazienti che potrebbero beneficiare largamente di strumenti così evoluti spinge a studiare la loro eventuale implementazione: ad esempio come chatbot informativi per soggetti anziani (i quali spesso risultano, ad oggi, esclusi dalle potenzialità offerte dalle "usuali" piattaforme tecnologiche che si basano su tablet o smartphone) o per la cura di specifici tipi di malattie che sembrano ben adattarsi alle caratteristiche di questi particolari device (si parla, infatti, di possibili sperimentazioni nell'ambito della demenza senile, del Parkinson, ecc.)[2].

Su un versante prettamente giuridico, questi scenari innovativi, pur promettendo strabilianti risultati in termini di supporto ai processi curativi, presentano notevoli criticità in particolar modo con riferimento alla disciplina in materia di protezione di dati personali ora, come noto, contenuta, in ambito europeo, nel Regolamento UE 2016/679 (Regolamento generale sulla protezione dei dati; d'ora in avanti Regolamento o, con acronimo anglosassone, GDPR)[3]. Diversi sono, infatti, gli elementi che destano sospetto e richiedono un'indagine approfondita: la possibile realizzazione di processi decisionali unicamente automatizzati e le garanzie che questi devono prevedere (art. 22 GDPR); i problemi di governance dei ruoli privacy con riferimento alla catena di soggetti coinvolti; i rischi per la sicurezza, con

[1] In generale in tema di applicazione dell'intelligenza artificiale al contesto sanitario, si v. W. NICHOLSON PRICE, *Artificial Intelligence in Health Care: Applications and Legal Implications*, in *The SciTech Lawyer*, 14, 1, 2017, 10 ; J. CHUNG, *What Should We Do About Artificial Intelligence in Health Care?*, in *NYSBA Health Law Journal*, 22, 3, 2017, 37 (in Rete: https://ssrn.com/abstract=3113655).

[2] Con particolare attenzione agli aspetti legati alla privacy ed alla sicurezza dei dati, si v. A. PFEIFLE, *Alexa, What Should We Do about Privacy? Protecting Privacy for Users of Voice-activated Devices*, 93 *Wash. L. Rev*. 421 (2018); M. E. STUCKE, A. EZRACHI, *Alexa et al., What Are You Doing with My Data?*, in *Critical Analysis of Law*, 5, 1, 2018, 148; M.B. HOY, *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants*, in *Medical Reference Services Quarterly*, 37, 1, 2018, 81; A. HASSOON, J. SCHRACK, D. NAIMAN, D. LANSEY, Y. BAIG, V. STEARNS, D. CELENTANO, S. MARTIN, L. APPEL, *Increasing Physical Activity Amongst Overweight and Obese Cancer Survivors Using an Alexa-Based Intelligent Agent for Patient Coaching: Protocol for the Physical Activity by Technology Help (PATH) Trial*, in *JMIR Res Protoc*, 7, 2, 27, 2018, 2, in Rete: https://www.researchprotocols.org/2018/2/e27/.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). La letteratura scientifica di commento al Regolamento europeo è, oramai, vastissima sia a livello nazionale che internazionale. Si v., tra gli altri, C. KUNER, L.A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (a cura di), *The EU General Data Protection Regulation: a Commentary*, OUP Oxford, 2020; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

ISSN 2284-4503

particolare attenzione ai sistemi di autenticazione, che l'utilizzo di una caratteristica biometrica come la voce pongono. Solo per citare i temi più dibattuti.
La tecnologia si pone in stretto rapporto con il mondo del diritto. La relazione è biunivoca ed il condizionamento reciproco. Gli assistenti vocali presentano per il giurista sfide non di poco momento: a lui è demandato il compito di determinare il corretto bilanciamento tra le esigenze dei singoli, con riferimento all'autodeterminazione informativa, e le necessità del sistema sanitario, con attenzione ai processi curativi ed alle scelte anche in termini di appropriatezza[4]. Sempre il giurista è chiamato ad un'attività marcatamente creativa, volta a trovare la regola applicativa partendo da principi generali e rispetto ad un legislatore che non può che inseguire le innovazioni tecnologiche con regole condannate inevitabilmente ad una rapida obsolescenza[5].
Questo articolo si propone di introdurre il tema dell'applicazione degli assistenti vocali a scenari di sanità digitale, evidenziando le criticità in termini di conformità alla disciplina in materia di protezione dei dati personali. Il secondo paragrafo sarà, pertanto, dedicato alla descrizione di alcuni reali scenari applicativi al fine di dimostrare l'attualità della materia qui oggetto di analisi. Il terzo paragrafo, invece, affronterà il complesso tema dell'utilizzo di algoritmi nei processi decisionali, focalizzando l'attenzione sull'art. 22 GDPR in materia di processi unicamente automatizzati e sottolineando l'importanza del principio di trasparenza in tale settore. Il quarto paragrafo, poi, sarà dedicato alle misure di sicurezza e porterà in esponente alcuni principi cardine del nuovo assetto regolatorio: la c.d. accountability (o responsabilizzazione, nella infelice traduzione italiana) e la privacy by design. In particolare, la trattazione sarà suddivisa in due sottoparagrafi: uno dedicato alle misure di carattere organizzativo, dove verranno analizzate le problematiche connesse alla gestione dei ruoli privacy in scenari cloud; l'altro alle misure di carattere tecnico, nello specifico con attenzione alle criticità che i sistemi di autenticazione vocale presentano, alle loro vulnerabilità ed alle possibili soluzioni atte a mitigarne i rischi. Le conclusioni saranno volte a tirare le fila di quanto descritto ed a disegnare possibili scenari futuri circa l'utilizzo di questi strumenti**.**

2. Impiego e potenzialità dell'assistente vocale in ambito sanitario

Gli scenari applicativi dell'assistente vocale in ambito sanitario sono molteplici e assumono contorni via via concreti: non è più necessario uno sforzo d'immaginazione per trovare dei punti d'incontro tra l'impiego di tale tecnologia ed il contesto medico-sanitario[6]. Ne è un esempio il caso del *Boston Children's Hospital* che ha introdotto tecnologie vocali attivando tre sperimentazioni: nel reparto di terapia

[4] Sull'appropriatezza dei sistemi sanitari si v., in prima battuta, B. BEATRICI, *L'istituzione della Commissione per l'aggiornamento del Livelli essenziali di assistenza (LEA) e la promozione dell'appropriatezza di essi nel Servizio sanitario nazionale*, in *GiustAmm.it*, 2016, 2, 13.
[5] Sul tema della creatività del giurista, connotazione principale di chi si voglia occupare di diritto dell'informatica, si v. G. PASCUZZI, *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica*, Bologna, 2013.
[6] Per una panoramica sull'attuale impiego degli assistenti vocali in ambito sanitario si v. D. METCALF, T. FISHER, S. PRUTHI, H. P. PAPPAS, *Voice Technology in Healthcare, Leveraging Voice to Enhance Patient and Provider Experiences*, Productivity Press – Taylor & Francis Group, 2020.

intensiva l'assistente vocale supporta i professionisti negli aspetti organizzativi[7], nell'unità di trapianti funge da interfaccia rapida e diretta per i controlli preliminari, mentre fuori dall'ospedale aiuta i pazienti affetti da patologie comuni e di modesta entità quali febbre e raffreddore[8]. Quest'ultimo impiego è stato da pochi mesi sperimentato anche dal *National Health Service* (NHS), primo caso in Europa, attraverso un accordo con Amazon: installando l'apposita app l'utilizzatore potrà chiedere ad Alexa dei consigli di carattere medico attingendo, quale unica fonte, alle informazioni verificate dal NHS[9]. I destinatari principali di questa iniziativa sono persone anziane o affette da cecità, a conferma della volontà dell'azienda sanitaria di migliorare l'assistenza nei confronti di soggetti che possono trarre massimo vantaggio dal supporto costante e digitale nella propria abitazione, alleggerendo il carico di lavoro nelle strutture sanitarie.

L'impiego dell'assistente vocale quale ausilio per la diagnosi e per la terapia del paziente è, quindi, finalizzato alla realizzazione di un vero e proprio Ambient Assisted Living (AAL)[10] al centro del quale vi sarà una tecnologia capace di adattarsi alle esigenze dell'utente e di assumere decisioni autonome. Tali processi sono resi ancor più efficaci grazie al linguaggio naturale che consente un'interazione diretta e garantisce un'estrema facilità d'uso. A sottolineare tali aspetti è la stessa Agenzia per l'Italia Digitale (AgID) che nel Libro bianco sull'intelligenza artificiale al servizio del cittadino[11] prospetta un proficuo utilizzo dell'assistente digitale quale logopedista o psicologo di soggetti dislessici affinché la patologia trovi sia un costante monitoraggio che un tentativo di correzione[12]. L'interesse si è concen-

[7] In un'ottica più ampia, l'impiego dell'assistente vocale per facilitare e rendere più rapide le attività burocratiche e organizzative potrebbe apportare un sensibile miglioramento nella gestione dei servizi sanitari. Ad esempio, attraverso sistemi di Intelligenza Artificiale in grado di elaborare il linguaggio naturale possono essere estratte rapidamente una serie di informazioni mediche relative ad un paziente contenute in molteplici fonti come fogli di accettazione, note mediche e cartelle cliniche elettroniche. Per uno studio sull'incidenza del tempo impiegato in media dai medici ambulatoriali per svolgere tali attività si v. C. SINSKY ET AL., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties*, 165 *Ann Intern Med.* 11 (2016); per un esempio di sistemi di tal sorta e dei potenziali benefici si v. I. HAZARIKA, *Artificial intelligence: opportunities and implications for the health workforce*, in *International Health*, ihaa007, in Rete: https://doi.org/10.1093/inthealth/ihaa007.

