LUISS

Dipartimento
di Giurisprudenza

Cattedra di Informatica Giuridica

Intelligenza Artificiale: responsabilità civile e la sua applicazione anche in ambito sanitario

Prof. Gianluigi Ciacci
RELATORE

Prof. Donatella Morana
CORRELATORE

MariaFlavia Staniscia,matr.153953
CANDIDATO

Anno Accademico 2021/2022

INDICE

INTRODUZIONE

La convergenza tra Internet e l'Intelligenza Artificiale (IA) genera uno scenario affascinante e al tempo stesso problematico poiché la rete alimenta l'intelligenza artificiale rendendo disponibili enormi quantità di dati (c.d. Big Data), mentre l'intelligenza artificiale permette alla rete un crescente sfruttamento di quegli stessi dati.

Questo nuovo ecosistema sta trasformando gli assetti economici, politici e sociali, le interazioni tra individui e la stessa vita privata perché, se da un lato, l'implemento dell'utilizzo di Internet e delle IA apre nuove frontiere al benessere e progresso, dall'altro, esso aumenta le opportunità di controllo e manipolazione degli individui, realizzando nuovi pericoli per i valori sociali e i diritti fondamentali quali la salute e il lavoro.

I sistemi di intelligenza artificiale e i dati da essi utilizzati per l'addestramento possono però offrire nuove occasioni per attività illegali e l'uomo potrebbe utilizzare l'intelligenza artificiale per perseguire legittimi interessi economici in modi dannosi per gli individui e la società.

I governi, inoltre, potrebbero servirsi dell'intelligenza artificiale non solo per scopi politici e amministrativi legittimi ma anche per anticipare e controllare il comportamento dei cittadini in modi che limitano le libertà individuali e interferiscono con il processo democratico.

Recentemente, tutte queste problematiche hanno suscitato un vivace dibattito in ambito sanitario, settore in cui l'utilizzo dell'I.A. è sempre più intenso e l'attenzione è stata posta soprattutto sui risultati raggiunti nel campo della chirurgia robotica e nel campo del trattamento dei dati personali sanitari a seguito dello scoppio della pandemia Covid-19.

Numerose sono state le imprese che hanno investito sia nel campo ricerca e sviluppo di nuovi robot medici sempre più autonomi, capaci di eseguire operazioni in completa autonomia, sia nel campo delle tecnologie di contact tracing, e ciò ha suscitato un forte interesse politico soprattutto per le famose applicazioni utilizzate dai governi per contrastare il diffondersi contagio.

La presente ricerca si pone l'obiettivo di verificare se il diritto positivo nazionale, comunitario e interazionale, sia in grado di poter far fronte alle problematiche che potrebbero nascere a seguito dell'utilizzo delle Intelligenze Artificiali nella vita quotidiana

Il primo obiettivo della presente ricerca è quello di verificare se l'errore medico derivante dall'utilizzo di robot autonomi all'interno delle sale operatorie, ovvero nell'impiego della

diagnosi clinica, possa essere fonte di responsabilità civile e, in particolare, se le attuali regole in tema di responsabilità medica possano tutelare il paziente danneggiato.

Il secondo obiettivo è quello di verificare se le attuali norme vigenti in materia di trattamento dei dati sanitari siano state sufficienti per tutelare i diritti fondamentali nell'era Covid-19, dove le imponenti restrizioni e la paura generata dal virus hanno indotto i governi di tutto il mondo a utilizzare l'I.A. al fine di contrastare il diffondersi del virus.

Per raggiungere questi obbiettivi occorrerà in primo luogo capire la nascita e l'evoluzione dell'I.A., il suo funzionamento e la sua capacità di rapportarsi con la vita quotidiana.

Il primo capitolo, infatti, si concentrerà sulla storia e l'evoluzione dell'I.A, i modelli di apprendimento della stessa e i tentativi dell'etica e del diritto di inquadrare questa nuova tecnologia nelle categorie classiche del diritto.

Il secondo capitolo, invece, si concentrerà sul diritto alla privacy: la sua evoluzione e le norme positive in tema di trattamento dei dati personali.

Il terzo capitolo, invece, si concentrerà sulle norme positive in tema di responsabilità civile e, in particolare, la responsabilità civile in campo medico dopo l'introduzione della legge Gelli – Bianco (l. n. 24/2017) e la responsabilità civile per trattamento illegittimo dei dati sanitari.

Per quanto attiene alla responsabilità civile del medico si cercherà di verificare se il settore della responsabilità medica possa essere applicata al medico-robot nel caso in cui quest'ultimo nella diagnosi ovvero nell'intervento, compia un errore tale da mettere in pericolo la salute del paziente.

Per quanto attiene alla responsabilità civile per trattamento illegittimo dei dati sanitari, la ricerca proverà a verificare se le regole stringenti contenute nel Regolamento Ue 2016/679 siano state sufficienti a tutelare i cittadini dalle numerose applicazioni di contact tracing sviluppate per contenere la diffusione del virus Covid-19 e, tale verifica sarà effettuata prendendo in considerazione anche le strategie applicate da diversi stati extra- Ue.

Trattandosi di tecnologie e diritto in costante evoluzione, la presente ricerca non si pone l'obiettivo di fornire verità assolute ma è stata redatta al sol scopo di indurre il lettore a riflettere sull'adeguatezza o meno del diritto positivo a queste nuove tecnologie.

L'esperienza Covid -19 è stata fondamentale per porre l'accento su una realtà che sembrava utopistica, perché è stata il banco di prova per verificare sia l'utilità dell'impiego dell'I.A. in un settore delicatissimo quale quello medico, sia la possibile inidoneità della legislazione positiva vigente a regolare tale fenomeno.

Capitolo 1

Intelligenza artificiale: la storia, l'etica e il diritto positivo

1.1 Storia ed evoluzione dell'intelligenza artificiale.

Con la locuzione Intelligenza Artificiale si è soliti indicare la disciplina che studia se e in che modo si possano riprodurre i processi mentali umani, cercando di avvicinare il funzionamento dei computer alle capacità dell'intelligenza umana, utilizzando le simulazioni informatiche al fine di formulare delle ipotesi in grado di comprendere le dinamiche sottese ai processi evolutivi degli organismi viventi.

La rivoluzione tecnologica e digitale, accompagnata dalla ricerca in aree come le neuroscienze e l'economia, ha accelerato gli studi e l'applicazione dell'Intelligenza Artificiale alla vita quotidiana e, negli ultimi decenni, si è assistito ad un cambiamento radicale sia sotto l'aspetto economico e professionale sia sotto l'aspetto del diritto.

Lo sviluppo dell'Intelligenza Artificiale non ha avuto una storia lineare, essendo stata caratterizzata da periodi di forte interesse scientifico e giuridico ed altri, definiti come "inverni dell'intelligenza artificiale"[1], caratterizzati da numerosi fallimenti e disinteresse della ricerca scientifica in questo campo.

Se dovessimo ipotizzare un "anno zero" dell'Intelligenza Artificiale lo potremmo far coincidere con il 1939, quando il Dr. John Vincent Atanasoff e Clifford E. Berry, dell'Iowa State University, costruiscono "l'Atanasoff Berry Computer" (conosciuto anche come ABC), il primo computer digitale totalmente elettronico.

L'ABC fu la prima macchina ad implementare e utilizzare i numeri binari[2] per rappresentare i numeri e i dati effettuando tutti i calcoli attraverso circuiti elettronici contenuti in un sistema suddiviso in due sottosistemi separati: elaborazione dei dati e memorizzazione.

L'avvento di questa nuova tecnologia portò importanti studiosi a elaborare nuove definizioni di scienza: nel 1950 Alan Turing pubblicò, sulla rivista "Mind", uno dei primi articoli sull'intelligenza artificiale dal titolo "*Computing machinery and intelligence"*, descrivendo quello che sarebbe divenuto poi noto come il test di Turing: criterio utilizzato per

[1] Cosi Nielsson N. J., The Quest for Artificial Intelligence, p. 1-707, Print version published by Cambridge University Press http://www.cambridge.org/us/0521122937 (5 maggio 2022)

[2] Cosi in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Treccani on line, definizione di sistema binario, https://www.treccani.it/enciclopedia/codice-binario, (5 maggio 2022) : *Il sistema binario è un sistema di numerazione posizionale in base due; la base è generalmente indicata come pedice della sequenza delle cifre. In tale sistema, utilizzato per rappresentare i numeri in un elaboratore elettronico, essendo il bit il dato elementare registrabile su supporti elettronici a due stati, ci sono soltanto due cifre, 0 e 1 (→ aritmetica finita (di macchina)). Dato un numero binario, il suo corrispondente decimale si ottiene sviluppandolo secondo le potenze di 2.(*

verificare le capacità di apprendimento di una macchina e, in particolare, appurare se una macchina potesse essere in grado di esibire un comportamento intelligente, pari all'essere umano[3].

Il termine Intelligenza Artificiale venne però coniato solo più tardi, nel 1956, dal matematico John McCarthy, per poter distinguere questo campo di ricerca dalla già nota cibernetica, che lo utilizzò in un seminario estivo denominato "Summer Research Project on Artificial Intelligence", organizzato al fine di ideare una macchina in grado di simulare l'intelligenza umana[4].

Gli anni successivi furono incentrati sullo studio, lo sviluppo e l'apprendimento di questo nuovo e autonomo campo scientifico: i matematici Warren McCulloch e Walter Pitts idearono una rete neurale artificiale utilizzando delle porte logiche e applicando metodi statistici che saranno successivamente, nel 1958, ripresi dallo psicologo americano Frank Rosenblatt per progettare un modello base di reti neurali che dimostrasse che quest'ultime avevano un grande potenziale nelle operazioni di apprendimento (tale modello base fu denominato "percettone[5]"); nel 1959, lo stesso McCarthy ideò il "Lisp" (List Processor), il primo linguaggio di programmazione funzionale di tipo dichiarativo che si basa sul concetto di programma come

[3] Così Mininni A., Il test di Turing, https://www.andreaminini.com/ai/test-di-turing/, (6 maggio 2022): Turing per elaborare il suo test prende spunto da un gioco, chiamato "gioco dell'imitazione" in cui partecipano tre soggetti che, per comodità, indicheremo come A, B e C. In questo gioco C è tenuto separato dagli altri due e può solo stabilire tramite una serie di domande scritte qual è l'uomo e qual è la donna; A e B hanno dei compiti prestabiliti: A deve ingannare C e portarlo a fare un'identificazione errata, mentre B dovrebbe aiutarlo a mantenere una identificazione corretta. Se noi sostituissimo, ad esempio, A con una macchina, e quest'ultima riuscisse ad ingannare C, mantenendo invariata la percentuale di volte in cui C indovina chi sia l'uomo e chi la donna, allora l'algoritmo dovrebbe essere considerato intelligente, dal momento che – in questa situazione – sarebbe indistinguibile da un essere umano.

[4] Così Haenlein M. E Kaplan. A. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence." California Management Review Volume: 61 fascicolo: 4, p. 5-14 Articolo pubblicato per la prima volta online il 17 luglio 2019, https://doi.org/10.1177/0008125619864925, (6 giugno 2022)

[5] Cosi Cappelli M., Enciclopedia Treccani, - Enciclopedia della Scienza e della Tecnica (2008): https://www.treccani.it/enciclopedia/percettrone_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/ (06 giugno 2022) definizione di Percettore: *Modello base di rete neurale proposto nel 1958 dallo psicologo americano Frank Rosenblatt. Sebbene sia oggi considerato datato, rappresenta tuttavia il modello di partenza per la progettazione di reti complesse. Il percettrone fu proposto come entità con un ingresso, un'uscita e una regola di apprendimento basata sulla minimizzazione dell'errore (error back-propagation). Rappresenta un modello computazionale più generale di quello di McCulloch-Pitts, grazie all'introduzione di pesi numerici e di uno speciale percorso di interconnessione. Nel modello originale le unità di calcolo sono elementi con soglia e la connessione è ricavata stocasticamente. L'apprendimento o la memorizzazione vengono ottenute per retroazione adattando i pesi numerici fintantoché l'uscita non sia resa pari a quella desiderata. Le capacità computazionali di un singolo percettrone non sono però elevate e le prestazioni ottenibili dipendono sia dall'insieme degli ingressi sia dalla funzione da implementare. Il modello di Rosenblatt (detto percettrone classico), proposto al Cornell Aeronautical Laboratory, venne poi perfezionato negli anni Sessanta del secolo scorso grazie anche al lavoro di Marvin Minsky e Seymour Papert. Oggi con il termine percettrone si intende proprio il modello proposto da questi ultimi. Il percettrone classico è in realtà una vera rete per la soluzione di problemi di riconoscimento di percorso, in quanto si basa sull'idea fondamentale di far apprendere al sistema un metodo di riconoscimento di specifici percorsi di ingresso. Più precisamente, il percettrone (esempio di rete in avanti a uno strato) rappresenta un caso particolare di rete neurale con uscite indipendenti tra loro. È proprio tale proprietà che rende lo studio del percettrone basilare per un suo impiego come modello elementare di una più vasta rete neurale composta di numerosi neuroni. Le unità elementari di un percettrone possono rappresentare funzioni booleane di base (AND, OR, NOT), mentre una rete con più strati potrebbe rappresentare qualsiasi funzione booleana. Un percettrone a singolo strato può invece rappresentare solo determinate funzioni booleane (AND e OR, ma non XOR)."*

funzione (tutte le strutture di dati, infatti, sono caratterizzate da liste chiamate S-expressioni, dove S sta per simbolico e la caratteristica di questa struttura è data dall'uso della notazione prefissa racchiusa tra parentesi (→ notazione))[6].

