amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 1/2023

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Intelligenza artificiale nell'ambito del sistema sanitario. Implicazioni in termini di privacy alla luce del nuovo GDPR

di Karidia Karaboue

(Avvocato)

Sommario

1. Introduzione – 2. Opportunità per i sistemi sanitari e crescente necessità di accesso ai dati – 3. Implicazioni in termini di privacy e protezione dei dati personali – 4. Spunti dal GDPR per migliorare la privacy e la protezione dei dati personali – 4.1. Diritto alla portabilità dei dati e diritto all'oblio – 5. Rafforzare gli obblighi: verso una maggiore responsabilità degli attori dei dati – 6. Riflessioni conclusive.

Abstract

The complexity and increase of data in health care means that the application of artificial intelligence (AI) will be increasing in the future. The main categories of applications, in particular, include diagnosis and treatment recommendations, patient engagement and adherence, and administrative activities. This paper, after analyzing the impact of Artificial Intelligence systems in the healthcare sector, looks at the privacy implications in light of the new European Union General Data Protection Regulation (GDPR).

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review.*

ISSN 2036-7821

1. Introduzione.

Sebbene l'intelligenza artificiale (IA) sia considerata un'innovazione contemporanea, in realtà il suo sviluppo si protrae da oltre mezzo secolo. La ricerca in tale settore, infatti, è iniziata negli anni Cinquanta, quando Alan Turing ha teorizzato la possibilità, per le macchine, di pensare come gli esseri umani[1].

Successivamente, risale al 1959 il primo caso di "apprendimento automatico", in cui gli scienziati hanno creato un programma in grado di risolvere enigmi in maniera autonoma[2].

Con particolare riferimento al settore sanitario, il potenziale dell'intelligenza artificiale per promuovere una migliore assistenza è al centro dei moderni dibattiti sulle politiche sanitarie[3].

Lo scenario delle possibili applicazioni, infatti, è sterminato. L'utilizzo delle nuove tecnologie digitali e di intelligenza artificiale riguarderebbe, *prima facie*, l'impiego di algoritmi per migliorare la raccolta, conservazione e trattamento dei dati personali relativi alla salute degli individui, informazioni che permetterebbero di studiare le caratteristiche fisiche e genetiche di ciascun paziente, al fine di implementare la prevenzione delle malattie, l'elaborazione di diagnosi o la realizzazione di un trattamento e un'assistenza personalizzata[4].

In tale ambito, comunque, le tecnologie di IA richiedono una serie di dati, soprattutto personali, per funzionare in maniera corretta: nello specifico, si tratta di informazioni relative alla salute del paziente[5].

Ciò posto, la promozione di sistemi intelligenti e l'opportunità di coglierne i vantaggi per il sistema sanitario dipendono, in gran parte, dalla possibilità per i pazienti

---

[1] In proposito, si veda A.M. TURING, *Computing Machinery and Intelligence*, MIND, 1950. Per quel che concerne il profilo definitorio, sebbene vi siano numerose definizioni di IA, è possibile asserire che si tratta di «una scienza e un insieme di tecniche computazionali che vengono ispirate – pur operando tipicamente in maniera diversa – dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire». AA. VV., *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence*, Stanford University Press, 2016.

[2] N. CRISTIANINI, *Intelligence Reinvented*, NEWSCIENTIST, 2016, p. 41 ss; R. PARLOFF, *The Deep-Learning Revolution*, FORTUNE, 2016, p. 106 ss.

[3] Per un approfondimento sul punto, A. HOLZINGER, *Trends in Interactive Knowledge Discovery for Personalized Medicine: Cognitive Science meets Machine Learning*, IEEE Intelligent Informatics Bulletin, 2014, p.14 ss.

[4] E. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, BIOLAW J., 2019, p. 164. L'autore afferma come vi siano «già oggi sistemi sperimentali che consentono di 'categorizzare e analizzare le informazioni trasmesse dai pazienti ai medici in linguaggio naturale e tracciare così delle dinamiche inedite grazie a meccanismi di machine reading, per cogliere sul nascere eventuali casi epidemici'». *Ibid*. In tema di diagnosi, si veda anche J. BUSH, *How AI is taking the scut work out of health care*, HARV. BUS. REV., 2018.

[5] R. MIOTTO *et al.*, *Deep Learning for Healthcare: Review, Opportunities and Challenges*, BRIEF BIOINFORM., 2018, p. 1246.

ISSN 2036-7821

gestire meglio i propri dati sensibili, grazie a un più facile accesso alle informazioni sulla propria salute[6].
Pertanto, in siffatto scenario, garantire la protezione della privacy appare essenziale, soprattutto se si considera che i pazienti spesso mostrano notevoli preoccupazioni riguardo alla condivisione dei propri dati nel contesto medico e clinico[7].
Con l'adozione del nuovo Regolamento generale sulla protezione dei dati (*General Data Protection Regulation* – GDPR)[8], l'Unione europea (UE), per prima, ha tentato di regolamentare l'IA attraverso la normativa sulla protezione dei dati[9].