[8] C. E. SMALL, D. NIGRIN, K. CHURCHWELL, J. BROWNSTEIN, *What will healthcare look like once smart speakers are everywhere?*, *Harvard Business Review*, pubblicato il 7 marzo 2018, in Rete: https://hbr.org/2018/03/what-will-health-care-look-like-once-smart-speakers-are-everywhere?autocomplete=true; B. METROCK, *The Story Behind Boston Children's Hospital KidsMD Alexa Skill, voicebot.ai,* pubblicato il 17 luglio 2018, in Rete: https://voicebot.ai/2018/07/17/the-story-behind-boston-childrens-hospital-kidsmd-alexa-skill/.

[9] Ad annunciare la collaborazione è stato il *Department of Health and Social Care* con un comunicato stampa disponibile in Rete: https://www.gov.uk/government/news/nhs-health-information-available-through-amazon-s-alexa; H. SIDDIQUE, *NHS teams up with Amazon to bring Alexa to patiens*, *The Guardian*, pubblicato il 10 luglio 2019, in Rete: https://www.theguardian.com/society/2019/jul/10/nhs-teams-up-with-amazon-to-bring-alexa-to-patients.

[10] S. REDDY, *Use of Artificial Intelligence in Healthcare Delivery*, in T. F. HESTON (a cura di), *eHealth - Making Health Care Smarter*, IntechOpen, 2018, in Rete: https://www.intechopen.com/books/ehealth-making-health-care-smarter/use-of-artificial-intelligence-in-healthcare-delivery.

[11] Agenzia per l'Italia Digitale, *Libro bianco sull'intelligenza artificiale al servizio del Cittadino*, versione marzo 2018, in Rete: https://ia.italia.it/assets/librobianco.pdf.

[12] L'AgID affronta contestualmente la possibilità che un simile utilizzo, e più in generale l'impiego di assistenti vocali in tutto il settore sanitario-assistenziale, dia luogo ad una duplice discriminazione: da un lato quella legata all'accesso e all'uso di tali tecnologie, dall'altro quella basata su fattori sociali dell'individuo, *ibidem*. Per ulteriori

trato anche nei confronti dei pazienti diabetici che potrebbero interrogare l'assistente a scopo informativo[13], ad esempio in riferimento alla quantità di zuccheri contenuti in un alimento, oppure potrebbero fornire i propri dati sanitari per ottenere indicazioni terapeutiche precise (le quali implicherebbero il trattamento di dati sanitari e l'assunzione di una decisione da parte dell'algoritmo)[14].

L'assistente vocale, inoltre, può rappresentare uno strumento chiave per patologie croniche particolarmente gravi che richiedono da un lato un'assistenza continua presso l'abitazione del paziente e, dall'altro, un confronto costante con il personale sanitario al fine di monitorare i sintomi e garantire un pronto intervento in caso di crisi acute. Le problematiche che si presentano in tale situazione riguardano in primo luogo la difficoltà del passaggio dal contesto ospedaliero a quello domestico e, una volta effettuata tale transizione, la scarsa accuratezza e il ritardo nel riportare i sintomi al medico curante. In merito al primo scenario, il *virtual assistant* potrebbe consentire l'elaborazione di programmi di supporto per i soggetti incaricati della cura del paziente presso la sua abitazione – o per il paziente stesso – essendo in grado di interagire costantemente con gli stessi e di adattarsi alle loro esigenze, anche laddove queste mutino con il passare del tempo. Riguardo alla registrazione dei sintomi, le tecnologie attualmente a disposizione sono per lo più vincolate all'utilizzo di uno schermo e spesso richiedono all'utente di effettuare numerosi passaggi per poter registrare singoli eventi sintomatici selezionando opzioni preimpostate senza poter registrare i sintomi in modo diretto. Il tempo e lo sforzo necessari per documentare ogni evento, soprattutto per patologie con sintomatologia complessa, induce l'utente a omettere alcune segnalazioni o ad effettuarle con minor precisione. In questo caso, il ricorso

approfondimenti sulla seconda tipologia di discriminazioni in diversi ambiti si v. G. NOTO LA DIEGA, *Against the Dehumanisation of Decision-Making - Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, 9, 3, 2018, 4, in Rete: https://www.jipitec.eu/issues/jipitec-9-1-2018/4677; per il settore dell'educazione si v. S. BAROCAS, A. D. SELBST, *Big Data's Disparate Impact*, 104 *Calif. L. Rev* 682 (2016), in Rete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899; nel contesto della prevenzione della criminalità negli Stati Uniti si v. F. ZUIDERVEEN BORGESIUS, *Report on discrimination, artificial intelligence, and algorithmic decision-making*, published by the Directorate General of Democracy (Council of Europe), Strasburgo, 2018, 14, in Rete: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73; in tema di protezione sociale e assistenza si v. E. PILKINGTON, *Digital dystopia: how algorithms punish the poor*, *The Guardian*, pubblicato il 14 ottobre 2019, in Rete: https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor.

[13] 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 (c.d. *behavioral health interventions*) supportandolo quotidianamente al fine di incentivare comportamenti che possano ridurre l'impatto della patologia stessa e l'occorrenza di patologie secondarie. Sull'impiego dell'assistente vocale per *behavioral health interventions* si v. E. SEZGIN, L. MILITELLO, Y. HUANG, L. SIMON, *A Scoping Review of Patient-Facing, Behavioral Health Interventions with Voice Assistant Technology Targeting Self-management and Healthy Lifestyle Behaviors*, in *Translational Behavioral Medicine*, 2020, in Rete: https://ssrn.com/abstract=3381183.

[14] Il supporto offerto attraverso l'assistente vocale può riguardare, inoltre, la prevenzione e il monitoraggio delle complicanze più frequenti del diabete, consentendo al personale sanitario di fornire indicazioni tempestive e personalizzate e di responsabilizzare il paziente su tali aspetti della patologia, si v. B. NAJAFI, M. SWERDLOW, G. A. MURPHY, D. G. ARMSTRONG, *Digital foot care – leveraging digital health to extend ulcer-free days in remission*, in D. C. KLONOFF, D. KERR, S. A. MULVANEY (a cura di), *Diabetes Digital Health*, Elsevier, 2020.

al linguaggio naturale e l'immediatezza dell'interazione offerti dall'assistente vocale potrebbero eliminare tali ostacoli oltre a rappresentare, in caso di necessità, uno strumento per ottenere in tempo reale indicazioni su come gestire, ad esempio, delle crisi acute o dei sintomi anomali[15].
L'attenzione verso tali sviluppi è costante anche a livello europeo: da ultimo il progetto "*Phara-On*"[16], finanziato dalla Commissione europea con 21 milioni di euro nell'ambito del programma *Horizon 2020*, si prefigge di assicurare un invecchiamento sano e attivo della popolazione attraverso una serie di piattaforme interoperabili e personalizzabili che integrano servizi, dispositivi e strumenti avanzati come gli assistenti vocali[17].
Il concretizzarsi dell'impiego di queste tecnologie in ambito sanitario richiede una rinnovata attenzione verso il rispetto dei principi che regolano la tutela dei dati personali concentrando il discorso non solo su elementi a carattere generale tipici del trattamento per mezzo di sistemi di Intelligenza Artificiale, ma anche su specifici aspetti propri dell'assistente vocale legati principalmente alla governance e alla sicurezza del trattamento. Su quest'ultimo aspetto si è concentrato il Garante per la Protezione dei Dati Personali (Garante) che nella recente scheda informativa ha indicato una serie di consigli pratici per un uso "*a prova di privacy*" degli smart assistant[18].
Pertanto, per accompagnare gli attuali scenari tecnologici verso uno sviluppo che sia fin da subito conforme alla tutela dei dati personali è necessario interrogarsi in via prodromica sulle principali criticità poste dalle decisioni automatizzate assunte da sistemi di reti neurali e, di seguito, sulle problematiche legate alle caratteristiche precipue dell'assistente vocale, quali la governance e la sicurezza tecnico-organizzativa.