Il punto di svolta si ebbe negli anni '70, quando fecero la loro prima comparsa i sistemi esperti [7] (s.e), tra quali possiamo ricordare, il sistema *MYCIN*[8], che rappresenta il capostipite di numerosi s.e. diagnostici e capace di riconoscere malattie infettive del sangue, e il sistema *HEARSAY*[9] basato sull'analisi del linguaggio parlato e in grado di comprendere il discorso "connesso" basato su un vocabolario di un migliaio di parole.

I s.e si differenziano dai primi "problem solver" poiché utilizzano conoscenze e tecniche di ragionamento al fine di risolvere problemi che normalmente richiederebbero l'ausilio di uno specialista "umano" e sono in grado di giustificare autonomamente problemi, anche complessi, appartenenti a uno specifico campo di competenza, senza che il programmatore abbia esplicitamente e preventivamente considerato tutte le possibili varianti del problema stesso.[10]

Il successo avuto negli anni '70 dalle prime Intelligenze Artificiali fece sì che nel ventennio successivo i computer registrarono una notevole crescita sia nella capacità di memoria che nella potenza di calcolo computazionale e la nuova Intelligenza Artificiale venne applicata in numerosi campi scientifici, quali ad esempio il sistema DENDRAL[11] in chimica, utilizzato per interpretare i dati di analisi spettrografica di un composto organico e formulare ipotesi sulla sua struttura, e il sistema MYCIN in ambito sanitario per l'analisi dei dati sanitari informatizzati[12].

---

[6] Così in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia della Matematica, Lisp, (07 maggio 2022), https://www.treccani.it/enciclopedia/lisp_%28Enciclopedia-della-Matematica%29/#:~:text=Il%20lisp%20si%20basa%20sul,tra%20parentesi%20(%E2%86%92%20notazione). : Tale notazione è utilizzata indifferentemente sia per la scrittura del codice sorgente sia per i dati e, per questa sua capacità il LISP è stato usato prevalentemente in ambiti di ricerca sull'intelligenza artificiale quali sistemi esperti, robotica, giochi e riconoscimenti di schemi.

[7] Cosi in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Italiana - V Appendice (1994), Sistemi Esperti (7 maggio 2022), https://www.treccani.it/enciclopedia/sistemi-esperti_%28Enciclopedia-Italiana%29/#:~:text=I%20s.e.%20sono%20programmi%20per,ricerca%20in%20intelligenza%20artificiale%20,"I s.e. sono programmi per calcolatore che cercano di riprodurre le prestazioni di esperti umani nella risoluzione di problemi. Essi rappresentano il più conosciuto risultato pratico della ricerca in intelligenza artificiale (v. in questa Appendice), pur non essendo rappresentativi della ricchezza di obiettivi e di approcci di quest'ultima. L'intelligenza artificiale, a sua volta, si può considerare una branca dell'informatica, ma è anche intimamente collegata con altre discipline, come la scienza cognitiva, la logica formale, la linguistica computazionale e lo studio dei processi decisionali".

[8] Così Shortliffe E. H, "Computer-Based Medical Consultations: MYCIN", Elsevier Computer Science Library, Amsterdam 2012, Vol. 2 p.1-264

[9] Così Hart P.E., Duda R. O., Einaudi M.T., Prospector- A Computer-Based Consultation System For Mineral Exploration, In Journal Of The International Association For Mathematical Geology 10, 1978, P. 589-610.

[10] Cosi in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Della Matematica Treccani (2013), Sistema Esperto, https://www.treccani.it/enciclopedia/sistema-esperto_%28Enciclopedia-della-Matematica%29/, (10 Maggio 2022)

[11] Così Lederberg J., "How DENDRAL Was Conceived And Born." In Proceedings Of ACM Conference On History Of Medical Informatics, 1987, P. 5-19, https://dl.acm.org/doi/10.1145/41526.41529 , (11 maggio 2022).

[12] Cosi Tripathi, M." EHR Evolution: Policy and Legislation Forces Changing the EHR", in Journal of AHIMA 83, n.10 (ottobre 2012): p. 24-29..

Negli anni ’80, sulla base degli studi dei fisici Paul Benioff, Richard Feynman e del matematico russo Yuri Manin[13], si iniziò a teorizzare la possibilità di creare un super elaboratore, oggi definito “computer quantistico”, in grado di sfruttare le leggi della meccanica e della fisica quantistica per oltrepassare finalmente i limiti dei cosiddetti super computer, spalancando di fatto le porte ai nuovi e interessantissimi orizzonti dell’Intelligenza Artificiale.

Negli anni ‘ 90 gli studi divennero più complessi e finalizzati a far replicare alle macchine il ragionamento seguito dal cervello umano (è di quegli stessi anni l’incontro di scacchi fra il supercomputer “Deep Blue”, costruito dall’IBM, contro il campione mondiale di scacchi russo Garry Kasparov [14]) tuttavia, si fece sempre più strada l’esigenza di utilizzare l’Intelligenza Artificiale quotidianamente e l’evoluzione degli studi sulla robotica, che nei capitoli successivi verranno analizzati per quanto riguarda il campo medico, portarono al raggiungimento di tale obiettivo.

Oggi, possiamo fare nostra la definizione dell’Università di Stanford che identifica l’I.A. come “***una scienza ovvero 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*”[15],** perché essa realizza due capacità particolarmente importanti: la connettività e la possibilità di aggiornamento, che permetteranno, tramite le ricerche neuroscientifiche sul cervello umano, alle macchine di evolversi e di acquisire competenze e caratteristiche umanoidi.

Il fine sopra citato è stato perseguito soprattutto in campo biologico ed informatico e il mondo del diritto ha cercato di regolare tali ambiti al fine di tutelare l’uomo e le sue libertà poiché, il problema che si riscontra, soprattutto nella quotidianità, è quello di regolamentare il rapporto uomo-macchina e di poter individuare le eventuali responsabilità nel caso in cui l’utilizzo o la costruzione dei nuovi dispositivi intelligenti arrechino dei danni all’utilizzatore ovvero ai terzi.

---

[13] Così Prati E., Mente Artificiale, Egea S.P.A, Milano, 2017 P. 1-188

[14] Così in, Encyclopædia Britannica, Inc, Deep Blue, Computer Chess-Playing System, https://www.britannica.com/topic/Deep-Blue (5 maggio 2022): il deep blue è un sistema di gioco di scacchi per computer progettato da Ibm all'inizio degli anni '90. come successore dichiptest edeep thought , i primi computer per scacchi appositamente costruiti, deep blue è stato progettato per avere successo dove tutti gli altri avevano fallito. nel 1996 ha fatto la storia sconfiggendo il gran maestro Russogarry Kasparov in una delle loro sei partite: la prima volta che un computer vinceva una partita contro un campione del mondo in condizioni di torneo. nella rivincita del 1997, vinse la sesta partita decisiva in sole 19 mosse; la sua vittoria per 3,5–2,5 (ha vinto due partite e ha avuto tre pareggi) ha segnato la prima volta che un campione del mondo in carica ha perso una partita contro un computer in condizioni di torneo. nella sua configurazione finale, il computer Ibm rs6000/sp utilizzava 256 processori che lavoravano in tandem, con la capacità di valutare 200 milioni di posizioni degli scacchi al secondo. la vittoria a scacchi di deep blue contro Kasparov avvenuta nel 1996 conquistò un'enorme visibilità sui mass media, mostrando al mondo che l'intelligenza artificiale poteva sostituirsi all'uomo nel prendere le decisioni e risolvere anche problemi molto complessi.

[15] D’Avack L., LA Rivoluzione Tecnologica E La Nuova Er Digitale: Problem Etici, In AA.VV. Intelligenza Artificiale Il Diritto, I Diritti, L’etica, Giuffrè Francis Lefebvre S.P.A, Milano, 2020 A Cura Di Ugo Ruffolo, P.5, Nota N.7.

Oggi, la razza umana interagisce con la razza umanoide "I.A." in molti campi della vita quotidiana si pensi, ad esempio, al frequente utilizzo delle nuove tecnologie quali le blockchain[16], l'ingegneria genetica[17], il machine learning[18], intelligenza artificiale[19], i big data[20], gli algoritmi[21], il cloud computing[22] etc. [23] e, il nuovo potere tecnologico rende la gente comune sempre più irrilevante di fronte all'ingente utilizzo dell'intelligenza artificiale e ciò concretizza il rischio di declassare l'uomo da attore principale a comparsa della vita civile [24].

---

[16] Cosi in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Neologismi 2018, "Blockchain" https://www.treccani.it/enciclopedia/blockchain_%28altro%29/#:~:text=s.%20f.%20inv.,nodo%2C%20per%20assicurarne%20la%20tracciabilit%C3%A0.&text=%C2%ABDagli%20anni%20Settanta%20il%20legame,allentato%2C%20fino%20alla%20finanziarizzazione%20attuale. (06 maggio 2022): f. inv. Tecnologia Basata Su Una Catena Di Blocchi Che Registrano E Gestiscono Le Operazioni Contabili Accessibili Solo Agli Utenti Di Ciascun Nodo, Per Assicurarne La Tracciabilità.

[17] Cosi In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedie On Line, Ingegneria Genetica, https://www.treccani.it/enciclopedia/ingegneriagenetica/#:~:text=Insieme%20di%20tecnologie%20che%20permettono,(%E2%9E%94%20biotecnologie%2C%20genetica), (6 maggio 2022): Insieme Di Tecnologie Che Permettono La Manipolazione In Vitro Di Molecole Di DNA, In Modo Da Provocare Cambiamenti Predeterminati Nel Genotipo Di Un Organismo (➔ Biotecnologie, Genetica). Mediante Queste Manipolazioni Genetiche È Possibile Produrre Nuove Combinazioni Di Geni, Determinare Specifiche Mutazioni, Introdurre Geni In Cellule In Cui Essi Possono Esprimere Nuove Funzioni."

[18] Cosi in Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Neologismi (2019), machine learning, https://www.treccani.it/vocabolario/machinelearning_%28Neologismi%29/#:~:text=le%20m.,computazionale%20e%20l'ottimizzazione%20matematica. (6 maggio 2022): loc. s.le m. inv. Branca Dell'intelligenza Artificiale Che Si Occupa Dello Sviluppo Di Algoritmi E Tecniche Finalizzate All'apprendimento Automatico Mediante La Statistica Computazionale E L'ottimizzazione Matematica.

[19] Cosi In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia On Line, Intelligenza Artificiale, https://www.treccani.it/enciclopedia/intelligenza-artificiale (6 maggio 2022): Disciplina Che Studia Se E In Che Modo Si Possano Riprodurre I Processi Mentali Più Complessi Mediante L'uso Di Un Computer. Tale Ricerca Si Sviluppa Secondo Due Percorsi Complementari: Da Un Lato L'i. Artificiale Cerca Di Avvicinare Il Funzionamento Dei Computer Alle Capacità Dell'intelligenza Umana, Dall'altro Usa Le Simulazioni Informatiche Per Fare Ipotesi Sui Meccanismi Utilizzati Dalla Mente Umana."