2. Opportunità per i sistemi sanitari e crescente necessità di accesso ai dati
In numerosi sistemi sanitari, l'IA è già stata impiegata con successo, principalmente sotto forma di tecnologie basate sull'apprendimento automatico e sul *deep learning*[10].
In entrambi i casi, una certa quantità di dati (l'*input*) viene fornita al sistema per essere elaborata (attraverso uno o più algoritmi), al fine di fornire un *output*[11].
Le differenze tra apprendimento automatico e *deep learning* riguardano il tipo e la quantità di dati che possono essere elaborati dal sistema e il modo in cui vengono generati gli algoritmi. Il *deep learning* descrive una forma più complicata di apprendimento, noto come rete neurale artificiale[12].
La principale evoluzione apportata dal passaggio dall'apprendimento automatico al *deep learning* è che, mentre nel primo caso sono richiesti algoritmi supervisionati

[6] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, J. LAW BIOSCI., 2019, pp. 317-318. Sul medesimo punto, anche E. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, cit., 167.

[7] *Ibid*.

[8] 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 circo-lazione di tali dati e che abroga la direttiva 95/46/CE.

[9] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., p. 318.

[10] F. JIANG *et al.*, *Artificial Intelligence in Healthcare: Past, Present and Future*, STROKEVASC. NEUROL., 2017, p. 243 ss. In particolare, «[g]li algoritmi e gli insiemi di dati sono alla base dei metodi di apprendimento automatico, o di machine learning, e in questo ambito, possono essere sostanzialmente suddivisi in due diverse tipologie, che sono legate all'intervento dell'operatore umano. Gli algoritmi supervised sono 'annotati' dagli operatori umani o dalle macchine già addestrate che, supervisionando l'apprendimento, permettono la classificazione dei dati. Anche in questo caso il fattore umano entra in causa nella supervisione fornendo una interpretazione che può essere anche culturale e quindi con bias, nei dati o nelle regole dell'algoritmo di addestramento, che influenzano l'output finale». M.C. CARROZZA *et al.*, *AI: profili tecnologici Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, 2019, p. 8.

[11] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 318-319. L'apprendimento automatico è più specificamente utilizzato per l'individuazione automatica di modelli in grandi quantità di dati, sulla base di deduzioni logiche.

[12] F. JIANG *et al.*, *Artificial Intelligence in Healthcare: Past, Present and Future*, cit., p. 243 ss. Inoltre, il *deep learning* può elaborare grandi quantità di dati grezzi e complessi, mentre l'apprendimento automatico è limitato a una quantità minore di informazioni che devono essere tradotte in un linguaggio che la macchina è in grado di comprendere (*i.e.* "dati strutturati").

ISSN 2036-7821

"costruiti dall'uomo", il processo utilizzato nel *deep learning* per ottenere l'output è generato dal sistema stesso. L'elevato livello di complessità del processo, tuttavia, rende i sistemi di *deep learning* piuttosto "opachi"[13]. Ciò, in particolare, in conseguenza del fatto che, allo stato attuale risulta ancora quasi impossibile capire come sia stato prodotto esattamente questo risultato, e ancor meno controllarlo[14].

In alcuni casi, i dati possono diventare parte dell'algoritmo stesso. Parte della dottrina fa riferimento a questa mancanza di trasparenza nel *deep learning* come a un fenomeno di "*black box*"[15], particolarmente problematico quando si tratta di dati sensibili dei pazienti[16].

Poste le doverose premesse, la ricerca sull'IA applicata al settore sanitario è un campo in rapida crescita[17].

Stante l'attuale sviluppo tecnologico, l'IA nel settore sanitario è, generalmente, concentrata in tre aree: (i) oncologia, (ii) neurologia e (iii) cardiologia[18].

Si tratta di aree della medicina in cui la diagnosi precoce è fondamentale[19]. In tal senso, i sistemi di IA stanno già fornendo supporto ai medici nel processo decisionale, fornendo loro informazioni pertinenti e aggiornate per la diagnosi e i trattamenti[20].

---

[13] T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, FUTURE HEALTHC. J., 2019, pp. 94-95.

[14] W. KNIGHT, *The Dark Secret at The Heart of AI*, MIT Technology Review, 2017. https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai. (ultima consultazione 03/12/2022).

[15] Sul punto, *ex multis*, R.A. FORD & W. NICHOLSON PRICE, *Privacy and Accountability in Black-Box Medicine*, MICH. TECH. L. REV., 2016, p. 1 ss; W. NICHOLSON PRICE, *Regulating Black-Box Medicine*, MICH. L. REV., 2017, p. 421 ss; F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015; T. SIMONITE, *AI Experts Want to End "Black Box" Algorithms in Government*, WIRED, 2017. https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government. (ultima consultazione 04/12/2022).

[16] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., p. 319.

[17] D. FAGGELLA, *The State of AI Applications in Healthcare – An Overview of Trends*, EMERJ, 2018. https://emerj.com/ai-sector-overviews/state-ai-applications-healthcare-overview-trends. (ultima consultazione 04/12/2022).

[18] P.J. LISBOA & A.F.G. TAKTAK, *The Use of Artificial Neural Networks in Decision Support in Cancer: A Systematic Review*, NEURAL NETW., 2006, p. 415 ss. *Deep learning*, in particolare, «is increasingly being applied to radiomics, or the detection of clinically relevant features in imaging data beyond what can be perceived by the human eye». T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, cit., p. 95. Sul medesimo punto, anche A. VIAL, D. STIRLING, M. FIELD *et al.*, *The role of deep learning and - radiomic feature extraction in cancer -specific predictive modelling: a review*, TRANSL. CANCER RES., 2018, p. 803 ss.