3. Quando a decidere è l'algoritmo

Al centro dello scenario ora descritto si pone l'Intelligenza Artificiale, artefice solitaria di numerose decisioni relative agli esseri umani. La ricerca di un equilibrio tra le prospettive di efficienza ed i timori di una spersonificazione dell'entità nelle cui mani (o, per l'appunto, circuiti) è rimesso il giudizio hanno indotto il legislatore europeo alla redazione dell'articolo 22 GDPR. Questo, infatti, attribuisce 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*

[15] E. SEZGIN ET AL, *Capturing At-Home Health and Care Information for Children With Medical Complexity Using Voice Interactive Technologies: Multi-Stakeholder Viewpoint*, in *J. Med. Internet. Res.*, 22, 2, 2020, in Rete: https://www.jmir.org/2020/2/e14202/.
[16] https://www.pharaon.eu/.
[17] Sull'assistente vocale quale supporto per soggetti anziani, ancor più se affetti da patologie degenerative, si v. M. WOLTERS, F. KELLY, J. KILGOUR, *Designing a spoken dialogue interface to an intelligent cognitive assistant for people with dementia*, in *Health Informatics Journal*, 22, 4, 2015, in Rete: https://www.researchgate.net/publication/281082000_Designing_a_spoken_dialogue_interface_to_an_intelligent_cognitive_assistant_for_people_with_dementia; per un'analisi critica dei rischi dell'impiego di nuove tecnologie a supporto di soggetti anziani, in particolare, in relazione al concetto di autonomia si v. D. L. GOMEZ., E. MANTOVANI, P. DE HERT, *Autonomy in ICT for Older Persons at the Crossroads Between Legal and Care Practices*, in S. GUTWIRTH ET AL. (a cura di), *European Data Protection: Coming of Age*, Springer, 2013, 145 – 159.
[18] Garante per la Protezione dei Dati Personali, *Scheda informativa sugli assistenti digitali (smart assistant): i consigli del Garante per un uso a prova di privacy*, ultima modifica 4 marzo 2020, in Rete: https://www.gpdp.it/web/guest/temi/assistenti-digitali.

analogo significativamente sulla sua persona»[19]. A preoccupare, fin dalla Direttiva 95/46/CE[20], è sempre stata la crescente riduzione del ruolo del soggetto umano nell'assunzione di decisioni aventi conseguenze significative per il destinatario delle stesse[21]. Tale fenomeno prospetta da un lato il diffondersi di una fiducia quasi cieca nell'azione della macchina, fiducia che potrebbe portare l'individuo ad accettare acriticamente la determinazione, dall'altro la potenziale violazione della dignità umana e dei diritti e libertà fondamentali dell'uomo[22].

L'interpretazione dell'articolo 22 pone diverse criticità sotto più aspetti rendendo la disciplina spigolosa e, talvolta, di difficile applicazione. Ancor più complessa è l'opera ermeneutica in caso di trattamenti posti in essere con mezzi tecnologici avanzati in un contesto sensibile quale quello sanitario[23]. Di conseguenza, per poter valutare la tenuta del Regolamento davanti a queste sfide, è essenziale inquadrarne i presupposti applicativi e vagliare l'efficacia delle tutele.

Per essere soggetta al divieto ex articolo 22.1[24], la decisione deve essere unicamente basata sul trattamento automatizzato e deve produrre effetti giuridici nella sfera dell'interessato o incidere in modo analogo significativamente sulla sua persona[25]. Tale proibizione è mitigata, però, dal secondo comma che introduce delle basi legali che legittimano il processo decisionale automatizzato[26]. Per quanto riguarda il trattamento che coinvolga categorie particolari di dati, questo sarà ammesso solo se necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare o laddove si basi sul

[19] Dal primo comma dell'articolo 22 ora citato emerge la stretta relazione che intercorre tra il processo decisionale automatizzato e la profilazione, tuttavia, tali fenomeni, per quanto connessi, non sono necessariamente compresenti, potendo la decisione automatizzata includerla o meno.

[20] Cfr. art. 15 (rubricato "*Decisioni individuali automatizzate*"), Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Direttiva 95/46/CE).

[21] Si legge nella Proposta della Direttiva 95/46: «*This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his "data shadow"*» (Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final – SYN 287, 13.9.1990, 29). Si v. L. A. BYGRAVE, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in *Computer Law & Security Review*, 17, 2001, 18.

[22] BYGRAVE, *op. cit.*

[23] Per un approfondimento critico in materia si v. P. GUARDA, *"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation*, in *BioLaw Journal*, 2019, 359-375, in Rete: http://www.biodiritto.org/ojs/index.php?journal=biolaw&page=article&op=view&path%5B%5D=369.

[24] È stato sostenuto che il primo comma non sancisse un divieto, bensì un "diritto in negativo", tuttavia tale interpretazione è stata definitivamente rigettata in seguito all'esplicita affermazione da parte del Working Party 29 della sussistenza di un «*divieto generale*». Si v. Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 206/679, adottate il 3 ottobre 2017, emendate in data 6 febbraio 2018, WP 251 rev.01, (Linee Guida).

[25] E. PELINO, *I diritti dell'interessato*, in L. BOLOGNINI, C. BISTOLFI, E. PELINO (a cura di), *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 270.

[26] Le quali consistono, schematicamente, nella necessità per la conclusione o l'esecuzione di un contratto tra titolare e interessato, nell'autorizzazione disposta dal diritto dello Stato Membro o dell'Unione purché siano attuate apposite misure a tutela dell'interessato e nel consenso esplicito dell'interessato.

consenso esplicito; inoltre, misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato dovranno essere attuate dal titolare.

Fondamentale per la corretta definizione dell'ambito applicativo di tale norma (e in seguito per lo studio dell'efficacia delle tutele) è l'individuazione del significato di decisione *unicamente basata* su un processo automatizzato[27]. È da rigettare la lettura che esclude l'applicazione della disciplina ex articolo 22 laddove sia integrato un qualsiasi intervento umano all'interno del processo decisionale. Tale interpretazione, infatti, consentirebbe di aggirare la previsione del GDPR inserendo nel processo un intervento umano meramente formale e fittizio[28]. 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, cosicché l'eventuale intervento umano limitato ad una presenza formale nulla muterebbe rispetto al fatto che la decisione sia stata assunta *unicamente* su dette *basi*[29]. A fare ulteriore chiarezza sono le Linee Guida secondo cui «*se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico*»[30]. Punto di riferimento, allora, è il *tipo* di coinvolgimento umano, e non la sua sola sussistenza, il quale deve essere caratterizzato necessariamente dall'autorità e dalla competenza del soggetto chiamato a intervenire affinché questi possa effettivamente modificare la decisione[31]. Ora, non si hanno difficoltà a immaginare un coinvolgimento umano avente tali qualità fintanto che le tecnologie utilizzate sono rudimentali e di facile comprensione. Le criticità sorgono nel momento in cui si prendono in considerazione tecnologie più avanzate le cui logiche divengono complesse, se non del tutto oscure. A vacillare davanti a fenomeni come quello dell'Intelligenza Artificiale sono proprio i concetti di competenza e autorità.

La riflessione appena svolta è strumento imprescindibile non solo per delineare l'ambito di applicazione dell'articolo 22, ma anche per valutare l'efficacia delle tutele che questo garantisce all'interessato in caso di decisione automatizzata legittimamente assunta dall'assistente vocale. Nello specifico, il terzo comma menziona il diritto di esprimere la propria opinione, di contestare la decisione e di

[27] In merito alla produzione di effetti sulla sfera giuridica dell'interessato, altro presupposto per l'applicazione dell'articolo 22, questa è intrinseca nel momento in cui si prendano in considerazione gli scenari descritti nel precedente paragrafo.

[28] Malgieri e Comandé si chiedono, provocatoriamente, se allora non si possa ritenere sufficiente l'intervento di un animale ben addestrato capace di apporre un timbro ad una decisione come farebbe un umano. Si v.G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 4, 2017, 251, in Rete: https://academic.oup.com/idpl/article-abstract/7/4/243/4626991. Dello stesso avviso: S. HÄNOLD, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings,* in M. CORRALES ET AL.(a cura di), *Robotics, AI and the Future of Law*, Singapore, 2018, 133, in Rete: https://doi.org/10.1007/978-981-13-2874-9_6; M. VEALE, L. EDWARDS, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in *Computer Law & Security Review,* 34, 2, 2018, 400, in Rete: https://strathprints.strath.ac.uk/62844/.

[29] G. MALGIERI, G. COMANDÉ, *op. cit.*

[30] Linee Guida, 23.

[31] Linee Guida, 23.

ottenere l'intervento umano[32], ma riguardo alla concreta realizzabilità ed effettività di quest'ultimo si pongono diversi interrogativi, soprattutto quando ad intervenire sia un medico. In primo luogo deve essere evidenziata una generale difficoltà tecnica nell'integrare la possibilità per l'interessato di richiedere l'intervento umano attraverso un mezzo progettato per essere in grado di agire e assumere determinazioni in autonomia come il vocal assistant. Ulteriori aspetti emergono in rapporto al fatto che la decisione si muoverà sui binari della scienza medica e che il soggetto chiamato a intervenire sarà, di conseguenza, un professionista del settore. Deve essere preso in considerazione, infatti, l'approccio di quest'ultimo nei confronti di una decisione assunta da un oggetto concepito e istruito al fine di sostituirglisi. In un primo scenario, il professionista potrebbe essere guidato da diffidenza e ostilità tendendo a contrapporsi *a priori* alla decisione assunta dal sistema[33]. In una seconda ipotesi, il medico potrebbe riporre eccessivo affidamento sulla determinazione meccanica[34]. Ciò potrebbe derivare dalla sua scarsa esperienza o, in generale, dalla soggezione nei confronti di un algoritmo avanzato, addestrato per mezzo di innumerevoli dati secondo criteri forniti da grandi esponenti del settore medico e, ipoteticamente, frutto di un investimento economico ingente per l'ospedale[35]. Non da meno, l'attendibilità (e utilità) dei risultati dipende anche dal *gold standard* scelto dai programmatori, ossia dal test di riferimento rispetto al quale diviene misurabile l'accuratezza di un secondo test diagnostico che si intende valutare (se ne dedurrà una maggiore o minore affidabilità dell'algoritmo)[36]. 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.

Inoltre, qualora il medico chiamato a riesaminare la decisione la dovesse ritenere errata si troverà davanti ad un bivio: potrà ufficializzare la sua posizione dovendone giustificare scientificamente i motivi e assumendosene la responsabilità, oppure, potrà adottare un approccio indulgente e assecondare il sistema. Per quanto il dilemma sembri di facile risoluzione agli occhi di un professionista fedele

[32] Sebbene tale livello minimo di tutela sia esplicitamente previsto solo per le decisioni assunte sulla base dell'art. 22.2 lettere a) e c), si ritiene che in caso di trattamento di dati particolari sia opportuno garantire almeno il medesimo standard adottato per i c.d. dati comuni.