[20] Cosi In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Neologismi (2012), Big Data, https://www.treccani.it/vocabolario/big-data_res-007d6462-8995-11e8-a7cb-00271042e8d9_%28Neologismi%29/ (6 maggio 2022): Loc. S.Le M. Pl. Ingente Insieme Di Dati Digitali Che Possono Essere Rapidamente Processati Da Banche Dati Centralizzate.

[21] Cosi In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Vocabolario On Line, Algoritmo , https://www.treccani.it/vocabolario/algoritmo/ (6 maggio 2022): "Termine, derivato dall'appellativo al-Khuwārizmī («originario della Corasmia») del matematico Muḥammad ibn Mūsa del 9° sec., che designa qualunque schema o procedimento sistematico di calcolo (per es. l'a. euclideo, delle divisioni successive, l'a. algebrico, insieme delle regole del calcolo algebrico ecc.). Con un a. si tende a esprimere in termini matematicamente precisi il concetto di procedura generale, di metodo sistematico valido per la soluzione di una certa classe di problemi. Come esempio consideriamo un a. che codifica un comportamento assai comune, quello di una persona che confronta due parole. Esprimeremo questo a. in un linguaggio naturale un po' rigido, tenendo presente che questa descrizione informale dell'a. è il punto di partenza anche per il disegno di nuovi algoritmi. A volte si usa, per lo stesso scopo, una rappresentazione grafica equivalente, il cosiddetto diagramma di flusso".

[22] Cosi In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia On Line, Cloud Computing , https://www.treccani.it/enciclopedia/cloudcomputing/#:~:text=Letteralmente%20%E2%80%9Cnuvola%20informatica%E2%80%9D%2C%20termine,e%20archiviare%20dati%20in%20rete. (6 maggio 2022): Letteralmente "Nuvola Informatica", Termine Con Cui Ci Si Riferisce Alla Tecnologia Che Permette Di Elaborare E Archiviare Dati In Rete. In Altre Parole, Attraverso Internet Il C.C. Consente L'accesso Ad Applicazioni E Dati Memorizzati Su Un Hardware Remoto Invece Che Sulla Workstation Locale. Per Le Aziende Di Grosse Dimensioni Implica Dunque Un Ingente Abbattimento Dei Costi; Non Sono Più Necessari Hardware Potenti (Costosi E Soggetti A Frequenti Manutenzioni), Ma Basta Una Macchina In Grado Di Far Funzionare L'applicativo D'accesso Alla "Nuvola". Non Mancano Però Le Perplessità; Da Un Lato I File Sono Accessibili Solo Tramite Rete, Dall'altro (Nonostante Le Rassicurazioni Dei Fornitori) Si Teme Per La Sicurezza Dei Dati Sensibili. Il C.C. Può Mettere A Disposizione Hardware In Remoto (Iaas - Infrastructure As A Service), Piattaforme Software (Paas - Platform As A Service) O Software In Remoto (Saas - Software As A Service)."

[23] Così in D'Avack L., op. cit. p.7

[24] Così in Benanti P., Le macchine sapienti, Marietti 1820, Bologna 2018, pp. 157

1.2 Processo decisionale e modelli di apprendimento: dalla scienza alle problematiche applicative

L'analisi della ricerca di strumenti di tutela non può prescindere dal comprendere cosa si intenda per Intelligenza Artificiale a livello tecnico e, soprattutto, quali sono ad oggi i modelli di apprendimento delle stesse.

La problematica già esposta in merito alla corretta definizione di Intelligenza Artificiale rende complessa anche la sua definizione in ambito tecnico; tuttavia, alcuni studiosi identificano l'Intelligenza Artificiale con quella branca delle scienze informatiche e dell'ingegneria che imita le funzioni cognitive degli esseri umani, mediante il ricorso ad algoritmi, i quali possono essere spiegati come sequenze di istruzioni elementari, sottoforma di linee di codice, utilizzati per creare artefatti in grado di replicare il cosiddetto "comportamento intelligente"[25].

Prima di analizzare il piano applicativo dell'I.A, occorrerà dare delle definizioni base di Algoritmo, Machine Learning, Reti Neurali e Deep Learning al fine di poter comprendere come le stesse ragionano e si rapportano con il mondo esterno.

L'algoritmo identifica una successione di istruzioni che definiscono le operazioni da eseguire sui dati per ottenere i risultati e si caratterizza per essere composto da un numero finito di istruzioni che devono presentare un punto di inizio e un punto di fine, ossia il punto da dove iniziare il procedimento risolutivo e il punto che si deve raggiungere affinché si possa interrompe l'esecuzione delle istruzioni.

Il Machine Learning, invece, è un sottoinsieme dell'intelligenza artificiale (AI) che si occupa di creare sistemi che apprendono o migliorano le performance in base ai dati che si utilizzano. E sul piano applicativo l'I.A. consiste in sistemi di software, eventualmente incorporati in hardware, che agiscono nella dimensione fisico digitale percependo l'ambiente che li circonda, attraverso l'acquisizione e l'interpretazione di dati e, ragionando sulla conoscenza pregressa e elaborando le informazioni ricavate da tali dati, assumo la migliore azione da intraprendere per il raggiungimento dello specifico obiettivo dato. [26]

I termini machine learning e I.A. sono spesso utilizzati come sinonimi ma non hanno lo stesso significato in quanto si potrebbe affermare che il machine learning rientra

[25] Shapiro S. C., Encyclopedia Of Artificial Intelligence. Second Edition Vol. 1, John Wiley & Sons Inc; University Of Michigan, 31 Gennaio 1992, P. 1-1792

[26] Cosi Cerea F., Intelligenza Artificiale A Servizio Dei Pazienti Per Il Contrasto A Covid-19, In Rivista Diritti E Persona, Supplemento Ngcc 3/2020, Wolters Kluwer S.P.A. Pp.. 45-49

nell'intelligenza artificiale ma non la esaurisce poiché, il concetto di intelligenza artificiale non include esclusivamente il machine learning.

Gli algoritmi sono i motori che alimentano il Machine Learning e nel campo dell'apprendimento automatico si è soliti distinguere tre approcci principali: l'apprendimento per rinforzo, l'apprendimento non supervisionato e l'apprendimento supervisionato.

L'apprendimento per rinforzo (addestramento per rinforzo), permette al sistema di apprendere dai risultati delle azioni proprie o altrui e, in questo modo, il sistema è in grado di distinguere successi e fallimenti ed applicare autonomamente ricompense e penalità ad essi associate.[27]

L'apprendimento non supervisionato, invece, permette al sistema di apprendere senza ricevere indicazioni o istruzioni dall' esterno e, tale tipo di apprendimento, viene soprattutto utilizzato per il "*clustering*", cioè per raggruppare all'interno di un insieme gli elementi che presentano similarità o connessioni rilevanti.

L'apprendimento supervisionato, viceversa, permette al sistema di apprendere attraverso la supervisione o l'insegnamento (*c.d- training set*) che viene fornito tramite un addestramento a coppie, ciascuna delle quali collega la descrizione di un caso alla risposta corretta.

Tale ultima metodologia di apprendimento è oggi l'approccio più utilizzato e viene applicato in numerosi campi della vita quotidiana come, ad esempio, nei sistemi progettati per riconoscere oggetti all'interno di immagini, nei sistemi di selezione del personale, nei sistemi che raccomandano prodotti per l'acquisto, nei sistemi di valutazione delle richieste di prestito.

L'algoritmo di apprendimento del sistema utilizza l'insieme di addestramento per costruire un modello computazionale, come ad esempio una rete neurale, un albero decisionale o un insieme di regole e tale modello ha lo scopo di catturare la conoscenza originariamente presente nell'insieme di addestramento, ossia la correlazione che esiste fra casi e risposte,[28]e di trasformarla in conoscenza per l'I.A.

Le Reti Neurali, che per completezza espositiva verranno analizzate successivamente nella parte inerente ai big. data, costituiscono un sottoinsieme del machine learning e identificano l'elemento centrale degli algoritmi di deep learning.

[27] AA.VV. Intelligenza Artificiale Il Diritto, I Diritti, L'etica, Giuffrè Francis Lefebvre S.P.A, Milano, 2020 A Cura Di Ugo Ruffolo, Pp. 1-648

[28] Ibidem

Il Deep Learning fa parte della più ampia famiglia di metodi di Machine Learning e si basa sull'apprendimento non supervisionato di livelli gerarchici multipli di caratteristiche (e di rappresentazioni) dei dati che sfruttano una classe di algoritmi di apprendimento automatico e li applicano nei vari livelli di unità non lineari a cascata per svolgere compiti di estrazione di caratteristiche e di trasformazione.

Le architetture di Deep Learning sono state applicate nella computer vision, nel riconoscimento automatico della lingua parlata, nell'elaborazione del linguaggio naturale, nel riconoscimento audio, nella bioinformatica etc.

Effettuate tali precisazioni terminologiche, occorrerà ora verificare i processi di addestramento dell'I.A, ponendo l'attenzione all'addestramento supervisionato e al suo utilizzo nel campo della raccolta di dati personali anche sanitari.

In relazione all'addestramento supervisionato, esso viene spesso utilizzato per l'inserimento di dati che vertono su caratteristiche e comportamenti individuali e sociali: l'intelligenza artificiale viene impiegata in molti campi della vita quotidiana e si è dimostrata determinante anche in campo medico per la diagnosi e l'individuazione di terapie personalizzate.

Inoltre, l'utilizzo dei sistemi artificiali basati sui dati personali presuppone e stimola la creazione di ampi insiemi di dati, i cosiddetti *Big Data*, la cui raccolta è facilitata dall'utilizzo da parte delle persone fisiche dei personal computer collegati a Internet, il quale rappresenta uno dei più potenti mezzi di raccolta e diffusione dell'informazione su scala globale.

L'integrazione dell'intelligenza artificiale ai Big Data consente di affrontare le grandi sfide dell'umanità. quali ad esempio preservare un ambiente salubre, fornire risorse alla popolazione, sconfiggere le malattie, eliminare la povertà etc.[29] e negli ultimi anni il rifiorire delle potenzialità delle intelligenze artificiali è dovuto sostanzialmente a due fattori, da un lato la crescita esponenziale della quantità di dati informatizzati disponibili e in continuo aggiornamento e dall' altro dal miglioramento delle capacità di calcolo delle tecnologie informatiche.

Tali dati vengono estratti tramite il processo di *Data Mining*, che consiste nell' estrazione di informazioni significative e comprensibili a partire da grandi quantità di dati (Big Data), attraverso algoritmi automatici o semi automatici e processo generale di *Machine Learning*

[29] Ibidem: *"L' intelligenza artificiale, in combinazione con le grandi masse di dati, può permettere agli scienziati di scoprire correlazioni, formulare ipotesi e di sviluppare modelli basati sull' evidenza; ai medici di fornire diagnosi più accurate, e cure mirate e personalizzate; alle imprese di anticipare le tendenza dei mercati e adottare le decisioni più efficienti; ai consumatori di compiere scelte più informate e ottenere servizi personalizzati; alle autorità pubbliche di identificare i rischi, prevenire i danni, ottimizzare la gestione di beni pubblici (es: l'ambiente) e coordinare le azioni dei cittadini (es: la gestione del traffico e i consumi energetici)."*

(ML) nella sua declinazione di Deep Learning, permette di processare una quantità maggiore di dati anche in formati diversi e non precedentemente etichettati e classificati come video, audio, testi, i quali tramite il Data Mining (DM) vengono estratti per far affiorare una nuova conoscenza nascosta nella complessità dei Big Data.[30]

Una più recente ed efficiente modalità di ML utilizza reti neuronali artificiali (*Artificial Neuronal networks, ANNs)*[31] che si ispirano al modello di architettura neuronale della corteccia encefalica umana e per il loro funzionamento si prevede un addestramento dapprima supervisionato dall'uomo e poi gradualmente sempre più autonomo.