[19] F. JIANG *et al.*, *Artificial Intelligence in Healthcare: Past, Present and Future*, cit., p. 245.

[20] V.J. MAR & H.P. SOYER, *Artificial Intelligence for Melanoma Diagnosis: How Can We Deliver on the Promise?*, ANN. ONCOL., 2018, p. 1628. A tal proposito, l'uso dell'IA, combinato con la diagnostica per immagini, ha dimostrato un grande potenziale nel supportare la rapida identificazione della presenza o dell'assenza di alcuni tipi di cancro, a volte con una maggiore accuratezza rispetto agli specialisti.

ISSN 2036-7821

A ogni modo, comunque, l'intelligenza artificiale in tale contesto non si limita alla mera assistenza clinica o al processo decisionale. Individuando automaticamente le somiglianze tra le cartelle cliniche dei pazienti, i sistemi di IA possono aiutare i ricercatori a identificare rapidamente la coorte di pazienti ottimale per uno specifico studio clinico[21].

3. Implicazioni in termini di privacy e protezione dei dati personali

Le sfide senza precedenti che il diritto alla privacy si trova ad affrontare con lo sviluppo di Internet e dell'intelligenza artificiale erano imprevedibili al momento dell'elaborazione delle moderne leggi sulla privacy[22].

Sebbene a volte siano riluttanti a consentire l'accesso ai dati per la ricerca sanitaria, la maggior parte degli attori in causa condivide regolarmente i dati personali attraverso dispositivi portatili e siti web di test genetici[23].

Gli usi (e gli abusi) secondari dei dati sono un problema che i legislatori europei hanno voluto affrontare quando hanno adottato il GDPR.

Nello specifico, il nuovo GDPR e conseguentemente, il d.lgs del 10 agosto 2018, n.101, assicurano un'applicazione ed una protezione dei dati personali omogenea su tutto il territorio dell'Unione europea, garantendo in tal modo una migliore protezione di un diritto fondamentale non solo per i cittadini europei, bensì per tutti gli individui che si trovano sul territorio dell'Unione[24].

Applicato al settore medico, il GDPR ha un duplice scopo. Da un lato, mira a prevenire rigorosamente gli usi secondari e non autorizzati dei dati personali (sia da parte del settore privato che di quello pubblico). Dall'altro lato, mira a semplificare l'accesso ai dati personali, sempre più necessario per lo sviluppo della ricerca, pur tenendo conto dell'importanza della privacy. A tal fine, il GDPR prevede una riduzione degli obblighi in termini di formalità amministrative prima di accedere e utilizzare i dati sanitari.

Laddove la Direttiva prevedeva pesanti formalità di dichiarazione alle autorità nazionali, il GDPR mira a responsabilizzare maggiormente gli attori dei dati piuttosto che a limitare la loro capacità di avviare la ricerca[25].

---

[21] In merito, si approfondisca con C. CASTANEDA *et al.*, *Clinical Decision Support Systems for Improving Diagnostic Accuracy and Achieving Precision Medicine*, J. CLIN. BIOINFORMA., 2015, p. 4 ss; Z. OBERMEYER & E. J. EMANUEL, *Predicting the Future – Big Data, Machine Learning, and Clinical Medicine*, N. ENG. J. MED., 2016, p. 1219 ss.

[22] Sul punto, in particolare, si rimanda a O. DIGGELMANN & M. NICOLE CLEIS, *How the Right to Privacy Became a Human Right*, HUM. RIGHTS LAW REV., 2014, p. 442.

[23] S. ARMSTRONG, *What Happens to Data Gathered by Health and Wellness Apps?*, BMJ, 2016, pp. 353-354.

[24] Per un'analisi approfondita si rimanda a L. CALIFANO & C. COLAPIETRO, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[25] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 321-322. Con riferimento all'ambito sanitario, il GDPR ricompresi nei dati relativi alla salute «tutti gli aspetti che riguardano la salute fisica o mentale di una persona, compresa la prestazione dei servizi di assistenza sanitaria in quanto capaci di rivelare informazioni relative allo stato di salute. Esse

ISSN 2036-7821

I dati medici, in particolare, sono classificati come "dati sensibili". Questi dati sono protetti da un quadro specifico che ne vieta il trattamento (art. 9 del GDPR). Sono tuttavia previste eccezioni sostanziali per facilitare l'accesso ai dati rilevanti, pur riconoscendone la percettibilità.

Anche se, in taluni casi, negli ordinamenti giuridici vengono presentati come diritti separati, il diritto alla protezione dei dati è una componente essenziale del diritto alla privacy. Di conseguenza, se non è possibile garantire la protezione dei dati, è altrettanto impossibile assicurare il rispetto della privacy[26].

In generale, i dati personali sono dati che consentono l'identificazione diretta o indiretta (ad esempio attraverso la triangolazione) di una persona interessata[27].