[33] F. CABITZA, *Breeding electric zebras in the fields of Medicine*, *HUML 2016: Proceedings of the IEEE workshop on the Human Use of Machine Learning*, 2017, in Rete: https://www.academia.edu/33155120/Breeding_electric_zebras_in_the_fields_of_Medicine.

[34] In un'ottica non limitata al solo campo medico si v. T. ZARSKY, *Transparent predictions,* 4 *U. Ill. L. Rev.* 1552 (2013), in Rete: https://www.illinoislawreview.org/wp-content/ilr-content/articles/2013/4/Zarsky.pdf; F. CABITZA, *op. cit.*

[35] I due scenari costituiscono l'applicazione al settore sanitario del c.d. *automation bias*, ossia un fenomeno psicologico che induce il soggetto a fare troppo o troppo poco affidamento su un sistema decisionale. Si v. L. EDWARDS, M. VEALE, *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, 16 *Duke Law & Technology Review* 1 (2017).

[36] F. CABITZA, C. ALDERIGHI, R. RASOINI, G. F. GENSINI, *Potenziali conseguenze inattese dell'uso di sistemi di intelligenza artificiale oracolari in medicina*, in *Recenti Prog Med*, 108, 2017, 400, in Rete: https://recentiprogressi.it/r.php?v=2802&a=28353&l=332398&f=allegati/02802_2017_10/fulltext/04_Prospettive%20-%20Cabitza.pdf.

all'etica e alla deontologia, non si può negare l'attuale tendenza alla c.d. medicina difensiva che potrebbe indurre il medico a scegliere l'opzione più plausibile tra quelle idonee a supportare la decisione dell'algoritmo, seppur non coincida con quella che ritiene essere la migliore[37].

Infine, lo specialista sanitario che interverrà dovrà sempre avere la competenza e l'autorità per mettere in discussione la decisione e, se del caso, modificarla. Tornano, dunque, i due elementi individuati dal Working Party al fine di garantire un intervento non fittizio. Nel caso dell'Intelligenza Artificiale, e in particolare delle reti neurali, sarà sempre meno probabile che il professionista sia dotato di tali qualità poiché caratteristica principale del processo logico seguito dall'algoritmo è l'opacità, c.d. black box issue[38]. Così sarà necessario ricercare dei sistemi che siano dotati di un livello di trasparenza che consenta la valutazione dell'intero processo decisionale, anche alla luce dell'articolo 12 GDPR che sancisce esplicitamente il principio di trasparenza, pilastro del trattamento dei dati personali[39]. Questo approccio è necessario per ottemperare anche ad un altro obbligo gravante sul titolare del trattamento, ossia quello di fornire all'interessato «*informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*»[40].

Tali considerazioni inducono a vagliare con attenzione l'atteggiamento di fiducia da parte del legislatore europeo nei confronti dell'intervento umano nel processo decisionale automatizzato, soprattutto se applicato all'ambito sanitario. La perfettibilità è una caratteristica propria non solo della macchina, ma anche dell'uomo, e prendere coscienza dell'impatto psicologico e prestazionale che l'automazione ha su colui che dovrebbe essere chiamato a giudicarne la validità rappresenta il primo passo verso la configurazione di tutele che si rivelino efficaci quando sia un algoritmo a decidere.

---

[37] F. CABITZA, *op. cit.*

[38] L'algoritmo non consente l'accesso alle logiche interne rendendo intelligibili solo gli *output*, e non il percorso seguito a partire dall'*input*. Si v. F. PASQUALE, *Black Box Society. The Secret Algorithms That Control Money and Information*, *Harvard University Press*, Cambridge – Massachusetts, 2015, in Rete: http://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf. Per una descrizione del concetto di *black box* si v. anche G. NOTO LA DIEGA, *op. cit.*, 9-10.

[39] Si segnala che un interessante progetto di Google volto a garantire forme di IA più trasparenti e comprensibili all'uomo è parzialmente ispirato ad una teoria sviluppata in ambito giuridico a partire dalle esigenze di tutela dei dati personali, c.d. *counterfactuals explanation*, https://pair-code.github.io/what-if-tool/index.html#about . Si v. S. WACHTER, B. MITTELSTADT, C. RUSSELL, *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, 31 *Harvard Journal of Law & Technology* 841-887 (2018), in Rete: https://arxiv.org/abs/1711.00399.

[40] Artt. 13.2.f) e 14.2.g) GDPR. Non potendo dar conto in questa sede del pur fondamentale dibattito che vede contrapposti gli autori che sostengono la sussistenza del solo diritto all'informazione e quelli che affermano un più ampio diritto alla spiegazione, si rimanda per la prima teoria a. S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2017, 95, in Rete: https://academic.oup.com/idpl/article/7/2/76/3860948; per la seconda teoria a B. GOODMAN, S. FLAXMAN, *European Union regulations on algorithmic decision-making and a "right to explanation"*, *ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)*, New York (2016), in Rete: https://arxiv.org/abs/1606.08813; G. NOTO LA DIEGA, *op. cit.*; G. MALGIERI, G. COMANDÉ, *op. cit.*; A. D. SELBST, J. POWLES, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 7, 4, 2017, 236, in Rete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125 .

4. Le misure di sicurezza: un quadro complesso

Nel momento in cui si ricorre all'assistente vocale per il trattamento di dati sanitari, l'analisi giuridica non può limitarsi all'articolo 22 GDPR. Imprescindibile, infatti, è il riferimento all'articolo 5 GDPR che sancisce i principi del trattamento[41] e introduce il concetto di accountability: il titolare è competente per il rispetto di questi e deve essere in grado di comprovarne l'ottemperanza. Si potrebbe dire, in tal senso, che l'accountability costituisce il *principio dei principi*[42] e ha il pregio di portare l'attenzione del titolare su determinati risultati da raggiungere in termini di tutela dei dati affinché gli obblighi giuridici si traducano in misure di protezione verificabili nei fatti[43].

Pertanto, la responsabilizzazione, così configurata, svolge un ruolo fondamentale nel discorso relativo ai processi decisionali automatizzati quali trattamenti che espongono l'interessato a gravi rischi. Questi non sarà tutelato solo dall'attribuzione di specifici diritti[44], ma anche da un generale e prodromico obbligo per il titolare di attivarsi concretamente adottando misure adeguate al livello di rischio per conformare il trattamento agli standard introdotti dal GDPR. Tra questi, assume particolare rilevanza il principio di sicurezza («*integrità e riservatezza*» ex articolo 5.1 GDPR) così come specificato dall'articolo 32 GDPR che, sulla falsariga dell'articolo 24.1, individua i parametri fondamentali per valutare l'adeguatezza delle misure tecniche e organizzative da adottare e ne elenca alcuni esempi. È proprio in rapporto alle misure di sicurezza che il concetto stesso di AAL genera forti criticità applicative[45], prospettando specifici scenari di rischio legati alle caratteristiche principali del vocal assistant. Per quanto riguarda le misure di sicurezza organizzative, il trattamento dei dati attraverso applicazioni progettate per gli assistenti vocali come Alexa o Google Home implica la necessità di trovare una coerente configurazione della governance del trattamento per il rapporto tra fornitori di servizi cloud e sviluppatori di applicazioni. In merito alle misure di sicurezza tecniche, il ruolo della voce nell'interazione con l'assistente comporta sì una facilità di utilizzo, ma rende maggiormente vulnerabile lo strumento di fronte a malfunzionamenti e attacchi esterni.

[41] L'art. 5.1 GDPR fa riferimento ai principi di: liceità, correttezza e trasparenza (lett. a)), limitazione della finalità (lett. b)), minimizzazione dei dati (lett. c)), esattezza (lett. d)), limitazione della conservazione (lett. e)) e integrità e riservatezza (lett. f)).

[42] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Le obbligazioni di compliance in materia di protezione dei dati*, in L. BOLOGNINI, C. BISTOLFI, E. PELINO, (a cura di), *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 324.

[43] I caratteri dell'accountability sono definiti dall'articolo 24.1 GDPR, rubricato per l'appunto «*Responsabilità del titolare del trattamento*»: *«Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario»*. *Ibid.*, 325.

[44] Si faccia riferimento al già ampiamente discusso art. 22.3 GDPR, nonché agli artt. 13.2.f), 14.2.g), 15.1.h) GDPR.

[45] La questione della scarsa sicurezza degli oggetti connessi alla Rete è stata più volte sollevata fino a portare taluni a sostenere che questi non siano stati congegnati pensando alla sicurezza, lasciata in secondo piano. Tra i molti, si v. S. R. PEPPET, *Regulating the Internet of Things: first steps toward managing discrimination, privacy, security and consent*, 93 *Texas Law Review* 133 (2014), in Rete: https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf.