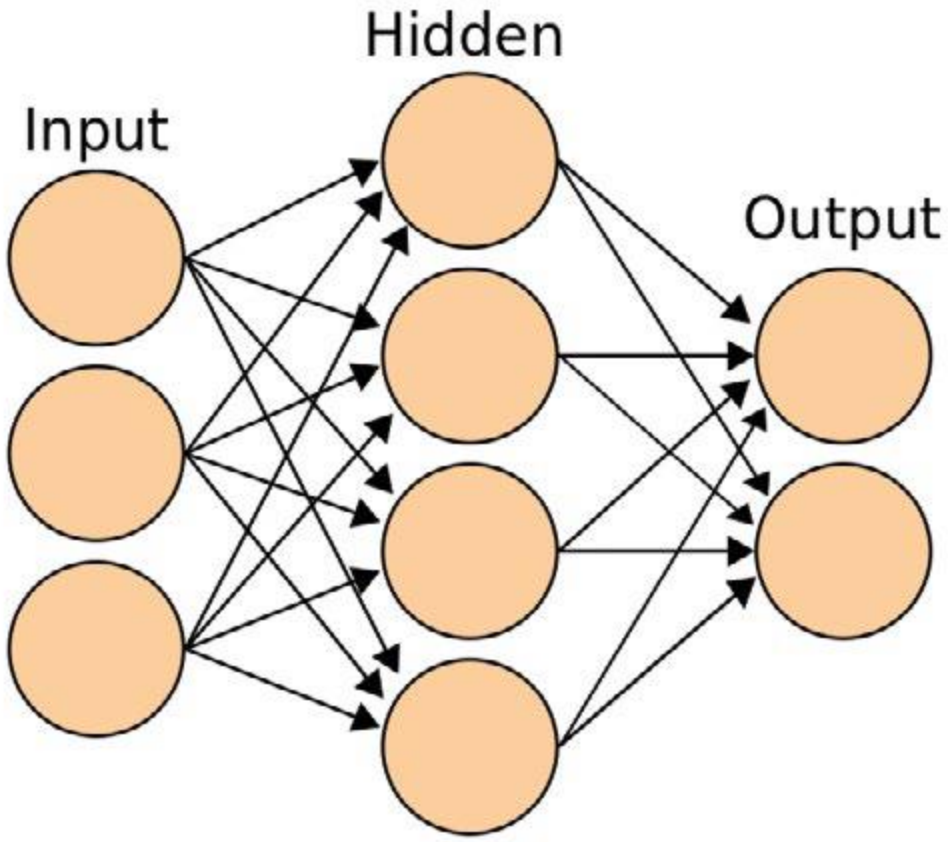
Tecnicamente, le ANNs sono composte da strati multipli interconnessi di neuroni di input, hidden e output e le connessioni tra di essi si rafforzano quando aiutano la macchina ad arrivare alla risposta corretta, in caso contrario si indeboliscono; tale meccanismo di addestramento permette di perfezionare il ragionamento dell'intelligenza artificiale, la quale nel corso dell'addestramento può affinare un algoritmo fino al punto di raggiungere un grado elevato di accuratezza.[32]

[30] Malva A. E Zurlo V., La Medicina Nell' Era Dell' Intelligenza Artificiale: Applicazioni In Medicina Generale, In Rivista Società Italiana Di Medicina Generale N.4 , Vol.6 , 2019 Pp. 28-31.

[31] Cosi Martinelli G., In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia Italiana - V Appendice (1994), Definizione Reti Neurali, https://www.treccani.it/enciclopedia/reti-neurali_%28Enciclopedia-Italiana%29/#:~:text=La%20r.n.%20%C3%A8%20un%20insieme,reale%20come%20il%20sistema%20nervoso. , (09 maggio 2022): "La R.N. è un insieme di elementi semplici interconnessi in parallelo in larga misura, la cui organizzazione gerarchica è progettata in modo da interagire con gli oggetti del mondo reale come il sistema nervoso. l'aspetto più tipico della R.N. è la capacità di acquisire ''esperienza'', nel senso di autorganizzarsi sulla base di esempi del compito che deve svolgere"..

[32] Malva A. E Zurlo V. op. cit. (Figura 1)

Una rete neuronale artificiale può essere così illustrata:



(Figura 1)[33]

I numerosi passi avanti nell'utilizzo dell'I.A. nella vita quotidiana potrebbe produrre l'effetto di peggiorare la vita dell'essere umano, poiché questo ultimo, in alcune attività lavorative, potrebbe essere sostituito dalle macchine rendendo superfluo l'apporto umano e, inoltre, la raccolta massiva di dati personali potrebbe cagionare un danno alla riservatezza, rendendo ostensibili dei dati che dovrebbero rimanere privati.

Il possibile utilizzo dell'intelligenza artificiale in contesti quali la finanza o la classificazione del comportamento umano potrebbe portare a risultati paradossali come quelli evidenziati da Cathy O'Neil nella sua opera "*Weapons of math destruction: how big data increases inequality and threatens democracy"* il quale, studiando il funzionamento degli algoritmi li identifica quali possibili armi di distruzione matematica.*[34]*.

[33] Malva A. E Zurlo V. op. cit. (Figura 1)

[34] O'Neill C., Weapons Of Math Destruction: How Big Data Increases Inequality And Threatens Democracy, Penguin Books Ltd, Crown 2017 Pp. 1-272: " un algoritmo elabora un sacco di statistiche e ne estrae una probabilità che una certa persona possa

Pertanto, l'alternativa al processo decisionale totalmente automatizzato resterebbe quella delle decisioni umane, correlate dalle loro imperfezioni, e, al fine di non cadere da un estremismo all'altro, gli studiosi del diritto stanno cercando di regolare l'utilizzo delle intelligenze artificiali partendo dai valori dell'etica e tentando di positivizzare delle regole di condotta volte a preservare i basilari diritti di una società democratica.

1.3 Le intelligenze artificiali tra diritto positivo ed etica

Nell'epoca moderna si è avvertita sempre più l'esigenza di bilanciare l'utilizzo dell'intelligenza artificiale e il rispetto dei diritti dello stato democratico e, al fine di poter garantire il rispetto delle libertà individuali costituzionali, gli studiosi e i giuristi contemporanei utilizzano gli strumenti di diritto esistenti e le regole etiche delineate Gruppo di lavoro AI4People, costituito su iniziativa dell'Unione Europea.

In via preliminare, occorre sottolineare che a livello giuridico non esiste una vera e propria definizione di Intelligenza Artificiale o di ''Machine Learning'' e come anticipato l'espressione Intelligenza Artificiale è stata in origine coniata da John McCarthy e altri studiosi che l'hanno definita come "la scienza e la tecnologia di rendere intelligenti le macchine"[35].

Interessante è la distinzione tra Intelligenza Artificiale debole (weak AI) che racchiude al suo interno sistemi in grado di simulare alcune funzionalità cognitive dell'uomo senza tuttavia raggiungere le capacità intellettuali tipiche dello stesso (si tratta, a grandi linee, di programmi di problem-solving in grado di replicare alcuni ragionamenti logici umani per risolvere problemi, prendere decisioni, ecc. come nel gioco degli scacchi) e Intelligenza Artificiale forte (strong AI) all'interno della quale si fanno rientrare i sistemi in grado di diventare sapienti o addirittura coscienti di se´.[36]

Le prime norme positive europee in tema di Intelligenza artificiale sono state promulgate con il nuovo regolamento europeo[37] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il quale introduce non solo regole più chiare in materia di informativa e consenso ma riscrive, altresì`, la disciplina applicabile alle decisioni

essere una cattiva assunzione, un mutuatario rischioso, un terrorista, o un insegnante scadente. Questa probabilità è distillata in un punteggio, che può sconvolgere la vita dell'interessato. E tuttavia quando la persona reagisce, prove in contrario, meramente "evocatrici" semplicemente non funzionano. La contestazione deve essere inoppugnabile. Le vittime umane delle armi di distruzione matematica (…) sono tenute ad uno standard di prova molto più alto rispetto gli algoritmi"

[35] McCarthy J., Minsky M. L., Rochester N., Shannon C.E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf. (13 maggio 2022)

[36] Cosi Uricchio A., Robot Tax: Modelli Di Prelievo E Prospettive Di Riforma, In Giurisprudenza Italiana N. 7/2019, Utet Giuridica, Torino Luglio 2019 Pag 1751

[37] Reg. UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, che ha abrogato la dir. 1995/46/CE.

automatizzate, oggetto di specifica considerazione negli artt. 13, 14, 15 e 22 Regolamento UE 679/2016 (cd. GDPR).[38]

Il GDPR fornisce le nuove coordinate utili alla ricostruzione del quadro normativo volto a garantire che la profilazione e il processo decisionale individuale automatizzato non siano utilizzati in modo tale da incidere ingiustificatamente sui diritti fondamentali degli individui.

L'art 4 par. 4 del Reg. UE n. 679/2016, fornisce la definizione di profilazione a livello europeo e la identifica come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità , il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".[39]

Il profilo si caratterizza quindi per la concorrente presenza di tre elementi:

- si deve trattare di una forma automatizzata di elaborazione
- deve essere effettuato su dati personali
- l'obiettivo deve essere quello di valutare aspetti personali di un soggetto.

Il processo decisionale automatizzato ha una portata diversa e può parzialmente sovrapporsi o risultare dalla profilazione, nel senso che decisioni automatizzate possono essere prese con o senza profilazione (e la profilazione può non essere funzionale a decisioni automatizzate) e in maniera parzialmente o totalmente automatizzata.[40]

Il processo decisionale automatizzato viene espressamente regolato dall'art 22[41] del GDPR, il cui contenuto può essere così` sintetizzato: l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo

[38] Così Pellecchia E., Profilazione E Decisioni Automatizzate Al Tempo Della Black Box Society: Qualità Dei Dati E Leggibilità Dell'algoritmo Nella Cornice Della Responsible Research And Innovation, In Le Nuove Leggi Civili Commentate 5/2018, Nlcc 5/2018 Wolters Kluwer S.P.A. Pp. 1209-1235

[39] Art.4 par 4 Reg. UE n. 679/2016

[40] Così Pellecchia E. Op Cit.

[41] Art 22 Reg. UE n. 679/2016 che dispone testualmente: "1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.*

significativamente sulla sua persona; tuttavia, ci sono delle eccezioni alla regola e laddove si applichi una di queste eccezioni, il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato[42].

La norma non vieta le decisioni automatizzate ma vieta di assumere decisioni basate unicamente su sistemi totalmente automatizzati[43] e tale ratio si evince della lettura degli emendamenti apportati dal Parlamento europeo in sede di prima lettura[44].

Questo primo approdo normativo segna il crescente interesse dell'Unione europea al desiderio di voler positivizzare delle regole giuridiche che possano garantire i diritti e le libertà delle persone fisiche a fronte al crescente utilizzo delle intelligenze artificiali e gran parte dell'elaborazione in corso di sviluppo in sede euro-unitaria riguarda il settore della responsabilità per danni derivanti dall'uso di smart product e, in particolare, sul profilo del livello di autonomia dell'A.I. e del possibile livello ''controllo umano" dei dispositivi che la incorporano.[45]

L'autonomia di apprendimento e decisionale è la caratteristica che segna la vera rivoluzione portata dall'I.A., la quale potrà animare prodotti che avranno una sempre maggiore capacità di interpretare l'ambiente che li circonda ed interagire con gli esseri umani e con altri

[42] Pellecchia E. Op Cit.

[43] Pellecchia E. Op Cit., inoltre, Sul Punto È Emerso, Inoltre, Un Dibattito Concernente L'impiego Dell'avverbio ''Unicamente'' Utilizzato Per Delimitare L'ambito Dei Trattamenti Vietati Dal Regolamento. La Dottrina È Infatti Divisa Tra Coloro Che Ravvisano Un Deficit Di Protezione Degli Interessati, Sostenendo Che L'utilizzo Di Tale Avverbio Comporterebbe La Sottrazione Al Divieto Di Tutte Quelle Decisioni In Cui Sia Ravvisabile Un Intervento Umano, Benché´ Minimo; E Coloro Che, Invece, Ritengono – Ai Fini Di Tale Esonero – Che L'intervento Umano Debba Essere Significativo. Pare Che Quest'ultima Sia La Posizione Condivisa Dal Comitato Europeo Per La Protezione Dei Dati Che, Nelle Sue Guidelines On Automated Individual Decision-Making And Profiling For Purposes Of Regulation 2016/679 (Da Ultimo Aggiornate Il 6 Febbraio2018), Esclude Che Il Titolare Del Trattamento Possa Eludere Il Divieto In Esame ''By Fabricating Human Involvement'' (21). Cfr., In Senso Fra Loro Opposto, Wachter-Mittelstadt-Floridi, Why A Right To Explanation Of Automated Decision-Making Does Not Exist In The General Data Protection Regulation, In International Data Privacy Law, Volume 7, Issue 2, May 2017, 76-99, Https://Doi.Org/10.1093/Idpl/Ipx005 E Malgieri-Comande` , Why A Right To Legibility Of Automated Decision- Making Exists In The General Data Protection Regulation, In International Data Privacy Law, Vol. 7, Issue 4, 243-265.