I dati relativi alla salute, i dati genetici e i dati biometrici, in particolare, sono considerati altamente sensibili. A tali dati il GDPR assegna un quadro più protettivo rispetto a quello applicabile ad altri tipi di dati personali[28].

Il GDPR, in tal senso, vieta il trattamento di tutti i dati sensibili; tuttavia, l'articolo 9, paragrafo 2, prevede un elenco sostanziale di eccezioni a questo principio generale di divieto. La prima di queste si applica nel caso in cui «l'interessato abbia prestato esplicito consenso al trattamento di tali dati personali per una o più finalità specifiche»[29].

È interessante notare che queste fattispecie sono stabilite come condizioni alternative. La formulazione dell'articolo implica quindi che l'ottenimento di un consenso specifico e informato, come richiesto dal GDPR, non è necessario, purché si applichi un'altra base giuridica per il trattamento[30].

---

ricomprendono informazioni sulla persona assunte sin dalla fase di accesso al servizio sanitario, o ancora, al momento della registrazione. Tali informazioni possono essere rappresentate anche da un numero o da un simbolo; in altre parole, è possibile definire dati relativi alla salute tutte quelle informazioni idonee a rivelare lo stato di salute fisica». F. COMITO, *La tutela dei dati personali in ambito di assistenza sanitaria e sociosanitaria*, in *Amministrazione in Cammino*, 2021, p. 4.

[26] *Ibid*. In Canada e negli Stati Uniti, per esempio, le norme sulla protezione dei dati riguardano la raccolta e l'utilizzo dei dati personali. Talvolta, tuttavia, l'IA non si basa su alcun dato personale, il che significa che in queste circostanze non si applica alcuna normativa sulla protezione dei dati. I criteri per definire i dati personali rispetto a quelli non personali diventano quindi cruciali per determinare l'ambito di applicazione di un regolamento sui dati. L'UE ha tuttavia adottato un regolamento specifico per i dati non personali. Questo regolamento mira a rafforzare la libera circolazione dei dati non personali e ad agevolare lo sviluppo di un mercato digitale comune all'interno dell'UE.

[27] L. PANGRAZIO & N. SELWYN, *'Personal Data Literacies': A Critical Literacies Approach to Enhancing Understandings of Personal Digital Data*, NEWMED. & SOC., 2019, p. 437 ss.

[28] Come previsto dall'Art. 6 del GDPR.

[29] Come previsto dall'Art. 9.2.a del GDPR. In argomento, si veda G. FIORIGLIO, *La protezione dei dati sanitari nella Societa`algoritmica. Profili informatico-giuridici*, J. ETHICS & LEG. TECH., 2021, p. 87 ss.

[30] Per esempio, il trattamento dei dati sensibili è consentito quando «è necessario per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o di statistica» (art. 9.2.j, GDPR), a condizione che siano previste garanzie adeguate (art. 89, GDPR). È, pertanto, comprensibile che l'obiettivo del GDPR sia quello di consentire una certa flessibilità nel contesto della ricerca scientifica che utilizza dati sensibili.

ISSN 2036-7821

Gli Stati membri, tuttavia, possono mantenere o introdurre ulteriori condizioni, comprese le limitazioni, per quanto riguarda il trattamento di dati genetici, biometrici o relativi alla salute (artt. 9.4 e 89 del GDPR) e rendere più rigorosi i requisiti di consenso con disposizioni specifiche (artt. 6.2 e 9.2.a del GDPR)[31].
Tale discrezionalità potrebbe, a parere di chi scrive, ostacolare questo obiettivo ed è stata criticata per il suo impatto negativo sulle iniziative di armonizzazione internazionale[32].
Inoltre, ai sensi del GDPR, la de-identificazione non è automaticamente considerata un modo sufficiente per impedire la re-identificazione delle persone. Pertanto, i dati de-identificati rimangono nella categoria dei dati personali protetti[33].
Il GDPR esclude solo i dati anonimi dal suo campo di applicazione.
Il Regolamento, in proposito, prevede specifiche condizioni per l'anonimizzazione; un processo che prevede una serie di tecniche per impedire la reidentificazione. Il considerando 26 specifica, a proposito di queste tecniche, che per «determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments»[34].
La categorizzazione dei dati sensibili presenta dei vantaggi, in quanto tiene conto della necessità di una maggiore cautela nel trattamento dei dati relativi alla salute. Può essere efficace per prevenire usi secondari non autorizzati, ma questa categoria speciale può anche agire come un disincentivo per i ricercatori, soprattutto in considerazione delle elevate sanzioni in cui incorrono in caso di violazione di tali dati[35].

---

[31] T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, cit., pp. 95-96.

[32] L'adozione di condizioni restrittive e disparate per il trattamento dei dati sensibili potrebbe creare conflitti legislativi all'interno dell'UE tra gli Stati membri, con il rischio di ostacolare la ricerca transfrontaliera, soprattutto nel campo della genetica. Si veda, per un approfondimento generale in merito a tale tematica K. PORMEISTER, *Genetic Research and Applicable Law: The Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-Border Genetic Research*, J. LAWBIOSCI., 2019.