Nello sviluppare questi due aspetti si è rivelato imprescindibile l'impiego di un approccio by design affinché tanto la governance quanto la progettazione tecnica siano concepiti *ab origine* per essere conformi ai principi del trattamento dei dati personali.
I concetti di data protection by design e by default sono introdotti dallo stesso Regolamento all'articolo 25: la protezione per impostazione predefinita (by default) si sostanzia in quelle misure funzionali a garantire che vengano trattati solo i dati personali necessari alle finalità perseguite, mentre la protezione fin dalla progettazione (by design) comporta la creazione di prodotti e servizi che tengano conto sin dalla loro ideazione delle previsioni a tutela dei dati personali[46]. È interessante notare come la previsione esplicita di queste misure segni un cambiamento di prospettiva rispetto al passato, in cui era adottato un approccio "difensivo" verso i rischi derivanti dall'utilizzo degli strumenti tecnologici per il trattamento dei dati personali[47]. Tale nuovo indirizzo mostra la via da seguire laddove si intenda sviluppare un'app per assistente vocale a supporto del paziente: la tecnologia avanzata implica delle criticità specifiche, ma è in questa stessa che si può ricercare la soluzione per garantire all'interessato i propri diritti e libertà.
Muovendo da tale presupposto nel prosieguo della trattazione si analizzeranno in primo luogo le misure organizzative con le problematiche connesse alla gestione dei ruoli privacy in scenari cloud ed in secondo luogo le misure tecniche evidenziando criticità e possibili soluzioni che i sistemi di autenticazione vocale presentano.

4.1 Misure di sicurezza organizzative: un gioco di ruoli

L'articolo 32 GDPR alla lettera d) del primo comma suggerisce l'adozione di una «*procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*». Tale ipotesi ha carattere organizzativo-procedurale e si rivela particolarmente adatta a garantire la sicurezza dei trattamenti che utilizzino l'Intelligenza Artificiale, o più in generale sistemi cloud[48]. La garanzia di una verifica costante delle misure di sicurezza adottate ha un duplice scopo: da un lato tutela lo svolgersi del trattamento e gli interessi dei soggetti coinvolti, dall'altro assicura che, laddove si ricorra ad una serie di trattamenti collegati che si sviluppano in sequenza, ogni anello della catena sia sempre dotato di misure a tutela della sicurezza e non comporti rischi per le fasi successive[49]. Ne consegue che il titolare dovrà preoccuparsi di verificare che anche gli altri servizi di cui eventualmente si avvalga non solo adottino misure di sicurezza adeguate, ma predispongano anche accorgimenti per assicurarne una costante disponibilità ed efficacia.

[46] L. Bolognini, E. Pelino, C. Bistolfi, *op. cit.,* 324, 401; F. Bravo, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *op. cit.,* 835.
[47] F. Bravo, *op. cit.,* 790; A. Principato, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contr. e impr./Europa*, 2015, 197 ss.
[48] F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 132.
[49] *Ibid*.

Sempre sul piano organizzativo, l'articolo 32 menziona la possibilità di aderire a codici di condotta e di ottenere una certificazione, nonché l'obbligo di formare i soggetti autorizzati a trattare i dati personali[50] finalizzato sia a istruirli sull'attività da svolgere sia a renderli edotti dei potenziali rischi connessi[51]. Quest'ultima disposizione pone l'accento sul rapporto tra il titolare e gli altri soggetti preposti al trattamento, in particolare il responsabile, e offre l'occasione per riflettere sull'importanza che le scelte di governance assumono anche in materia di sicurezza. Certamente l'individuazione del responsabile è in primo luogo una forma di accountability[52], in quanto la conformità al Regolamento non può prescindere dalle pratiche e dai valori di un'organizzazione e quindi passa anche attraverso la ripartizione delle responsabilità[53]. Ciononostante, il considerando 81 GDPR supera la generale dimensione della responsabilizzazione e associa specificamente la valutazione delle garanzie offerte dal responsabile all'implementazione di misure di sicurezza: «*[…] il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento*». Il responsabile del trattamento, infatti, deve essere in grado di adempiere agli obblighi di adottare le misure previste dall'articolo 32[54] e di assistere il titolare nel garantire il rispetto degli articoli da 32 a 36[55].

Muovendo ancora dal considerando 81 GDPR, può essere sviluppata un'ulteriore riflessione volta a precisare il raggio d'azione della data protection by design quale misura di sicurezza tecnica. L'articolo 25 del Regolamento fa esplicito riferimento solo alla figura del titolare quale soggetto tenuto a implementare forme di protezione fin dalla progettazione, facendo sorgere delle perplessità applicative relativamente al responsabile, assente dalla lettera della norma. Ciò ha particolare rilievo nel caso in cui quest'ultimo sia il produttore dello strumento tecnologico di cui il titolare intende avvalersi ai fini del trattamento: l'obbligo di predisporre, sin dalla progettazione, un sistema *privacy-compliant* non sarebbe applicabile proprio al soggetto che avrebbe la possibilità concreta di adempierlo, ossia il produttore (o *designer*). Ad offrire una via d'uscita da questa *impasse* è, per l'appunto, il considerando 81 GDPR, anche alla luce degli articoli 24.1 e 28.3.c). Dal momento che il titolare è tenuto a ricorrere a responsabili che presentino sufficienti garanzie per la sicurezza del trattamento, e considerando che quest'ultima è assicurata anche dalla data protection by design (soprattutto in contesti tecnologici avanzati), il titolare che scelga come responsabile del trattamento il produttore di un sistema privo di

[50] Art. 32.4 GDPR.

[51] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.,* 328.

[52] «*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*», art. 28.1 GDPR.

[53] A conferma di ciò il considerando n. 79 lega la tutela dei diritti e delle libertà dell'interessato e la responsabilità generale del titolare e del responsabile ad una «*chiara ripartizione delle responsabilità*». Si v. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.,* 328.

[54] Art. 28.3.c) GDPR.

[55] Art. 28.3.f) GDPR.

forme di protezione *ab origine* violerà gli obblighi impostigli dal GDPR a tutela della sicurezza[56]. Pertanto, il titolare del trattamento dei dati sanitari dovrà ponderare accuratamente la scelta del soggetto produttore dell'assistente vocale e responsabile del trattamento valutando, alla luce dei rischi, le concrete possibilità per quest'ultimo di assicurare l'integrazione nel *device* di misure di sicurezza adeguate e la loro attuazione.

In via prodromica, però, deve essere analizzato l'aspetto relativo alla corretta individuazione dei ruoli di titolare e responsabile e sull'atto di designazione laddove il *device* in questione implichi il ricorso a sistemi cloud. Il *cloud computing* è costituito da un insieme di tecnologie *hardware* e *software* collegate in Rete tramite cui il *cloud provider* offre l'erogazione online di servizi di gestione, memorizzazione, archiviazione e/o elaborazione di dati[57]. Un esempio è fornito proprio dalle applicazioni destinate agli assistenti vocali: i produttori dell'assistente consentono a terze parti di sviluppare delle *skills*[58] che potranno essere utilizzate dagli utenti per mezzo degli assistenti vocali[59]. In questo caso non è facile configurare quale sia il rapporto tra il fornitore del servizio cloud[60] e lo sviluppatore della *skill* dal punto di vista della disciplina a tutela dei dati personali. Un punto di riferimento per procedere nell'analisi è fornito dal Working Party che, in via generale, ha individuato nel fruitore del servizio cloud il titolare del trattamento e nel *cloud provider* il responsabile[61]: «*The cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller. […] When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor*»[62]. Nella maggior parte dei casi[63], infatti, è lo sviluppatore della *skill* a determinare autonomamente i mezzi e le finalità del trattamento, mentre il fornitore del servizio cloud non partecipa a tale determinazione.

[56] Medesimo ragionamento può essere fatto nel caso in cui il titolare utilizzi un dispositivo prodotto da un soggetto che rimane estraneo al trattamento (ossia privo della qualifica di responsabile). In tal caso il titolare violerà gli obblighi di sicurezza non in forza dell'individuazione di un responsabile privo delle garanzie necessarie, ma in ragione della scelta di mezzi non adeguati a garantire la sicurezza del trattamento. Si v. F. BRAVO, op. cit., 835-836; E. COVELLO, *La privacy by design nel rapporto tra titolare e responsabile del trattamento dati: le soluzioni*, NetworkDigital360, pubblicato il 21 marzo 2019, in Rete: https://www.cybersecurity360.it/legal/privacy-dati-personali/la-privacy-by-design-nel-rapporto-tra-titolare-e-responsabile-del-trattamento-dati-le-soluzioni/.

[57] L. GRECO, *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 276. Per le diverse tipologie di servizi che il cloud provider può fornire (SaaS, DaaS, HaaS, PaaS), si v. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design*, Torino, 2017, 207-208.

[58] Con il termine skill si suole indicare una applicazione per l'assistente vocale, in particolare nel caso di Alexa. Si v. A. PFEIFLE, *op. cit*. Relativamente alla possibilità per terze parti di creare delle skills: https://developer.amazon.com/it-IT/alexa/alexa-skills-kit#Ready%20to%20start%3F.

[59] M. B. HOY, *op. cit.*

[60] Di seguito si farà riferimento al produttore dell'assistente vocale e al fornitore del servizio cloud identificandoli nello stesso soggetto in quanto ciò rispecchia lo scenario attuale, almeno per quanto riguarda i major players del settore (ad esempio Amazon e Google).

[61] Art. 29 WP, Opinion 05/2012 on cloud computing, adopted on 1 July 2012, WP196.

[62] Art. 29 WP, Opinion 05/2012 on cloud computing, 8-9.