[44] Finocchiaro G., Intelligenza Artificiale E Protezione Dei Dati Personali, In Giurisprudenza Italiana, Luglio 2019, Pp. 1670-1677, Nota 38: "Il Parlamento Europeo Aveva Emendato, In Prima Lettura, Il Testo Del Regolamento Proposto Dalla Commissione Europea, Prevedendo All'art. 20 (Rubricato In Origine ''Misure Basate Sulla Profilazione''), Che La Profilazione Idonea A Produrre Effetti Giuridici Sull'interessato O A Incidere Sui Suoi Interessi, Diritti E Liberta` Non Potesse Essere Basata ''Unicamente O In Modo Predominante'' Sul Trattamento Automatizzato, Bensì` Che Dovesse Includere Obbligatoriamente ''Una Valutazione Umana, Compresa Una Spiegazione Della Decisione Conseguita Dopo Tale Valutazione'' (5º Comma). E ` Dunque Evidente Che, Nella Versione Non Definitiva Del Regolamento, Era Vietata Non Solo La Decisione Basata Unicamente Sul Trattamento Automatizzato (Come Oggi Previsto), Ma Anche Quella Decisione In Cui L'apporto Umano Risultasse Minore Rispetto All'impiego Di Sistemi Automatizzati. Inoltre Era Accordato Agli Interessati Il ''Diritto Di Ottenere Una Valutazione Umana E Una Spiegazione Della Decisione'', Diritto Che – Nel Testo Poi Approvato Del Regolamento E Oggi Vigente – E` Stato Limitato Al ''Diritto Di Ottenere L'intervento Umano'' (Art. 22, 4º Comma) E Al Diritto Di Accedere Ad ''Informazioni Significative Sulla Logica Utilizzata'' Nell'ambito Di Un Processo Decisionale Automatizzato (Art. 15, 1º Comma, Lett H)".

[45] Cosi Amidei A., Intelligenza Artificiale E Product Liability: Sviluppi Del Diritto Dell'unione Europea, In Giurisprudenza Italiana - Luglio 2019 Pp.1715-1726

oggetti, apprendendo nuovi comportamenti ed eseguendo azioni in modo indipendente, senza necessità dell'intervento umano.

L'elevata autonomia dell'I.A. e dei ''robot'' dalla stessa animati ha indotto molti Autori ad interrogarsi sulla possibilità di attribuire alla macchina una separata personalità giuridica, quale soluzione possibile al fine di evitare i cosiddetti ''vuoti di responsabilità '' relativi alle condotte degli agenti software [46].

L'inteso sviluppo tecnologico dell'A.I. ha indotto, inoltre, il Parlamento Europeo nella Risoluzione del 16 febbraio 2017, inerente al diritto civile della Robotica, a formulare delle ''raccomandazioni alla Commissione[47] allo scopo di prevenire il rischio di un *responsibility gap*, ossia di un ''vuoto di responsabilità '' per eventi lesivi cagionati dall'intelligenza artificiale self-learning in conseguenza di un suo processo evolutivo di apprendimento tanto autonomo da essere imprevedibile.[48]

Il Parlamento Europeo, nella risoluzione in esame ha adottato una definizione per descrivere la caratteristica dell''''autonomia del robot" e tale caratteristica si estrinsecherebbe nella capacità di prendere decisioni autonomamente e metterle in atto nel mondo esterno senza un controllo e con un livello di autonomia variabile a seconda del grado di complessità con cui è stata progettata l'interazione della macchina con l'ambiente. [49]

Secondo la prospettiva adottata dal Parlamento Europeo più`i robot sono autonomi e meno possono essere considerati come meri strumenti nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore, ecc.)'' e le caratteristiche enfatizzate sono l'ottenimento dell'autonomia grazie alla dotazione di sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività), lo scambio e l'analisi di tali dati, l'autoapprendimento dall'esperienza e attraverso l'interazione e l'adattamento del proprio comportamento e delle proprie azioni all'ambiente.

Infine, il Parlamento ha invitato la Commissione ad elaborare e a sottoporre al legislatore comunitario una proposta di direttiva per l'individuazione di norme civilistiche volte a regolare

---

[46] *Di tale avviso* A. AMIDEI, Robotica Intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo, in U. RUFFOLO (a cura di) Intelligenza artificiale e responsabilità, Giuffrè, Milano, 2017, 63 ss.; G. PASSAGNOLI, Ragionamento giuridico e tutele nell'intelligenza artificiale, in Persona e Mercato, 3/2019, 79 ss; G. COMANDÈ, Responsabilità e accountability nell'era dell'Intelligenza Artificiale, in F. DI CIOMMO, O. TROIANO (a cura di) Giurisprudenza e Autorità indipendenti nell'epoca del diritto liquido, Studi in onore di Roberto Pardolesi, Piacenza, La Tribuna, 2018, 1010; E. PALMERINI, Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea, in Resp. civ. e prev., 2016, 6, 1837 ss.

[47] Parlamento Europeo, Risoluzione del 16 febbraio 2017, Gazzetta Ufficiale Unione Europea, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT#:~:text=C%20252%2F241,Gioved%C3%AC%2016%20febbraio%202017,non%20contravvengano%20alla%20Prima%20Legge., (20 maggio 2022)

[48] Cosi Amidei A., op cit p.18

[49] Parlamento Europeo, Risoluzione del 16 febbraio 2017, cit., punto AA- AB.

in modo uniforme diversi aspetti connessi all'impiego di robotica avanzata, integrata dall'intelligenza artificiale.

La Risoluzione del 2017 rappresenta una tappa di notevole importanza nello sviluppo del dibattito sul tema dell'Intelligenza Artificiale, infatti, per la prima volta nell'Unione, un documento di natura politica dà atto delle implicazioni non soltanto etiche, ma anche giuridiche della diffusione dell' I.A., facendo espresso riferimento alla prospettiva che le condotte di macchine robotiche avanzate, programmate per imparare, evolversi e conseguentemente comportarsi in modo autonomo a prescindere dal controllo umano, possano non essere interamente prevedibili da chi le progetta, programma e/o produce, e ponendosi il conseguente problema di come allocare la responsabilità per danni derivanti da tali devianti condotte.

La strategia europea per l'I.A. è stata presentata nell'aprile 2018 e nel dicembre dello stesso anno è stato promulgato il piano coordinato sull'intelligenza artificiale con comunicazione della Commissione al Parlamento europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni[50] e, nell'ambito dello stesso progetto, è stato pubblicato il primo report ''*Algorithmic decision-making*''[51] che ha introdotto la definizione di *decision-making algorithm*.[52]

Il progetto prevede, inoltre, il coinvolgimento degli stakeholders[53] per sviluppare i concetti di equità, accountability, trasparenza e affidabilità dei sistemi decisionali automatizzati.

Nella comunicazione in esame la Commissione Europea ha dato una definizione di intelligenza artificiale[54]ed ha affidato a un gruppo di esperti indipendenti (AI4People.), il compito di sviluppare un progetto di orientamenti etici , al fine di creare una maggiore fiducia verso l'I.A. ed evitare possibili ripercussioni dovute al "cattivo" uso della nuova tecnologia[55],

---

[50] Comunicazione Della Commissione Al Parlamento Europeo, Al Consiglio Europeo, Al Consiglio, Al Comitato Economico E Sociale Europeo E Al Comitato Delle Regioni Piano Coordinato Sull'intelligenza Artificiale, Bruxelles, 7.12.2018 COM(2018) 795 Final, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0795 (20 maggio 2022)

[51] Ibidem: ''sistema software – compresi i suoi test, formazione e dati di input, nonché´ i relativi processi di governance – che, autonomamente o con coinvolgimento umano, prende decisioni o applica misure relative a sistemi sociali o fisici sulla base di dati personali o non personali, con impatti a livello individuale o collettivo''

[52] Cosi Gambino A.M., E Manzi M., Intelligenza Artificiale E Tutela Della Concorrenza, In Giurisprudenza Italiana - Luglio 2019 P. 1744

[53] Si Definiscono Stakeholders Tutti I Soggetti, Individui Od Organizzazioni, Attivamente Coinvolti Nell'iniziativa Promossa Dalla Commissione

[54] Comunicazione Della Commissione Al Parlamento Europeo, Al Consiglio Europeo, Al Consiglio, Al Comitato Economico E Sociale Europeo E Al Comitato Delle Regioni Piano Coordinato Sull'intelligenza Artificiale, *op. cit supra:* Per "*intelligenza artificiale" (IA) si intendono quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici. Usiamo l'IA quotidianamente, ad esempio per bloccare lo spam nella posta elettronica o per parlare con gli assistenti digitali*.

[55] ibidem"*Per una maggiore fiducia, necessaria affinché la società accetti e usi l'IA, la tecnologia dovrebbe essere prevedibile, responsabile, verificabile, dovrebbe rispettare i diritti fondamentali e seguire regole etiche. L'uso dell'IA potrebbe altrimenti provocare effetti indesiderati, quali la creazione di una camera dell'eco in cui le persone ricevono solo informazioni che*

affinché lo sviluppo e la diffusione di tali sistemi avvenga all'interno di un quadro sociotecnico in cui gli interessi individuali e il bene sociale siano non solo preservati, ma, ove possibile, potenziati.

Il Gruppo di lavoro AI4People, costituito su iniziativa dell'Unione Europea, ha sviluppato o un progetto finalizzato a tutelare l'autorealizzazione umana, cercando di prevenire gli eventuali danni che potrebbero sorgere nel caso in cui venga utilizzata un'I.A; l'obiettivo è stato quello di creare fiducia nell'utilizzo di un'Intelligenza Artificiale e per raggiungere lo scopo sono stati elaborarti dei principi guida che potessero ispirare i legislatori.

Il gruppo di esperti ritiene che debbano essere rispettati sette principi etici fondamentali:

- *Iniziativa e controllo da parte dell'uomo*
- *Robustezza tecnica e sicurezza, compresa la resilienza agli attacchi, un piano di sicurezza generale, precisione, affidabilità e riproducibilità*
- *Privacy e governance dei dati, compreso il rispetto della privacy, della qualità dell'integrità dei dati e dell'accesso ai dati*
- *Trasparenza, inclusa la tracciabilità, la spiegabilità e la comunicazione*
- *Diversità, non discriminazione ed equità, compresa la prevenzione dei pregiudizi, l'accessibilità, un modello di design universale e la partecipazione di tutte le parti interessate*
- *Benessere sociale e ambiente, compresi la sostenibilità e il rispetto dell'ambiente, l'impatto sociale e la democrazia*
- *Responsabilità, compresa la verificabilità, la minimizzazione e la comunicazione di impatti negativi, compromissioni e mezzi di risarcimento".*[56]

Sulla scorta di tali principi etici, nel febbraio del 2020, la Commissione ha presentato il Libro Bianco sull'intelligenza artificiale, un documento unico nel suo genere che pone l'Europa

corrispondono alle loro opinioni, o un rafforzamento delle discriminazioni, come nel caso dell'algoritmo divenuto razzista in 24 ore a causa dell'esposizione a materiale razzista. È fondamentale che gli umani comprendano in che modo l'IA prende le decisioni. L'Europa può diventare un leader globale nello sviluppo e nell'utilizzo stabile dell'IA e nella promozione di un approccio antropocentrico e di principi etici fin dalla progettazione. Per ancorare più saldamente tali principi allo sviluppo e all'uso dell'IA, la Commissione ha affidato a un gruppo di esperti dell'IA ad alto livello e indipendente il compito di sviluppare un progetto di orientamenti etici dell'IA. Una prima versione sarà pubblicata entro la fine del 2018 e gli esperti presenteranno alla Commissione la versione finale degli orientamenti nel marzo 2019, dopo un'ampia consultazione nell'ambito dell'Alleanza europea per l'IA41. L'ambizione è quindi di estendere a livello globale l'approccio etico dell'Europa. La Commissione sta aprendo la cooperazione a tutti i paesi terzi che desiderano condividere gli stessi valori. Ulteriori sviluppi nel campo dell'IA richiedono inoltre un quadro normativo sufficientemente flessibile da promuovere l'innovazione garantendo allo stesso tempo livelli elevati di protezione e sicurezza. La Commissione sta valutando se, alla luce di queste nuove sfide, i quadri normativi dell'UE e degli Stati membri in materia di sicurezza e responsabilità siano idonei allo scopo o se vi siano lacune da colmare. A tal fine la Commissione pubblicherà entro la metà del 2019 una relazione sulle potenziali lacune e orientamenti in materia di sicurezza e responsabilità per l'IA."