[33] In tal senso, quando si parla di de-identificazione esi fa riferimento a una forma di anonimizzazione dove i dati personali sono mantenuti intatti, ma i riferimenti a essi o le specifiche informazioni di identificazione, come ad esempio i nomi, vengono sostituiti con identificatori anonimi. Sul punto G. DE GREGORIO & R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy Digitale*, Milano, 2019, pp. 447-484; G. RESTA, *Anonimato, responsabilità, identificazione prospettive di diritto comparato*, DIR. INFOR., 2014.

[34] Considerando 26 del GDPR.

[35] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., p. 322.

ISSN 2036-7821

4. Spunti dal GDPR per migliorare la privacy e la protezione dei dati personali

Al fine di garantire alle persone un maggiore controllo sui propri dati, il GDPR rafforza i requisiti per un consenso valido previsti dall'articolo 7. Il consenso valido è ora definito come «liberamente fornito, specifico, informato e inequivocabile»[36]. Sebbene il Regolamento non stabilisca che il consenso debba essere scritto, esso deve essere esplicito e informato. Il considerando 32 specifica a questo proposito che «silence, pre-ticked boxes or inactivity should not therefore constitute consent». Questo margine di discrezionalità ha lo scopo di fornire alle corti di giustizia una sufficiente flessibilità nel valutare la validità dei modelli di consenso[37].

Questi nuovi requisiti promuovono l'uso di processi di consenso semplificati rispetto a procedure burocratiche rigide. Sono destinati a promuovere il livello di fiducia necessario per una condivisione dei dati maggiormente efficace, in primo luogo aumentando il senso di controllo degli individui sui propri dati. Tuttavia, se i requisiti per il consenso sono più severi, il GDPR prevede molte eccezioni che consentono il trattamento di dati sensibili e non sensibili[38].

Per essere lecito, qualsiasi trattamento richiede una base legittima e il consenso valido è solo una delle possibili basi elencate nell'articolo 6 per l'utilizzo di dati non sensibili. Le altre cinque basi includono «when the processing of personal data is necessary for the performance of a contract to which the data subject is party. [or] a task carried out in the public interest»[39]. Di conseguenza, finché può essere applicata qualsiasi altra base, la liceità del trattamento non è più condizionata dall'ottenimento di un consenso valido.

Nel caso di dati sensibili, l'articolo 9 stabilisce che il trattamento basato sul consenso deve essere limitato a finalità predefinite e qualsiasi ulteriore trattamento degli stessi dati implica la richiesta di nuovo consenso. Tuttavia, gli usi secondari dei dati sono consentiti quando tale trattamento persegue finalità di ricerca scientifica (art. 89.1, GDPR)[40].

---

[36] Come previsto dall'Art. 4.11 del GDPR. Tuttavia, le fasi più concrete per la valutazione di ciò che costituisce un consenso esplicito valido ai sensi del GDPR rimangono ancora aperte all'interpretazione delle giurisdizioni nazionali.

[37] T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, cit., p. 96.

[38] *Ibid*.

[39] Come previsto dagli Artt. 6b e 6e del GDPR.

[40] Il considerando 156 specifica tuttavia che «[t]he further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfill those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist». Per un approfondimento in merito, si veda G. CHASSANG, *The Impact of the EU General Data Protection Regulation on Scientific Research*, ECANCERMEDICALSCIENCE, 2017, p. 709 ss.

ISSN 2036-7821

In particolare, il GDPR intende impedire lo scenario del consenso implicito, come ad esempio la partecipazione basata sul regime di "opt-out", in quanto non è sempre chiaro agli interessati a cosa stiano effettivamente fornendo consenso[41].
Una sfida importante per ogni azienda che tratta dati personali coperti dal GDPR è quindi quella di garantire che il consenso sia debitamente informato ed espresso.
Se, infatti, è necessario modificare i requisiti di consenso per proteggere meglio la privacy e gli interessi dei soggetti, bisognerebbe tenere in debita considerazione le specificità della ricerca scientifica, per non rallentare lo sviluppo di tecnologie utili. Requisiti di consenso specifici, limitati a scopi predeterminati, possono essere piuttosto limitanti nel contesto della ricerca, poiché spesso è difficile prevedere le potenzialità dei dati raccolti. Il considerando 33 del GDPR riconosce questa sfida, ma non fornisce un mezzo per evitare gli obblighi delineati dallo stesso Regolamento[42].
Il GDPR, in tale ottica, fornisce agli interessati un altro diritto che mira a rafforzare il loro senso di controllo sul trattamento dei loro dati. In particolare, in base a tale previsione, i soggetti non saranno «subject to a decision based solely on automated processing, including profiling»[43].
Nello specifico ambito sanitario, le tecnologie di intelligenza artificiale possono essere direttamente interessate da questo nuovo diritto, il quale implica, per esempio, che un sistema di *deep learning* creato per fornire suggerimenti terapeutici non possa essere utilizzato come unica base per decidere quale farmaco sarà eventualmente prescritto[44].
Le eccezioni a questa regola si applicano quando sono previste dalla legislazione degli Stati membri o quando sono necessarie per stipulare un contratto o, ancora, quando il trattamento è basato sul consenso preventivo dell'individuo. In questi casi, gli interessati hanno il diritto di ricevere una giustificazione per la decisione automatizzata[45].
Tuttavia, il problema sorge quando l'IA diventa così complessa ed elabora una tale quantità di dati che non è possibile fornire una giustificazione. Il fenomeno del c.d. "*black box*"[46] dei sistemi di *deep learning* può allora diventare un vero ostacolo per l'implementazione dell'IA nell'assistenza sanitaria.