[63] Sarà sempre necessario verificare di volta in volta quale sia la relazione che ciascun autore del trattamento instaura con i dati per attribuire le qualifiche che più rispecchiano la reale situazione di fatto. Per degli indici

Identificato il rapporto tra fruitore e fornitore del cloud (nel caso in analisi, sviluppatore della *skill* e produttore dell'assistente vocale), si può procedere ad esaminare lo scenario che la concreta designazione a responsabile prospetta in tale contesto. In primo luogo, lo sviluppatore dovrà scegliere un fornitore che presenti garanzie sufficienti per mettere in atto misure di sicurezza adeguate. Ciò comporterà un onere significativo per il titolare, che dovrà infatti assicurarsi che il responsabile abbia predisposto delle procedure interne in grado di gestire problematiche tecniche di elevata complessità: in caso di violazione dei dati sulla piattaforma cloud sarà il fornitore a dover individuare la criticità, porvi rimedio e notificare l'accaduto al titolare[64]. Più in generale, da un lato il responsabile dovrà riuscire ad implementare le specifiche misure ex articolo 32 GDPR affinché siano adeguate ai sistemi interconnessi e intelligenti, che presentano particolari vulnerabilità e logiche opache; dall'altro, il titolare dovrà avere le competenze tecniche per comprendere se tali misure siano effettivamente adeguate.

In secondo luogo, una volta individuato un responsabile che risponda a tali requisiti, questi dovrà essere formalmente designato, dal momento che il Regolamento non ammette che un soggetto rivesta tale ruolo in assenza di un titolo che disciplini il suo rapporto con il titolare in modo dettagliato[65]. Il dovere di regolare con precisione i caratteri del trattamento svolto dal responsabile offre al titolare la possibilità di porre in essere ulteriori misure di sicurezza organizzative che vanno al di là dell'individuazione del responsabile in sé. In tal modo, infatti, egli potrà limitare il più possibile l'autonomia del fornitore del cloud affinché questo non svolga altro ruolo se non quello di supporto tecnologico per le sole finalità e con le sole modalità fissate dallo sviluppatore. Si dia il caso di un titolare che ponga in essere il trattamento di dati sanitari e che per far ciò si avvalga di un fornitore cloud: nell'atto di designazione dovrà stabilire che quest'ultimo non possa utilizzare i dati trattati per monitorare le preferenze dell'utente o per finalità di marketing. Così il titolare potrà scongiurare a monte, attraverso un approccio organizzativo by design, un uso improprio dei dati sanitari trattati[66], a cui tra l'altro è riservata una tutela particolarmente elevata. Rispetto a tale possibilità, però, si deve prendere in considerazione il fatto che i contratti di erogazione di servizi cloud di questo genere hanno solitamente la struttura dei contratti standard con clausole scarsamente negoziabili e personalizzabili riguardo alle modalità della prestazione del servizio e alle misure di sicurezza[67]. Di conseguenza, l'asimmetria nel potere contrattuale potrebbe impedire al titolare di predisporre, per mezzo del contenuto dell'atto di designazione, misure di tal genere a tutela del trattamento svolto con un sistema intelligente. Resta comunque fondamentale sensibilizzare gli sviluppatori di app destinate all'ambito sanitario all'importanza di una configurazione *ab origine privacy-compliant* poiché ciò può portarli a scegliere con maggior attenzione il produttore di assistenti vocali da designare quale responsabile, prediligendo quello

d'ausilio nella verifica del ruolo del fornitore quale responsabile si v. A. MANTELERO, Il cloud computing, in Panetta (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Milano, 2019, 518-521.

[64] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.,* 339.

[65] L'articolo 28.3 GDPR dispone che: «*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento […]*». Sono previsti, inoltre, vincoli sia sulla forma (scritta) e sul contenuto (minuziosamente elencato nel prosieguo dell'articolo 28.3).

[66] Laddove il responsabile dovesse procedere al trattamento dei dati per finalità proprie non previste dall'atto di designazione sarà considerato titolare autonomo con le relative responsabilità. Art. 28.10 GDPR.

[67] A. MANTELERO*, op. cit.*, 521.

che si dimostri maggiormente in linea con i principi del Regolamento e aperto ad una personalizzazione, seppur parziale, dell'atto di designazione [68].

4.2 Misure di sicurezza tecniche: implicazioni e potenzialità dell'uso della voce

Come descritto sopra l'articolo 32 GDPR indica in primo luogo i parametri fondamentali per valutare l'adeguatezza delle misure da adottare: si dovrà tener conto «*dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*». In secondo luogo, la disposizione individua un elenco non esaustivo di misure idonee a garantire la sicurezza del trattamento, come la pseudonimizzazione e la cifratura[69]. Tra le misure tecniche, inoltre, possono essere inserite quelle ex articolo 25 GDPR, già oggetto di trattazione nei precedenti paragrafi.
Nel caso in cui il titolare intenda trattare dati sanitari ricorrendo ad un assistente vocale, egli dovrà, quindi, concentrarsi da un lato sui rischi legati alle caratteristiche dei dati stessi[70], dall'altro sulle vulnerabilità proprie di un sistema che ruota intorno alla voce. Il fatto che l'assistente, quale nodo centrale nella rete degli oggetti intelligenti, possa essere attivato mediante la pronuncia da parte di qualsiasi individuo di una wake word, espone un numero significativo di dati personali al pericolo di comunicazione a soggetti indistinti. Tale accessibilità indiscriminata è dovuta al fatto che il software di riconoscimento vocale[71] è progettato per attivare il sistema principale solo laddove tra i diversi rumori ambientali venga registrato un *input* vocale che sia riconosciuto come corrispondente, appunto, alla wake

[68] Inoltre, in ragione della localizzazione dei principali players del settore, la scelta di avvalersi di fornitori di servizi cloud implica tendenzialmente il venire in essere di flussi transfrontalieri di dati. In virtù del dettato degli articoli 44 e seguenti del Regolamento, al di fuori dei casi in cui il Paese di destinazione offra un livello di tutela ritenuto adeguato dalla Commissione europea o sussistano altri specifici strumenti di tutela ad hoc, le parti dovranno ricorrere a soluzioni contrattuali che risentiranno anch'esse dell'asimmetria ora descritta. *Ibidem*, 525-526; L. GRECO, *op. cit.,* 276-277. Per una più ampia trattazione in tema di trasferimento di dati personali verso paesi terzi si v. M. C. MENEGHETTI, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in G. FINOCCHIARO (a cura di), *op. cit.,* 423-485; F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in V. CUFFARO, R. D'ORAZIO, D. RICCIUTO (a cura di), *op. cit.,* 961-982.
[69] Nell'elenco compaiono anche la «*capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*» (art. 32.1.b)) e la «*capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico e tecnico*» (art. 32.1.c)). Seppur tali previsioni configurino in realtà degli obiettivi a cui tendere, rischiando di confondere mezzi e fini, non si può non constatare la loro importanza nell'ambito dei sistemi di Intelligenza Artificiale. La prima vuole assicurare la qualità e l'accessibilità dei dati (contro eventuali *bias* e/o utilizzo improprio dei dati). La seconda ha un ruolo centrale nel caso dei trattamenti interconnessi tipici dei sistemi di Intelligenza Artificiale, poiché la lunghezza della catena dei trattamenti e la loro connessione può richiedere tempi di ripristino molto variabili che possono avere conseguenze critiche in determinate situazioni, si pensi ad un incidente tecnico che renda indisponibili i dati utilizzati da un device destinato al controllo dei livelli di insulina nel sangue e al conseguente rilascio di tale sostanza. SI v. F. GIOVANELLA, *op. cit*., 1223-1224; F. BRAVO, *op. cit.*, 805-806; F. PIZZETTI, *op. cit*., 132.
[70] Come si è visto il trattamento di dati particolari è infatti idonei ad esporre l'interessato a gravi pericoli soprattutto in caso di processi decisionali automatizzati.
[71] Si fa riferimento a tecniche di riconoscimento vocali *speaker-independent*, ossia progettate per riconoscere cosa è detto, ma non da chi.

word[72]. In caso di mera attivazione (e non autenticazione) mediante una parola predefinita, il sistema non prende in considerazione chi sia il soggetto che l'ha pronunciata, concentrandosi solo sulla sua rispondenza al modello di riferimento. Laddove vi sia esito positivo, il comando assegnato verrà eseguito avviando un'applicazione o svolgendo una diversa azione richiesta[73].

Un'ulteriore debolezza è rappresentata dalla possibilità di un malfunzionamento che induca l'identificazione come wake word di un termine solo similare, ma non corrispondente. Ciò comporta che l'accesso, e dunque la facoltà di impartire un comando, sia accordato addirittura a soggetti che non hanno nemmeno posto in essere un tentativo di interazione con l'assistente e si trovino semplicemente a parlare nelle sue prossimità[74]. Non meno rilevante è lo scenario in cui le falle nel processo di riconoscimento vocale *speaker-independent* siano sfruttate da terzi soggetti per programmare un attacco finalizzato alla violazione dei dati[75].

Di fronte a tali criticità, una possibile misura di sicurezza volta ad arginare il problema dell'accesso indiscriminato è quella dell'autenticazione[76] vocale (e non più mero riconoscimento). Da ciò emerge

[72] Tale parte del processo di attivazione vocale è stata spesso oggetto di critiche poiché comporta che l'assistente vocale sia sempre in ascolto e dunque potenzialmente in grado di registrare tutti i rumori, comprese le conversazioni, senza il bisogno che il processo di attivazione sia completato (o neppure iniziato). Si v. M. B. HOY, *op. cit.*, 85; A. RUSSAKOVSKII, *Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7*, pubblicato il 10 ottobre 2017, in Rete: https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/. Per un interessante esperimento condotto su un dispositivo *Echo Dots* che ha dimostrato l'avvenuta registrazione di parziali conversazioni senza che fosse stata pronunciata la wake word si v. M. FORD, W. PALMER, *Alexa, are you listening to me? An analysis of Alexa voice service network traffic*, in *Personal and Ubiquitous Computing*, 23, 2019, 67-79, in Rete: https://doi.org/10.1007/s00779-018-1174-x.