[56] AA.VV. Intelligenza Artificiale Il Diritto, I Diritti, L'etica, Giuffrè Francis Lefebvre S.P.A, Milano, 2020 A Cura Di Ugo Ruffolo pp 1-648

in una posizione di avanguardia nella regolamentazione del settore ed in cui vengono poste le basi per la tutela dei diritti dei consumatori e la promozione dell'innovazione nel campo dell'I.A.[57].

1.4 Il libro bianco sull'intelligenza artificiale dell'Unione Europea: un possibile equilibrio tra innovazione e protezione dei diritti e delle libertà individuali della persona

L'Unione Europea ha adottato il Libro Bianco sull'Intelligenza artificiale[58] nel 2020, il quale sottolinea l'importanza di basare l'I.A. europea su valori comuni e diritti fondamentali condivisi da tutti i Paesi membri, quali la dignità umana, tutela del consumatore e la tutela della privacy, al fine di una corretta armonizzazione tra gli Stati membri per evitare la frammentazione del mercato unico attraverso l'introduzione di singole e diversificate iniziative nazionali, suscettibili di compromettere la certezza del diritto e di indebolire la fiducia dei cittadini.

Al fine di delineare la potenzialità dello sviluppo normativo sull'intelligenza artificiale nel diritto positivo dell'Unione europea, occorrerà analizzare le disposizioni più importanti del Libro Bianco; l'analisi verrà svolta senza alcuna pretesa di esaustività ma al sol fine di verificare l'approccio normativo europeo sul settore in analisi.

Uno dei principali elementi costitutivi del testo in esame è quello di creare *un ecosistema di fiducia* che dovrebbe implementare l'utilizzo da parte cittadini, delle imprese e delle organizzazioni pubbliche, delle applicazioni di IA e aumentare la certezza del diritto, utilizzando un approccio di tipo antropocentrico basato e sulla comunicazione che tenga conto anche dei contributi ottenuti durante la fase pilota degli orientamenti etici elaborati dal gruppo di esperti ad alto livello sull'IA.

All'interno del Libro Bianco sull'intelligenza artificiale la Commissione Europea ha affermato che l'uso dell'IA può essere estremamente utile per rendere prodotti e processi più sicuri ma, al contempo, ha specificato che l'applicazione non regolamentata dell'AI potrebbe causare la violazione dei diritti fondamentali quali i diritti alle libertà di espressione, di riunione, la dignità umana, l'orientamento sessuale, la protezione dei dati personali, il diritto a un ricorso

[57] Commissione Europea, White Paper on Artificial Intelligence: a European approach to excellence and trust COM(2020) 65, 19.2.2020,https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en, (20 maggio 2022)

[58] Commissione Europea, op cit p.22 In particolare, l'Unione Europea intende conseguire un ``ecosistema di eccellenza'', attraverso l'istituzione di un partenariato pubblico-privato e la concessione di incentivi agli operatori del diritto che ricorreranno alle tecnologie basate sull'I.A. e raggiungere un ``ecosistema di fiducia unico, mediante la configurazione di un ambiente in cui tutti i consociati si sentano sicuri nell'utilizzo delle nuove tecnologie e gli operatori commerciali possano confidare legittimamente su una situazione legislativa rispondete ai principi di tassatività, determinatezza e prevedibilità

giurisdizionale effettivo e a un giudice imparziale, nonché una lesione alla tutela dei consumatori.[59]

Secondo la Commissione, il quadro normativo dovrebbe concentrarsi su come ridurre al minimo i diversi rischi di danno potenziale connessi all'uso dell'IA nel campo della tutela dei diritti fondamentali, nonché focalizzare lo studio sulle questioni legate alla sicurezza e alla responsabilità, e ciò perché le distorsioni e le discriminazioni rappresentano un rischio intrinseco di qualunque attività sociale od economica a cui nemmeno il processo decisionale umano è immune e se presenti nell'IA, potrebbero avere effetti maggiori e colpire o discriminare numerose persone in assenza dei meccanismi di controllo sociale che disciplinano il comportamento umano.

In particolare, la caratteristica dell'opacità, propria delle intelligenze artificiali, che si sostanzia nella difficile comprensione, anche da parte degli esperti che li hanno generati, del funzionamento e delle motivazioni in base alle quali modelli di apprendimento sempre più diffusi e complessi forniscono input, determina un forte impatto in termini di rendicontabilità, sicurezza e responsabilità soprattutto quando le I.A. sono utilizzate in ambiti rilevanti e critici della nostra società come la salute, l'assistenza, la guida autonoma, le tecnologie militari, l'economia, la finanza, la giustizia, le assicurazioni etc.*[60]*.

[59]Commissione Europea, Op Cit. P.22, In Cui Si Specifica Che *"l'uso dell'IA può pregiudicare i valori su cui si fonda l'unione e causare violazioni dei diritti fondamentali, compresi i diritti alle libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale (ove applicabili in determinati settori), la protezione dei dati personali e della vita privata o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori. tali rischi potrebbero derivare da difetti nella progettazione complessiva dei sistemi di ia (anche per quanto riguarda la sorveglianza umana) o dall'uso di dati senza che ne siano state corrette le eventuali distorsioni (ad esempio se un sistema è addestrato utilizzando solo o principalmente dati riguardanti gli uomini, il che comporta risultati non ottimali per quanto concerne le donne). l'I.A. può svolgere molte funzioni che in precedenza potevano essere esercitate solo dagli esseri umani. i cittadini e le persone giuridiche saranno pertanto sempre più soggette ad azioni realizzate e a decisioni prese da sistemi di ia o con la loro assistenza; si tratta di un risultato non sempre facile da comprendere e cui è difficile opporsi in modo efficace ove necessario. l'I.A. aumenta inoltre le possibilità di seguire e analizzare le abitudini quotidiane delle persone. vi è ad esempio il rischio potenziale che l'I.A. venga utilizzata, in violazione della normativa dell'ue sulla protezione dei dati e di altre norme, dalle autorità statali o da altri soggetti a fini di sorveglianza di massa, oppure dai datori di lavoro per osservare il comportamento dei loro dipendenti. poiché permette di analizzare grandi quantità di dati e di individuare collegamenti tra di essi, l'I.A. può essere usata anche per ricostruire e deanonimizzare dati riguardanti le persone, il che implica nuovi rischi per la protezione dei dati personali anche in relazione a set di dati che di per sé non contengono dati personali. l'I.A. è utilizzata anche dagli intermediari online per stabilire priorità riguardo alle informazioni da fornire ai loro utenti oppure a fini di moderazione dei contenuti. i dati trattati, le modalità con cui vengono progettate le applicazioni e il margine di intervento umano possono incidere sui diritti alla libertà di espressione, alla protezione dei dati personali e alla privacy nonché sulle libertà politiche*."

[60] Ibidem in cui la Commissione aggiunge: "le caratteristiche specifiche di molte tecnologie di I.A., tra cui l'opacità (effetto "scatola nera"), la complessità, l'imprevedibilità e *un comportamento parzialmente autonomo, possono rendere difficile verificare il rispetto delle normative dell'ue in vigore volte a proteggere i diritti fondamentali e possono ostacolarne l'applicazione effettiva. le autorità preposte all'applicazione della legge e le persone interessate potrebbero non disporre dei mezzi per verificare come sia stata presa una determinata decisione con il coinvolgimento di sistemi di I.A. e, di conseguenza, se sia stata rispettata la normativa pertinente. le persone fisiche e giuridiche possono incontrare difficoltà nell'accesso effettivo alla giustizia in situazioni in cui tali decisioni possono avere ripercussioni negative su di loro*."

La mancanza di disposizioni chiare in materia di sicurezza che affrontino tali rischi può creare, oltre a rischi per le persone interessate anche incertezza giuridica per le imprese che commercializzano nell'UE i prodotti che integrano sistemi di IA e, pertanto, la Commissione propone dei possibili adeguamenti del quadro legislativo vigente dell'UE per quanto concerne l'Intelligenza Artificiale.

Prima di passare a analizzare i possibili interventi individuati dalla Commissione Europea nel Libro Bianco, occorrerà effettuare una breve excursus storico-giuridico sulla normativa vigente in materia di responsabilità da prodotto difettoso e su quella riguardante la sicurezza dei prodotti.

La responsabilità da prodotto difettoso è stata introdotta con la Direttiva 85/374/CEE, la quale è stata recepita nel nostro ordinamento inizialmente con il D.P.R. n. 224/1988 e successivamente confluita nel D.lgs. 206/2005 (c.d. Codice del Consumo), con lo scopo di tutelare i consumatori finali dai danni derivanti da un possibile "difetto" degli stessi.

Il codice del consumo, all'art 117, dà la definizione di prodotto difettoso, il quale è identificato come quel bene che non offre la sicurezza che ci si può legittimamente attendere dallo stesso in considerazione del modo in cui il esso è stato messo in circolazione, la sua presentazione, le sue caratteristiche visibili, le istruzioni e le avvertenze fornite, l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere, tenendo in considerazione anche le conoscenze del tempo in cui il prodotto è stato messo in circolazione[61].

Il codice del consumo prevede all'art 119 la responsabilità del produttore, la quale si caratterizza per essere una responsabilità presunta poiché prescinde dall'elemento soggettivo della colpa: la responsabilità del produttore sorge quando il prodotto non conforme agli standard e difettoso viene messo in circolazione anche se solo in visione o in prova.

Nel caso in cui non sia possibile individuare il produttore, il D.lgs. 206/2005 prevede la responsabilità sul fornitore che ha distribuito commercialmente il prodotto e che ha omesso di comunicare identità e domicilio del produttore, o di altro eventuale fornitore, entro tre mesi

[61] Art 117 D.Lgs. 206/2005 : *Un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze, tra cui: a) il modo in cui il prodotto è stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni e le avvertenze fornite; b) l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere; c) il tempo in cui il prodotto è stato messo in circolazione. 2. Un prodotto non può essere considerato difettoso per il solo fatto che un prodotto più perfezionato sia stato in qualunque tempo messo in commercio. 3. Un prodotto è difettoso se non offre la sicurezza offerta normalmente dagli altri esemplari della medesima serie.*

dalla richiesta scritta del danneggiato;[62] si tratta di una responsabilità alternativa o sostituiva, il cui accertamento giudiziale può prevedere che il terzo indicato come produttore o precedente fornitore sia chiamato nel processo ai sensi dell'art. 106 cpc con possibile e conseguente estromissione del fornitore convenuto.

Per ottenere il risarcimento del danno dal produttore, il danneggiato dovrà provare il difetto, il danno e il nesso causale che ricollega il primo al secondo, inteso come suo effetto e conseguenza[63] e il produttore potrà liberarsi della responsabilità solo provando di non aver mai messo in circolazione il prodotto ovvero che il difetto non esisteva al momento dell'immissione sul mercato oppure che lo stesso sia insorto dalla necessità di conformare la merce stessa ad una norma imperativa o a un provvedimento vincolante.

Inoltre, il produttore potrà liberarsi dalla responsabilità anche provando che con le conoscenze scientifiche e tecniche conosciute al tempo della commercializzazione del prodotto non era stato possibile individuare gli elementi di difettosità ovvero che la relativa realizzazione non è avvenuta per la vendita o per qualsiasi altra distribuzione a titolo oneroso nell'ambito della propria attività professionale.

Nel caso in cui le contestazioni riguardino una parte componente ovvero la materia prima, il produttore potrà liberarsi dimostrando che il difetto è interamente dovuto alla concezione del prodotto in cui è stata incorporata la parte o la materia prima ovvero alla conformità di questa alle istruzioni date dal produttore che l'ha utilizzata.