---

[41] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 324-325.

[42] Spesso, infatti, non è possibile identificare pienamente lo scopo del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, le persone interessate dovrebbero essere autorizzate a dare il proprio consenso a determinate aree della ricerca scientifica, se in linea con gli standard etici riconosciuti per la ricerca scientifica. Come espressamente previsto dall'Art. 33 del GDPR.

[43] Art. 22 del GDPR.

[44] E. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, cit., pp. 167-168.

[45] T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, cit., pp. 95-96.

[46] Secondo un'idea corrente «la maggior parte dei sistemi di apprendimento automatic (machine learning), e soprattutto quelli di deep learning, sono essenzialmente scatole nere (black boxes), in cui non si può davvero

ISSN 2036-7821

4.1. Diritto alla portabilità dei dati e diritto all'oblio

I dati personali, in base a quanto previsto dal GDPR, devono essere ottenuti in un formato strutturato, di uso comune e leggibile da una macchina[47].

Inoltre, gli interessati hanno il diritto generale di accedere e correggere i dati personali che un'organizzazione abbia raccolto su di loro. Il GDPR, in tale ottica, include un nuovo interessante diritto alla portabilità dei dati[48].

Nel settore sanitario, si ritiene che la portabilità dei dati abbia benefici pratici per l'accesso ai dati, in quanto consente agli utenti di salvare i dati e di condividerli, per esempio, con il proprio medico o con la struttura sanitaria mediante un'apposita app[49].

Tuttavia, l'articolo 20 del Regolamento esclude dal suo ambito di applicazione i dati personali che non sono stati forniti dall'interessato stesso. In tal senso, infatti, il diritto alla portabilità dei dati, anche in considerazione della collocazione sistematica (GDPR), è prima di tutto «un diritto personale dell'individuo teso a realizzare l'identità in senso digitale dell'individuo e segna in tal senso la strada europea nel settore»[50].

---

controllare come l'algoritmo raggiunga il risultato che raggiunge». A. SANTOSUOSSO, *Intelligenza artificiale, conoscenze neuroscientifiche e decisioni giuridiche*, in *Teoria e Critica della Regolazione Sociale*, Milano, 2021, p. 188. La *black box* – afferma l'autore – è una «metafora atecnica e suggestiva, al pari di altre, come per es. essere un 'oracolo'». *Ibid*. In realtà, la scatola nera si definisce «in opposizione a quello che è ritenuto spiegabile o spiegato, rispetto al quale la scatola nera, per la quale conosciamo solo gli stimoli in entrata (input) e le risposte in uscita (output), si presenta come un'unità le cui operazioni interne non possono essere oggetto di indagine». *Ibid*.

[47] Art. 20 del GDPR.

[48] Per un approfondimento, *inter alia*, E. BANI & E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, in V. FALCE, *Financial Innovation tra disintermediazione e mercato*, Torino, 2021, pp. 137-179. In breve, affermano gli autori, «l'idea di fondo è semplice: si vuole consentire a ciascun individuo che utilizzi servizi on-line di "portare" i propri dati personali da un servizio / fornitore all'altro, in modo da poterli riutilizzare in piena autonomia senza perdere il patrimonio di informazioni creato in precedenza. Il precedente logico e storico, in ambito europeo, è dato dalla portabilità del numero telefonico da un operatore all'altro e la portabilità dei mutui». *Ibid*. In argomento, si vedano anche S. TROIANO, *Il diritto alla portabilità dei dati*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p. 195 ss; E. BATTELLI & G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in E. TOSI (a cura di), *Riservatezza e protezione dei dati tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 185, in particolare, pp. 187 ss e 193 ss; R.H. WEBER, *Data portability and big data analytics. New competition policy challenges*, CONCORR. MERC., 2016, p. 59 ss; I. GRAEF, J. VERSCHAKELEN, P. VALCKE, *Putting the right to data portability into a competition law perspective*, in *Law: The Journal of the Higher School of Economics*, in Annual Review, 2013, p. 53 ss; V. ZENO-ZENCOVICH, *Una svolta giurisprudenziale nella tutela della riservatezza*, DIR. INFOR., 1986, pp. 934 ss.

[49] A. ST JOHN, *Europe's GDPR Brings Data Portability to U.S. Consumers*, consumerreports, 2018. Disponibile al sito https://www.consumerreports.org/privacy/gdpr-brings-data-portability-to-us-consumers. (ultima consultazione 05/12/2022).