[73] Ciò può dar vita a situazioni inaspettate, com'è accaduto, ad esempio, a San Diego, dove alcuni proprietari di un *Amazon Echo device* hanno ricevuto una notifica da parte di Amazon relativamente al tentativo di acquisto di una casa per le bambole pur non avendo mai impartito il relativo comando. Ad aver effettuato l'ordine, in realtà, è stato un giornalista televisivo che, nel riportare una notizia riguardo all'acquisto su Amazon, ha pronunciato la frase «*I love the little girl, saying 'Alexa order me a dollhouse'*» attivando i dispositivi di coloro che stavano guardando il programma. Si v. A. LIPTAK, *Amazon's Alexa started ordering people dollhouse after hearing its name on TV*, *The Verge*, pubblicato il 7 gennaio 2017, in Rete: https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.

[74] Si deve considerare, poi, che il medesimo rischio di accesso indiscriminato (*rectius* comunicazione) è riferibile al caso in cui si chieda all'assistente vocale di ricordare qualcosa all'utente in via automatica ad un determinato momento senza poter prevedere a monte chi assisterà all'esecuzione del comando. Se è vero che vi sono dei promemoria a contenuto informativo tendenzialmente neutro, è altrettanto vero che l'utilizzo di questa opzione per ricordare di assumere una medicina o di recarsi ad una visita medica implica la comunicazione di dati sanitari dell'interessato a tutti i presenti. In questo caso il tentativo di tutelare i dati personali senza inficiare i benefici di un simile *reminder* risulta complesso, in quanto il principale vantaggio sta proprio nell'attivazione automatica e nel carattere vocale.

[75] Alcune tipologie di attacchi ricorrono a suoni udibili ma non comprensibili, oppure a ultrasuoni, in modo da essere impossibili da percepire per la persona. Si v. E. ALEPIS, C. PATSAKIS, *Monkey Says, Monkey Does: Security and Privacy on Voice Assistants*, in *IEEE Access*, 5, 2017, 17842, in Rete: https://ieeexplore.ieee.org/document/8023746?denied=; Z. GUOMIN, C. YAN, X. JI, T. ZHANG, T. ZHANG, W. XU, *DolphinAttack: Inaudible Voice Commands*, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and* Communications *Security*, New York, 2017, 103–117.

[76] L'autenticazione (o verificazione) consiste in un confronto di tipo "uno a uno" (1:1) tra il modello creato sul momento e uno specifico *template* a lui associato al fine di accertare se il soggetto sia effettivamente chi dichiara di essere. Diversamente, l'identificazione attribuisce un'identità al soggetto attraverso un raffronto di tipo "uno

come la voce si rapporti con il principio di sicurezza in modo polivalente: da un lato l'attivazione vocale crea delle forti vulnerabilità, dall'altro presenta caratteristiche idonee all'implementazione di un algoritmo *speaker-dependent*[77] che utilizzi la voce quale fattore di autenticazione. Il passaggio dall'attivazione all'autenticazione ha mostrato un esito soddisfacente nel bloccare il tentativo di accesso a informazioni provenienti da oggetti intelligenti associati all'assistente[78], potendosi configurare a tutti gli effetti come misura di sicurezza di cui l'utente può usufruire, ad esempio, quando l'interazione con l'assistente comporti l'accesso e la comunicazione di dati sanitari[79].

Tuttavia, l'autenticazione per mezzo della voce è estremamente complessa da progettare a causa della variabilità dei parametri e delle interferenze ambientali[80]. La voce, infatti, è una caratteristica biometrica[81] ibrida, che si pone all'intersezione tra l'insieme degli attributi fisici e quelli comportamentali[82]. Inoltre, la voce è un *soft biometric* poiché è soggetta a diversi cambiamenti dovuti a situazioni contingenti (*e.g.* stato di raffreddamento, emozioni intense, ecc.) o al passare del tempo (*e.g.* età) che ne compromettono parzialmente la *permanenza*[83]. Un ulteriore problema è legato al contesto in cui il sensore effettua la registrazione: la frequenza del verificarsi di rumori di sottofondo o di altre distorsioni può minare il livello della *performance* del processo biometrico inficiando l'esattezza del risultato. Pertanto, anche se l'introduzione dell'autenticazione può garantire un livello di sicurezza maggiore rispetto alla sola attivazione vocale, nel caso in cui si trattino dati sanitari il processo biometrico di autenticazione[84] così configurato potrebbe risultare insufficiente. In particolare, permane il rischio di

a molti" (1:N) tra il *template* generato al momento del tentativo di identificazione e tutti i *template* presenti nell'archivio e relativi a un insieme di soggetti.

[77] Per sistema di riconoscimento vocale *speaker-dependent* si intende un algoritmo addestrato a riconoscere non solo quanto venga detto da un soggetto, ma anche l'identità di quest'ultimo che dunque è soggetta a verificazione (autenticazione).

[78] E. FUREY, J. BLUE., *She Knows Too Much – Voice Command Devices and Privacy*, *2018 29th Irish Signals and Systems Conference (ISSC)*, Belfast, 2018, 1-6, in Rete: https://ieeexplore.ieee.org/document/8585380.

[79] In tal modo non verrebbe significativamente inficiata l'esperienza dell'utente in termini di *usability*, non verrebbe richiesta l'installazione di ulteriori sensori o *hardware* specifici (sono sufficienti i microfoni già di cui l'assistente è già dotato) e il ricorso al fattore biometrico garantirebbe un elevato livello di sicurezza.

[80] Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA, oggi DigitPA), *Brevi note sulle tecnologie biometriche in un contesto ICT*, gennaio 2004, in Rete: https://www.privacy.it/archivio/cnipabiometria.html.

[81] La biometria è una scienza che si basa su tecniche di analisi quantitativa di caratteristiche fisiche, fisiologiche o comportamentali finalizzate al riconoscimento di un individuo. Si v. Q. XIAO, voce *Biometria*, in *Enciclopedia della Scienza e della Tecnica*, 2007, in Rete: http://www.treccani.it/enciclopedia/biometria_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/. Tali caratteristiche presentano quattro proprietà: (i) universalità; (ii) unicità; (iii) permanenza; e (iv) collezionabilità. Per ulteriori approfondimenti si v. Art. 29 WP, Documento di lavoro sulla biometria, adottato l'1 agosto 2003, WP 80; S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria, I codici a barre del corpo*, Torino, 2013, 134.

[82] R. DUCATO, *I dati biometrici,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *op. cit.*, 1285-1321.

[83] Per un'interessante tabella comparativa delle caratteristiche dei diversi attributi biometrici, tra i quali la voce, si v. K. DELAC, M. GRGIC, *A survey of biometric recognition methods, Proceedings of the 46th International SyrnPo-Sium Electronics in Marine*, Zadar, 2004, 188, in Rete: https://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/survey.pdf.

[84] Per un approfondimento sul processo biometrico di autenticazione e sulle sue fasi si v. CNIPA, *op. cit.*; S. VENIER, E. MORDINI, *Second-generation biometrics*, in R. FINN, D. WRIGHT (a cura di), *Privacy and emerging fields of science technology: Towards a common framework for privacy and ethical assessment*, 2010, 113-114, in Rete:

violazione del sistema attraverso il furto d'identità (*spoofing)*[85]. Un primo metodo oggetto di sperimentazione e implementazione per ridurre tale vulnerabilità è la *liveness detection*. Questa mira a rendere il sistema capace di determinare se un campione provenga da un essere umano vivente o al contrario da una copia artificiale (o artefatta)[86]. Un'ulteriore tecnica *anti-spoofing* è la fusione biometrica multimodale (*multimodal biometric system*) che combina diversi sottoinsiemi biometrici monomodali[87] per irrobustire il processo di verifica dell'identità.

L'adozione del *multimodal biometric system*, però, comporta notevoli costi finanziari e richiede all'utente di condividere simultaneamente diversi dati biometrici[88], aumentando i rischi connessi al trattamento di questi ultimi[89]. A tal riguardo, seppur antecedentemente rispetto al Regolamento, il Garante aveva richiesto che la decisione di avvalersi di sistemi basati su più caratteristiche biometriche fosse preceduta da un'attenta valutazione di necessità: «*occorre evitare, se non per motivate ed eccezionali esigenze, di ricorrere a sistemi che impieghino più di una caratteristica biometrica dell'interessato*»[90]. Pertanto, nel caso degli assistenti vocali, non parrebbe opportuno ricorrere alla fusione biometrica multimodale in via generale, ma solo laddove i rischi per i diritti e le libertà connessi al trattamento dei dati a cui si vuole avere accesso siano tanto gravi da giustificare la sussistenza di *motivate ed eccezionali esigenze*. Un caso di elezione potrebbe essere rappresentato dal trattamento di dati sanitari.