La responsabilità da prodotto difettoso *(c.d. product liability)* si interseca con quella della product safety, ossia la politica dell'Unione Europea volta a garantire che gli articoli messi in vendita dalle imprese siano sicuri la cui normativa generale è contenuta nella Direttiva 2001/95/CE, la quale impone che i prodotti immessi sul mercato dell'UE debbano essere sicuri e corredati da tutte le informazioni che ne consentano la tracciabilità, quali l'identità del fabbricante, un certificato di prodotto e un foglio illustrativo che contenga tutte le avvertenze e informazioni relative a qualsiasi rischio intrinseco derivante dall'utilizzo della cosa.

Alla luce della direttiva in esame, un prodotto è considerato sicuro se rispetta specifiche disposizioni nazionali o norme comunitarie e, in mancanza di tali disposizioni o norme, la valutazione sulla sicurezza deve basarsi su criteri successivi quali gli orientamenti della Commissione, le buone prassi nel settore interessato, le prassi sullo stato di avanzamento delle

[62] Art 106 D.Lgs 206/2005: Quando il produttore non sia individuato, è sottoposto alla stessa responsabilità il fornitore che abbia distribuito il prodotto nell'esercizio di un'attività commerciale, se ha omesso di comunicare al danneggiato, entro il termine di tre mesi dalla richiesta, l'identità e il domicilio del produttore o della persona che gli ha fornito il prodotto

[63] Art. 120, Comma 1, D.Lgs 206/2005

conoscenze e delle tecnologie e in ultimo sulla sicurezza che i consumatori possono ragionevolmente aspettarsi.

La Direttiva 2001/95/CE impone, inoltre, alle autorità nazionali incaricate dell'applicazione della legge la facoltà di controllare la sicurezza dei prodotti e intraprendere le azioni adeguate contro gli articoli pericolosi.

Al fine di garantire una tutela a livello europeo è stato istituito anche un sistema per lo scambio rapido di informazioni, gestito dalla Commissione che consente alle autorità nazionali di allertare rapidamente gli altri Stati membri della presenza di un qualsiasi prodotto che presenti un rischio grave per la salute e la sicurezza.

In caso di utilizzo del sistema di allarme rapido, le autorità nazionali devono fornire tutte le informazioni utili che identificano l'articolo e la sua distribuzione in qualsiasi altra parte dell'Unione Europea e la Commissione ha il potere di intervenire rapidamente a livello europeo con misure di validità di un anno (rinnovabile), a fronte di un grave rischio provocato da un determinato prodotto.

Recentemente è stata data attuazione della decisione (UE) 2019/417, la quale ha stabilito delle linee guida per la gestione del sistema d'informazione rapida dell'Unione europea (RAPEX) inerente sia alla sicurezza dei prodotti e del suo sistema di notifica, sia disposizioni puntuali in materia alimentare, farmaceutica e dispositivi medici.

Questo breve inquadramento della product liability e della product safety è stato necessario poiché la Commissione europea nel Libro Bianco ripercorre le norme vigenti dell'UE e si interroga sulla possibilità di apportare delle modificazioni alla normativa vigente, al fine di prevenire ai rischi derivanti dai sistemi di I.A.[64]

Dalle considerazioni svolte dagli esperti nella relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di

[64]Commissione Europea, Op Cit. P.22: *" Esiste un vasto corpus di norme vigenti dell'UE in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi , comprendente norme settoriali ed integrato dalle legislazioni nazionali; tale corpus di norme è pertinente e potenzialmente applicabile a una serie di applicazioni di IA emergenti. Per quanto riguarda la protezione dei diritti fondamentali e dei diritti dei consumatori, il quadro legislativo dell'UE comprende atti normativi come la direttiva sull'uguaglianza razziale, la direttiva sulla parità di trattamento in materia di occupazione e di condizioni di lavoro, le direttive sulla parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e in materia di occupazione, una serie di norme sulla tutela dei consumatori, sulla protezione dei dati personali e sulla privacy, in particolare il regolamento generale sulla protezione dei dati, nonché altre normative settoriali riguardanti la protezione dei dati personali, come la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie . Inoltre, a partire dal 2025 si applicheranno le norme sui requisiti di accessibilità dei beni e dei servizi previste dall'atto europeo sull'accessibilità. I diritti fondamentali devono inoltre essere rispettati in sede di attuazione di altre normative dell'UE, anche nel settore dei servizi finanziari, della migrazione o della responsabilità degli intermediari online. Se da un lato la legislazione dell'UE rimane in linea di principio pienamente applicabile, indipendentemente dal coinvolgimento dell'IA, dall'altro è importante valutare se tale normativa possa essere adeguatamente applicata per far fronte ai rischi derivanti dai sistemi di IA o se sia necessario apportare adeguamenti a determinati strumenti giuridici"*

responsabilità[65] che accompagna il Libro Bianco, la Commissione ritiene che il quadro legislativo europeo possa essere migliorato nei seguenti termini:

- ***Effettiva applicazione e rispetto della normativa nazionale e dell'UE in vigore,*** tale punto dovrà essere adattato perché le caratteristiche principali dell'I.A. rendono difficile garantire la corretta applicazione e il rispetto della normativa nazionale e dell'UE e a causa della loro opacità è difficile individuare e dimostrare eventuali violazioni delle disposizioni normative al fine attribuire la responsabilità e soddisfare le condizioni per chiedere un risarcimento e, pertanto, la Commissione ha invitato gli Stati a adeguare o chiarire la legislazione positiva al fine di tutelare i diritti e le libertà europee.
- ***Limiti dell'ambito di applicazione della legislazione dell'UE vigente****:* un aspetto particolarmente rilevante è la possibile applicazione alle I.A. della legislazione dell'UE in materia di sicurezza dei prodotti. Tuttavia, la Commissione evidenzia che la normativa vigente potrebbe tutelare il consumatore finale solo quando il software, è parte del prodotto finale, poiché in tale caso il produttore deve rispettare le norme

[65] Commissione Europea, Op Cit. P.22: "La relazione che accompagna il presente libro bianco analizza il quadro giuridico pertinente, individuando le incertezze riguardanti l'applicazione di tale quadro giuridico in relazione ai rischi specifici derivanti dai sistemi di IA e da altre tecnologie digitali. La conclusione è che la legislazione vigente in materia di sicurezza dei prodotti sostiene già un concetto ampio di sicurezza, con l'obiettivo di proteggere da tutti i tipi di rischi derivanti dal prodotto in funzione dell'uso dello stesso. Per garantire una maggiore certezza del diritto si potrebbero tuttavia introdurre disposizioni che contemplino esplicitamente i nuovi rischi derivanti dalle tecnologie digitali emergenti. • Il comportamento autonomo che mostrano alcuni sistemi di IA durante il loro ciclo di vita può comportare modifiche significative dei prodotti, che a loro volta hanno ripercussioni sulla sicurezza e possono rendere necessaria una nuova valutazione dei rischi. Potrebbe inoltre rendersi necessaria, come misura di salvaguardia, la sorveglianza umana dalla fase di progettazione e durante tutto il ciclo di vita dei prodotti e dei sistemi di IA. • Ove opportuno potrebbero essere presi in considerazione obblighi espliciti per i produttori anche in relazione ai rischi per la sicurezza mentale degli utenti (ad esempio dovuti alla collaborazione con robot umanoidi). • La legislazione dell'Unione in materia di sicurezza dei prodotti potrebbe prevedere prescrizioni specifiche che affrontino i rischi per la sicurezza derivanti dall'uso di dati errati in fase di progettazione, nonché meccanismi per garantire che sia mantenuta la qualità dei dati durante l'intero periodo di utilizzo dei prodotti e dei sistemi di IA. • Il problema dell'opacità dei sistemi basati su algoritmi potrebbe essere affrontato mediante prescrizioni in materia di trasparenza. • Potrebbe essere necessario adeguare e chiarire le norme vigenti in relazione ai casi di software indipendente immesso sul mercato senza altri componenti, oppure integrato in un prodotto dopo che quest'ultimo è stato immesso sul mercato, qualora ciò abbia un impatto sulla sicurezza. • Data la crescente complessità delle catene di approvvigionamento in relazione alle nuove tecnologie, disposizioni che richiedano specificamente una collaborazione tra gli utenti e gli operatori economici attivi lungo la catena di approvvigionamento potrebbero garantire la certezza del diritto. Le caratteristiche delle tecnologie digitali emergenti, come l'IA, l'Internet delle cose e la robotica, possono mettere in discussione alcuni aspetti dei quadri giuridici relativi alla responsabilità e renderli meno efficaci. Alcune di queste caratteristiche potrebbero rendere difficile far risalire il danno alla condotta di una persona, condizione indispensabile per invocare la responsabilità per colpa conformemente alla maggior parte delle norme nazionali in materia. Ne deriva la possibilità che i costi per le vittime aumentino in maniera significativa, e la potenziale difficoltà di avviare azioni per responsabilità nei confronti di soggetti diversi dal produttore e di ottenere elementi di prova a sostegno di tali azioni. • Le persone che hanno subito un danno provocato con il coinvolgimento di sistemi di IA devono godere dello stesso livello di protezione delle persone che hanno subito danni causati da altre tecnologie; nel contempo occorre che l'innovazione tecnologica possa continuare a svilupparsi. • È opportuno valutare attentamente tutte le opzioni che consentano di raggiungere tale obiettivo, compresa la possibilità di modificare la direttiva sulla responsabilità per danno da prodotti difettosi e ulteriori possibili interventi mirati di armonizzazione delle norme nazionali in materia di responsabilità. Ad esempio, la Commissione sta valutando se e in quale misura sia necessario mitigare le conseguenze della complessità adeguando l'onere della prova richiesto dalle norme nazionali in materia di responsabilità in relazione ai danni provocati dal funzionamento delle applicazioni di IA"

pertinenti in materia di sicurezza dei prodotti; tuttavia nel caso in cui il software sia indipendente (*standalone*), occorrerà stabilire se esso rientri nell'ambito di applicazione della normativa dell'UE in materia di sicurezza dei prodotti, ovvero creare una normativa ad hoc. Attualmente, la normativa generale dell'UE in materia di sicurezza si applica ai prodotti ma non ai servizi, per cui in linea di principio non si applicherebbe nemmeno ai servizi basati sulla tecnologia di I.A. come ad esempio servizi sanitari, finanziari e di trasporto. Su tale punto, la Commissione ha invitato gli esperti a formulare delle ipotesi normative tali da poter garantire il rispetto dei principi e delle libertà riconosciute dall'Unione Europea.

- ***Funzionalità mutevole dei sistemi di IA****:* la Commissione ha analizzato il particolare aspetto dell'integrazione del software nei prodotti, tra cui ricomprende anche l'I.A., la quale tramite i sistemi di autoapprendimento può modificare il funzionamento di tali prodotti e sistemi durante il loro ciclo di vita e può innestare nuovi rischi che non erano presenti nel sistema quando esso è stato immesso sul mercato. La Commissione ha rilevato che tali rischi non sono adeguatamente disciplinati dalla legislazione esistente, la quale si concentra prevalentemente sui rischi per la sicurezza presenti al momento dell'immissione sul mercato e, pertanto, ha invitato il legislatore europeo a cercare soluzioni in grado di tener conto della funzionalità mutevole dei sistemi di I.A.
- ***Incertezza in merito all'attribuzione delle responsabilità tra i diversi operatori economici lungo la catena di approvvigionamento:*** in tale ambito la Commissione osserva che la legislazione dell'UE in materia di sicurezza dei prodotti attribuisce al fabbricante la responsabilità del prodotto immesso sul mercato e di tutti i suoi componenti ma tali norme potrebbero divenire poco chiare nel caso in cui l'IA integra il prodotto dopo che quest'ultimo è stato immesso sul mercato da un soggetto diverso dal produttore. In tale caso, la legislazione attuale dell'UE prevede la responsabilità dei produttori ma lascia alle disposizioni nazionali in materia il compito di disciplinare la responsabilità di altri soggetti nella catena di approvvigionamento e ciò potrebbe comportare una diversificazione di tutela all'interno dei vari Stati Membri. La Commissione individuato tale problema ha invitato il legislatore europeo a armonizzare la disciplina.
- ***Evoluzione del concetto di sicurezza:*** in tale sezione la Commissione osserva come l'uso dell'IA nei prodotti e nei servizi può dar luogo a rischi che la legislazione dell'UE attualmente non affronta in modo esplicito come, ad esempio, quelli collegati alle minacce informatiche che possono riguardare la sicurezza personale ovvero rischi che possono derivare dalla perdita di connettività, ecc.