[50] E. BANI & E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, cit., p. 139. Sul medesimo punto anche G. ZANFIR, *The right to Data portability in the context of the EU data protection reform*, in *International Data Privacy Law*, 2012, p. 3; O. LYNSKEY, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, EU. L. REV., 2017, p. 793 ss; L. SCUDIERO, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability*, ECPL, 2017, p. 119 ss; G. MALGIERI, *Il diritto alla portabilità dei*

ISSN 2036-7821

Un altro diritto nuovo concesso dal GDPR agli interessati è il diritto alla cancellazione – o diritto all'oblio[51].
Tale diritto, consente alle persone di richiedere la cancellazione completa dei propri dati personali in possesso di organizzazioni pubbliche o private[52]. Si tratta di una novità assoluta apportata dal GDPR.
Questo diritto ha lo scopo di assicurare agli interessati che qualsiasi informazione personale da loro divulgata possa essere completamente cancellata su loro richiesta[53].
L'articolo 17, in particolare, prevede anche alcune limitazioni implicite all'applicazione del diritto alla cancellazione, in quanto si applica solo quando si basa su uno dei motivi che sono esplicitamente enumerati nel testo[54].
Tali motivi includono i dati personali raccolti che non sono più necessari in relazione alle finalità per cui sono stati raccolti. Infatti, laddove tali dati siano ancora necessari per il trattamento, la richiesta di cancellazione potrebbe essere validamente negata[55].
Altre eccezioni sono rappresentate dal caso in cui il trattamento sia necessario per motivi di interesse pubblico nel settore della salute pubblica (art. 17.1.c, GDPR) o quando comporta l'esercizio di pubblici poteri (art. 17.1.d, GDPR).
Nei casi in cui il diritto alla cancellazione si applica, la sua attuazione sarà ostacolata dalla difficoltà tecnica di garantire la cancellazione completa e sistematica dei dati personali, soprattutto se già condivisi con i collaboratori[56].
Tuttavia, va osservato comunque che l'articolo 20 del GDP (par. 3, primo periodo), stabilisce «una prevalenza del diritto all'oblio sul diritto alla portabilità (il secondo deve lasciare "impregiudicato" il primo), per cui quest'ultimo potrebbe trovarsi

---

dati personali, in G. COMANDÉ & G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, Milano, 2018, p. 56 ss. Le informazioni derivate dall'analisi dei dati raccolti da un dispositivo indossabile per la salute, per esempio, non sono quindi coperte da questo diritto, nonostante il loro potenziale beneficio per la ricerca. M. B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 327-328.

[51] Art. 17 del GDPR.

[52] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in C. PERLINGIERI & L. RUGGERI, *Internet e diritto civile*, Napoli, 2015, p. p. 29 ss; Si vedano, per un'analisi comparatistica sul tema, G. RESTA & V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, CONS. MERC., 2015; A. PALMIERI & R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, NUOVI QUAD. FORO IT., 2014; O. POLLICINO & M. BASSANINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Torino, 2013;

[53] Si consultino, generalmente, in tema di diritto alla cancellazione dei dati M. ZANICHELLI, *Il diritto all'oblio tra privacy e identità digitale*, INFOR. DIR., 2016. PP. 9-28; S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[54] T. DAVENPORT & L. KALAKOTA, *The potential for artificial intelligence in healthcare*, cit., p. 96.

[55] E. BANI & E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, cit., pp. 140-141.

[56] S. C. BENNETT, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, BERKELEY J. INT'L L., 2012, p. 161 ss.

ISSN 2036-7821

legittimamente impedito dalla richiesta di cancellazione di terzi i cui dati siano inseparabili da quelli del primo interessato»[57].
Nel contesto dell'IA, una specificità del *deep learning* è che l'algoritmo utilizzato per ottenere un risultato è creato automaticamente sulla base di dati che sono stati introdotti in precedenza. Questi dati diventano, quindi, parte dell'algoritmo e diventa impossibile identificare ed estrarre dati specifici per cancellarli. In caso di mancata cancellazione, il GDPR prevede sanzioni elevate in caso di violazione delle sue disposizioni[58].
Questo fa parte dell'intenzione generale del legislatore europeo di aumentare la responsabilità degli attori dei dati per la protezione della privacy e di promuovere lo sviluppo dell'autoregolamentazione per evitare situazioni di non conformità[59].
Tuttavia, nel campo dell'assistenza sanitaria, il diritto alla cancellazione implica che gli operatori sanitari possono essere costretti a cancellare le cartelle cliniche su richiesta dei pazienti. Di conseguenza, l'integrità delle informazioni contenute nella cartella clinica di un paziente potrebbe diventare difficile da preservare, con possibili ripercussioni negative sull'assistenza sanitaria – in particolare, si potrebbe verificare un problema di "blocco delle informazioni" quando si tenta di accedere alle cartelle cliniche elettroniche dei pazienti[60].

5. Rafforzare gli obblighi: verso una maggiore responsabilità degli attori dei dati

Il GDPR pone grande enfasi su aspetti come trasparenza, correttezza e responsabilità (art. 5, GDPR). Per favorire un approccio preventivo alla protezione della privacy e dei dati personali, il GDPR incoraggia l'adozione di mezzi tecnici prima del trattamento dei dati personali (art. 25 e considerando 78 del GDPR).
Il GDPR richiede inoltre che venga effettuata una valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment* – DPIA) ogni volta che un trattamento di dati possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35, GDPR).
Sebbene siano forniti esempi di tali trattamenti (art. 35.3, GDPR), la formulazione del testo suggerisce che tale elenco non è esaustivo. Di conseguenza, sono state pubblicate delle linee guida per aiutare a determinare quando è necessaria una DPIA[61].