Per quanto riguarda la possibile concreta implementazione nell'assistente vocale di una simile autenticazione per l'utilizzo di "app sanitarie", si potrebbe pensare di affiancare alla voce l'impronta digitale o il riconoscimento facciale. Dal momento che numerosi cellulari di ultima generazione sono dotati di tecnologie in grado di processare tali dati per verificare l'identità del soggetto, si potrebbe adottare un modello di fusione a livello della decisione finale che preveda la comunicazione da parte del cellulare del solo esito del processo (*i.e.* accettazione o rigetto), senza che il campione biometrico, il *template* e l'indice di corrispondenza siano accessibili all'assistente vocale. Sebbene non sia il più performante, questo livello di fusione consentirebbe una maggior tutela dell'interessato dai rischi legati al trattamento di più dati biometrici da parte di uno stesso sistema. Inoltre, l'impiego del cellulare non inficerebbe eccessivamente l'esperienza dell'utente, al quale non sarebbe richiesto di interagire fisicamente

https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf; S. AMATO, F. CRISTOFARI, S. RACITI, *op. cit*.

[85] Menzionato dal considerando n. 75 GDPR.

[86] Q. XIAO, *op. cit.*; G. BOCCI, *Controllo accessi e biometrie*, in F. DI RESTA (a cura di), *La tutela dei dati personali nella società dell'informazione*, Torino, 2009, 79; riguardo all'efficacia ancora da accertare di tale metodo: S. VENIER, E. MORDINI, *op. cit.*, 122.

[87] Q. XIAO, *op. cit.*

[88] Alla luce della definizione del Regolamento, gli elementi che connotano il dato biometrico possono essere così schematizzati: (i) *tipologia di utilizzo*: impiego come identificativi esclusivi; (ii) *funzione*: identificazione e autenticazione; (iii) *fonte*: caratteristiche fisiche, fisiologiche o comportamentali della persona; (iv) *oggetto*: informazioni uniche sulla persona da cui sono estratte, ottenute con particolari tecniche di misurazione e analisi matematica. Si v. L. BOLOGNINI, E. PELINO, *Dato personale e trattamento*, in L. BOLOGNINI, C. BISTOLFI, E. PELINO (a cura di), *op. cit.*, 70.

[89] S. VENIER, E. MORDINI, *op. cit.*, 122.

[90] Garante per la Protezione dei Dati Personali, Linee-guida in materia di riconoscimento biometrico e firma grafometrica, Allegato A al Provvedimento 12 novembre 2014, n. 513, Provvedimento generale prescrittivo in tema di biometria, in G.U. 2 dicembre 2014, n. 280 (Linee Guida sul riconoscimento biometrico).

con l'assistente vocale, di solito posizionato in un punto fisso della casa, bensì con il cellulare, spesso al fianco dell'utilizzatore[91].

5. Conclusioni

Le tecnologie da sempre supportano, e quindi condizionano, i processi curativi. Il medico utilizza gli strumenti che gli vengono resi disponibili al fine di assistere al meglio, secondo scienza e coscienza, i propri pazienti. Tradizionalmente ciò ha riguardato artefatti atti ad intervenire direttamente sulla fisicità, sul corpo del paziente. Sono, di seguito, divenuti strumenti volti alla gestione clinico-amministrativa degli utenti del servizio sanitario e di supporto ai processi decisionali. Il rapporto medico – paziente si è quindi trasformato, le modalità di interazione sono cambiate così come è mutata la percezione stessa degli attori coinvolti. Si è in questo modo spesso sottolineato il rischio di disumanizzazione del rapporto empatico che caratterizza il contesto sanitario. Siamo ora di fronte ad un cambiamento epocale. L'Intelligenza Artificiale applicata a strumenti che non solo mimano il comportamento umano nel gestire ed affrontare la 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, che si apprestano a diventare talvolta del tutto autonome: non più, quindi, un rapporto che, seppur condizionato da un *medium* tecnologico inserito all'interno del flusso informativo, rimaneva uomo a uomo, bensì un confronto oramai quasi esclusivamente uomo a macchina.

Il nuovo possibile approccio cognitivo del paziente rispetto ad un servizio sanitario che si dota di questo tipo di strumenti può essere riassunto in una espressione evocativa: "la macchina non sbaglia mai". L'errata percezione che un sistema completamente automatizzato debba necessariamente consegnare risposte efficaci induce poi a non contestualizzare l'ambito applicativo di queste "macchine" ed a ritenere il fallimento di alcuni processi curativi, a volte ineludibile alla luce di un quadro clinico già compromesso, come un errore medico, una medical malpractice cui solo l'intervento giudiziale può porre rimedio. Molto si gioca appunto sulla percezione, errata, corretta, distorta, che noi come esseri umani abbiamo dell'intervento della macchina stessa.

Al pari di qualsiasi strumento, anche gli assistenti vocali di ultimissima 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

[91] Laddove non fosse possibile adottare tale schema (o l'utente lo preferisse) si potrebbe fare affidamento su una password, abbandonando lo schema di autenticazione biometrica multimodale, al fine di irrobustire l'autenticazione vocale, pur nella consapevolezza della vulnerabilità dimostrata nel corso del tempo dalla password quale strumento di verifica dell'identità (ad esempio, il Report del 2017 di Verizon sulle violazioni di dati personali ha riportato che più dell'80% era dovuto a password deboli o rubate). Si v. G. D'ACQUISTO, *Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati*, in F. PIZZETTI (a cura di), *op. cit.*, 287; Data Breach Investigations Report 2017, Verizon, in Rete: https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/.

umano), al contesto socio-culturale nell'ambito del quale vengono utilizzati (*divide* generazionali, diversità culturali che impattano sugli stili di vita, ecc.). Occorrerà, pertanto, analizzare questi possibili *bias* al fine di riuscire a verificarli se non a risolverli.

Altro tema centrale in questa discussione è quello dei processi decisionali unicamente basati sul trattamento automatizzato dei dati sanitari di cui si è diffusamente trattato *supra*. Come già descritto, il legislatore europeo ha da ultimo previsto all'art. 22 GDPR una disciplina *ad hoc* per tali scenari. Oltre agli obblighi informativi che enfatizzano l'importanza della trasparenza di questi processi (in contesti fortemente caratterizzati da c.d. black-box), una delle garanzie principali è quella di prevedere un possibile intervento umano a richiesta da parte del paziente/utente. Il "*man in the loop*" dovrebbe essere dotato delle conoscenze (medico-informatiche) volte a poter valutare la decisione assunta dalla "macchina", criticarla ed infine, eventualmente, modificarla. Un soggetto che dovrebbe però essere scevro da condizionamenti e da quel tipico processo mentale che porta ad ancorarsi a livello euristico rispetto alla prima decisione assunta dallo strumento automatizzato (ciò anche a fronte del rischio – legale – di discostarsi da questa)[92].

Infine, rileva il tema dell'autenticazione vocale attraverso un processo che utilizza dati biometrici. Si è già dimostrato come i rischi siano numerosi e di diversa natura. Certo si ripete spesso "la sicurezza non è un risultato, bensì un processo". Soluzioni tecnico-applicative vengono approntate e consigliano di ricorrere a sistemi multimodali e a più fattori di autenticazione. Questo spesso ha una diretta (negativa) conseguenza in termini di usabilità dello strumento (specie per particolari categorie di pazienti, quali ad esempio gli anziani). Assieme all'innovazione tecnologica deve crescere anche la sensibilità generale rispetto a questi strumenti ed all'importanza di tutelare la privacy degli individui. Nessuno si lamenta del fatto di dover dare più mandate al blindato di casa, specie in zone dove il tasso di furti è elevato. Allo stesso modo processi di alfabetizzazione informatico-sanitaria dovrebbero accrescere l'interesse diretto da parte dei soggetti coinvolti a meglio tutelare i propri dati personali, oggetto di massivo trattamento da parte di questi strumenti.

Più in generale, dunque, è la tanto declamata privacy by design a giocare un ruolo essenziale[93]. I processi che riguardano il trattamento di dati personali devono essere fin dalla loro progettazione informati dei principi e delle tutele che l'ordinamento giuridico riconosce. Questo richiede l'attivazione di tavoli di lavoro veramente interdisciplinari dove la programmazione dei codici informatici sia supportata da esperti di saperi diversi, quali la medicina, la sociologia, la psicologia e, per quanto direttamente ci riguarda, il diritto[94]. Servirà, pertanto, un giurista in grado di comprendere, almeno negli elementi essenziali, i percorsi di sviluppo delle piattaforme informatiche. "*Medice, cura te ipsum*" recita un'espressione proverbiale nota nel mondo greco-latino poi ripresa nei testi evangelici[95]. Quello che

[92] Per approfondimenti in merito ai limiti cognitivi che il giurista incontra nella risoluzione di un problema, si v. G. PASCUZZI, *Il problem solving nelle professioni legali*, Bologna, 2017, 30-40.

[93] A. CAVOUKIAN, *Privacy by design: the definitive workshop - A foreword by Ann Cavoukian*, 3 *Identity Info. Soc'y* 247 (2010); B.-J. KOOPS, R. E. LEENES, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data Protection Law,* 28 *Int. Rev. Law Comput. Tech*. 1 (2013).

[94] In merito ai metodi interdisciplinari, si v. R. FRODEMAN ET AL. (eds.), *Oxford Handbook of Interdisciplinarity*, 2nd ed., Oxford University Press, 2017; S. MENKEN, M. KEESTRA, *An Introduction to Interdisciplinary Research*, Amsterdam University Press, 2016.

[95] Vangelo secondo Luca (4, 23).

le macchine promettono di fare diventa sempre più evidente in futuristici scenari (a dire il vero dai tratti talvolta distopici). Non si può più solamente deplorare la presunta tracotanza della tecnica, che disumanizzerebbe il rapporto medico-paziente. È ora necessario affrontare le criticità insite nelle nuove tecnologie e cercare di incidere sulla loro progettazione. È un compito che non può (o non può più) essere demandato ad altri.

ISSN 2284-4503