---

[57] E. BANI & E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, cit., p. 154.
[58] *Ibid*.
[59] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 325-326.
[60] D.F. SITTIG *et al.*, *New Unintended Adverse Consequences of Electronic Health Records*, YEAR BMED. INFORM., 2016, p. 16 ss.
[61] Si vedano le linee guida sulla valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment* – DPIA) e sulla determinazione se il trattamento è suscettibile di comportare un rischio elevato ai fini del Regolamento 2016/679.

ISSN 2036-7821

Tra gli altri criteri, un trattamento deve essere considerato suscettibile di comportare un rischio elevato quando coinvolge dati sensibili, dati relativi a soggetti vulnerabili (ad esempio, pazienti), o quando si basa su una nuova tecnologia o su un uso innovativo di una tecnologia esistente. Poiché le applicazioni dell'IA in ambito sanitario si basano solitamente su dati relativi alla salute e spesso costituiscono una novità tecnologica, è probabile che in ultima analisi sia necessaria una DPIA prima di qualsiasi trattamento in questo campo[62].
Come minimo, una DPIA deve riguardare: (i) una descrizione delle operazioni di trattamento e delle finalità del trattamento; (ii) una valutazione della necessità e della proporzionalità del trattamento, nonché dei rischi per gli interessati (visti dal punto di vista dell'interessato); e (iii) un elenco delle misure per mitigare tali rischi e garantire la conformità al GDPR. Un'eccezione all'obbligo di eseguire una DPIA si trova al considerando 91, che prevede specificamente che il trattamento dei dati personali non dovrebbe essere considerato su larga scala se il trattamento riguarda i dati personali di pazienti o clienti da parte di un singolo medico, di un altro operatore sanitario o di un avvocato. In questi casi, una valutazione d'impatto sulla protezione dei dati non dovrebbe essere obbligatoria.
Ancora, il GDPR ha introdotto un nuovo principio di "privacy by default" (art. 25 del GDPR, ovverosia per impostazione predefinita). Questo principio prevede che i mezzi tecnici per la minimizzazione dei dati siano implementati quando si sviluppa una tecnologia. I responsabili del trattamento dei dati sono ora obbligati a predisporre garanzie tecniche che assicurino l'accesso e il trattamento solo dei dati effettivamente necessari per il completamento di finalità predefinite.
Imponendo l'implementazione di meccanismi preventivi come la privacy by design e by default, il GDPR incoraggia la rapida adozione di misure tecniche adeguate per prevenire potenziali violazioni. Questi nuovi obblighi per gli sviluppatori di tecnologie contribuiscono a promuovere l'autoregolamentazione e sono accompagnati da sanzioni significative[63].

6. Riflessioni conclusive

Le opportunità offerte dall'integrazione delle tecnologie di intelligenza artificiale nel campo dell'assistenza sanitaria non devono essere sottovalutate. Gli sviluppi dell'IA possono aiutare a setacciare enormi volumi di dati per individuare schemi e correlazioni ed eseguire calcoli complessi, compiti che le macchine sono in grado di svolgere in maniera più efficiente degli esseri umani.

---

[62] M.B. FORCIER *et al.*, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, cit., pp. 329-330.

[63] Si veda, per un approfondimento, P. VOIGT & A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)*, Springer ed., 2017.

ISSN 2036-7821

Alla luce delle considerazioni elaborate, è plausibile concludere che l'introduzione delle nuove tecnologie nell'attuazione dei diritti fondamentali alla salute potrebbe determinare una trasformazione considerevole per quel che attiene le modalità di erogazione dei servizi sanitari che, comunque, non può prescindere da un attento ruolo di regia e regolazione da parte dei livelli di governo competenti[64].
Molte applicazioni di questo tipo sono già in uso e aiutano gli operatori sanitari a risparmiare tempo e denaro, migliorando la ricerca sanitaria e l'assistenza ai pazienti.
Tuttavia, se gli individui dovessero essere riluttanti a fornire l'accesso ai propri dati personali, l'impatto sarebbe devastante per l'implementazione dell'IA in qualsiasi sistema sanitario.
Una generale perdita di fiducia da parte del pubblico è comprensibile, visti gli esempi di alto profilo di uso improprio dei dati personali, come quello rivelato dal caso *Cambridge Analytica*[65].
I nuovi meccanismi del GDPR volti a prevenire tali usi indesiderati dei dati personali, in particolare attraverso il divieto di scenari di "opt-out" e alcuni requisiti di consenso, potrebbero rappresentare una valida soluzione.
Le specificità dell'IA e i nuovi rischi che ne derivano per la protezione della privacy sono, almeno in parte, affrontati nel GDPR: anche se alcuni meccanismi sembrano restrittivi e potrebbero costituire degli ingombranti ostacoli per gli sviluppatori di IA (come il diritto alla cancellazione).
La responsabilizzazione degli attori in merito alla gestione in senso lato dei dati potrebbe essere la direttrice sulla quale costruire una più solida architrave per il sistema della privacy nel settore sanitario.

[64] E. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, cit., p. 174.

[65] D. SIMBERKOFF, *How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation*, CMS wire, 2018. Disponibile al sito https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation. (ultima consultazione 07/12/2022).

ISSN 2036-7821