> I rischi individuati dalla Commissione possono essere presenti sia al momento dell'immissione dei prodotti sul mercato ovvero potrebbero presentarsi successivamente in caso di aggiornamenti del software o dall'apprendimento automatico durante l'uso del prodotto. Anche in tale caso, la Commissione Europea ritiene che la legislazione europea debba dotarsi di strumenti volti a rafforzare la base di conoscenze scientifiche di cui dispone sui potenziali rischi connessi alle applicazioni di IA, sfruttando anche l'esperienza dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA) al fine di valutare il panorama delle minacce dell'IA *"*[66]

La Commissione Europea, inoltre, detta una serie di prescrizioni da seguire sul futuro quadro normativo in materia di IA e, in particolare, per le applicazioni di IA ad alto rischio delineando gli elementi essenziali sulla base degli orientamenti forniti da un gruppo di esperti.

Le prescrizioni fornite dalla commissione sono state ripartite in base ai principi prima analizzati delineati dal Gruppo di lavoro AI4People[67]: i dati di addestramento, la tenuta dei dati e dei registri, le informazioni da fornire, la robustezza e la precisione, la sorveglianza umana e prescrizioni specifiche per determinate applicazioni particolari dell'IA, come quelle utilizzate a fini di identificazione biometrica remota.

In relazione ai dati di addestramento, la Commissione, al fine di rispettare tale principio, ritiene che l'Ue e gli Stati membri dovrebbero adottare delle prescrizioni volte a fornire ragionevoli garanzie circa la sicurezza dell'uso successivo dei prodotti e dei servizi basati sull'IA[68] , e ciò soprattutto per garantire la fiducia dell'utilizzatore; prescrizioni che impongano di adottare misure ragionevoli per garantire che l'uso successivo dei sistemi di IA non porti a risultati che implichino discriminazioni vietate. [69], e ciò soprattutto per evitare che situazioni eguali vengano trattate dall'I.A. in modo difforme e, prescrizioni volte a garantire un'adeguata protezione della privacy e dei dati personali durante l'uso dei prodotti e dei servizi basati sull'IA[70] , poiché il trattamento senza controllo dei dati personali potrebbe arrecare seri pregiudizi alla persona.

---

[66] Commissione Europea op.cit p. 21

[67] AA.VV. Intelligenza Artificiale Il Diritto, I Diritti, L'etica, Giuffrè Francis Lefebvre S.P.A, Milano, 2020 A Cura Di Ugo Ruffolo pp 1-648

[68] Commissione Europea, op cit p.22, p.20: "tale sicurezza è intesa come conformità agli standard stabiliti dalle norme dell'UE applicabili in materia di sicurezza (sia quelle vigenti, sia eventuali norme complementari). Si tratta ad esempio di prescrizioni volte a garantire che i sistemi di IA siano addestrati utilizzando set di dati sufficientemente ampi e che contemplino tutti gli scenari pertinenti, in modo da evitare situazioni pericolose"

[69] ibidem p. 21: "Tali prescrizioni potrebbero comportare, in particolare, l'obbligo di utilizzare set di dati sufficientemente rappresentativi, in particolare per garantire che rispecchino adeguatamente tutte le pertinenti dimensioni di genere, etnia e altri possibili motivi di discriminazione vietata

[70] Ibidem: Tali questioni sono disciplinate dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie per la parte che rientra nel loro rispettivo ambito di applicazione."

In relazione alla tenuta dei registri relativi alla programmazione dell'algoritmo, ai dati utilizzati per addestrare sistemi di IA ad alto rischio e, in alcuni casi, per la tenuta dei dati stessi la Commissione ha richiesto alle Istituzioni dell'Ue e agli Stati membri di prevedere, in primo luogo, dei sistemi che consentono essenzialmente di risalire alle azioni o decisioni potenzialmente problematiche dei sistemi di IA e di verificarle – e ciò al fine di diminuire la caratteristica dell'opacità, insita in tutte i sistemi di I.A.; in secondo luogo, la Commissione ha richiesto di introdurre l'obbligo normativo di tenere registri accurati dei set di dati utilizzati per addestrare e sottoporre a prova i sistemi di IA, compresa una descrizione delle principali caratteristiche e delle modalità di selezione di tali insiemi e, in taluni casi giustificati, prevedere la tenuta degli stessi set di dati, della documentazione relativa alle metodologie, alle procedure e alle tecniche di programmazione e di addestramento utilizzate per costruire, sottoporre a prova e convalidare i sistemi di IA, ove opportuno anche in materia di sicurezza, evitando distorsioni che potrebbero dar luogo a discriminazioni vietate.

Inoltre, la Commissione ha richiesto di introdurre normativamente l'obbligo di conservazione dei registri, della documentazione e, se del caso, i set di dati per un periodo di tempo limitato e ragionevole al fine di garantire l'effettiva applicazione della legislazione pertinente e adottare delle misure normative per garantire che tali elementi siano messi a disposizione su richiesta, in particolare per essere sottoposti a prove o ispezioni da parte delle autorità competenti.

Nel caso di dati sensibili quali i segreti commerciali, infine, nel suo report la Commissione ritiene sarebbe opportuno prevedere nuove modalità per garantire la tutela delle informazioni riservate poiché i segreti commerciali al pari dei dati sensibilissimi possono essere divulgati esclusivamente con il consenso dell'avente diritto.

In relazione Obblighi di informazione, la Commissione ha ribadito la centralità della trasparenza al fine di promuovere un uso responsabile dell'IA e rafforzare la fiducia degli utenti agevolando la riparazione del danno ove necessario, e, per fare ciò ha richiesto che la legislazione europea imponga delle norme che obblighino a fornite in maniera proattiva informazioni adeguate sull'uso dei sistemi di IA ad alto rischio.

Accanto a tale obbligo d'informazione primario, le nuove norme europee e nazionali dovrebbero introdurre dei nuovi obblighi volti a fornite informazioni chiare sulle capacità e sulle limitazioni dei sistemi di IA e, in particolare, per quanto riguarda l'obiettivo per il quale i sistemi sono stati concepiti, le condizioni alle quali ci si può attendere che funzionino come previsto e il livello di precisione previsto nel raggiungimento dell'obiettivo specificato, poiché

tali informazioni solo rilevanti non solo per coloro che applicano i sistemi, ma anche per le autorità competenti e le parti interessate che dovranno controllare l'uso della nuova tecnologia.

Per raggiungere tale obbiettivo, la Commissione ha ritenuto di dover ampliare le norme già esistenti, le quali dovranno ricomprendere anche l'obbligo di informare correttamente e chiaramente i cittadini quando questi interagiscono con un sistema di IA e non con un essere umano pretendendo che le informazioni fornite siano obiettive, concise e di facile comprensione e adeguate al contesto specifico.

In relazione al principio della Robustezza e precisione, la Commissione ha stabilito che al fine di rendere affidabili i sistemi di IA (ed in particolare le applicazioni di IA ad alto rischio) dovrebbero essere tecnicamente robusti e precisi e sviluppati in modo responsabile e con la debita e adeguata valutazione ex ante dei rischi che possono generare.

In tale contesto, secondo la Commissione, dovrebbero essere adottate delle prescrizioni normative che garantiscano la robustezza e la precisione dei sistemi di IA, o che almeno riflettano correttamente il loro livello di precisione, durante tutte le fasi del ciclo di vita della stessa, delle prescrizioni atte a garantire la riproducibilità dei risultati, al fine di verificare come l'I.A. abbia elaborato quel determinato risultato, delle prescrizioni atte a garantire che i sistemi di IA possano gestire adeguatamente gli errori o le incongruenze in tutte le fasi del ciclo di vita, al fine di correggerle e prescrizioni volte a assicurare la resilienza dei sistemi di IA sia dagli attacchi palesi sia dai tentativi meno evidenti di manipolare i dati o gli stessi algoritmi, e che siano in grado di garantire che in tali casi siano adottate misure di attenuazione, al fine di evitare delle discriminazioni.

In relazione alla sorveglianza umana, punto imprescindibile per la corretta utilizzazione dell'I.A., la Commissione ha affermato che la presenza del controllo umano deve aiutare a garantire che un sistema di IA non provochi degli effetti negativi e, pertanto, essa dovrebbe essere implementata.

Per raggiungere tala obbiettivo, la Commissione ha fornito delle indicazioni[71], ritenendo che le novelle normative debbano prevedere un controllo stringente sull'attività dell'I.A in modo tale che il risultato del sistema di IA non divenga effettivo prima che sia stato rivisto e convalidato da un essere umano (si pensi ad esempio alla decisione di respingere una richiesta di prestazioni di sicurezza sociale può essere presa unicamente da un essere umano), ovvero,

[71]Commissione Europea, op cit p.22:" l'obiettivo di un'I.A. affidabile, etica e antropocentrica può essere raggiunto solo garantendo un adeguato coinvolgimento degli esseri umani in relazione alle applicazioni di I.A. ad alto rischio. sebbene tutte le applicazioni di I.A. prese in considerazione nel presente libro bianco per un regime giuridico specifico siano ritenute ad alto rischio, il tipo e il livello adeguati di sorveglianza umana possono variare da un caso all'altro. dipende in particolare dall'uso previsto dei sistemi e dagli effetti che potrebbero derivarne per le persone giuridiche e i cittadini interessati, senza pregiudizio per i diritti stabiliti dal GDPR in relazione al trattamento di dati personali da parte di sistemi di I.A.

nel caso in cui il risultato del sistema di IA divenga immediatamente effettivo, la legislazione dovrà prevedere un controllo ex post umano (si pensi ad esempio alla decisione di respingere la richiesta di una carta di credito che può essere adottata da un sistema di IA, ma che successivamente venga riesaminata da parte di un essere umano).

Il controllo umano sull'attività dell' I.A potrebbe anche avvenire in tempo reale, infatti tra le opzioni fornite della Commissione vi è la possibilità di prevedere un sistema di monitoraggio dell'IA durante il suo funzionamento in modo tale che il controllore umano possa intervenire immediatamente e disattivarla (si pensi ad esempio alla previsione di un sistema di guida autonoma dotata di un pulsante o una procedura di arresto che un essere umano può attivare qualora che il funzionamento dell'auto non sia sicuro*)"*

In relazione alla Prescrizioni specifiche per l'identificazione biometrica remota[*72*], la Commissione ha stabilito che il trattamento dei dati biometrici di una persona è vietato ed è vietato anche l'utilizzo di sistemi di IA per l'identificazione biometrica remota, i quali hanno implicazioni sui diritti fondamentali quali la dignità di una persona e la sua privacy; tuttavia, tale divieto non è assoluto e al ricorrere di determinate condizioni potrebbe essere autorizzato il trattamento di questi dati[*73*].

La Commissione, basandosi sulla normativa vigente in materia di protezione dei dati personali e dei diritti riconosciuti dalla Carta dei diritti Fondamentali dell'Unione Europea, ha affermato che l'IA può essere utilizzata a fini di identificazione biometrica remota unicamente ove tale uso sia debitamente giustificato, proporzionato e soggetto a garanzie adeguate[74].

---

[72] Articolo 3, paragrafo 13, della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie; articolo 4, paragrafo 14, del GDPR; articolo 3, paragrafo 18, del regolamento (UE) 2018/1725]: per dati biometrici si intendono "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione o l'autenticazione univoca, quali l'immagine facciale o i dati dattiloscopici [impronte digitali]."

[73] commissione europea, op cit p.22: La raccolta e l'uso di dati biometrici a fini di identificazione remota, ad esempio mediante la diffusione di sistemi di riconoscimento facciale in luoghi pubblici, comporta rischi specifici per i diritti fondamentali. L'uso di sistemi di IA per l'identificazione biometrica remota ha implicazioni sui diritti fondamentali che variano notevolmente a seconda dello scopo, del contesto e della portata del loro uso. Le norme dell'UE in materia di protezione dei dati vietano in linea di principio il trattamento di dati biometrici allo scopo di identificare in modo univoco una persona fisica, salvo a determinate condizioni. I diritti violati sono ad esempio, la dignità delle persone. analogamente, i diritti al rispetto della vita privata e alla protezione dei dati personali che sono al centro delle preoccupazioni riguardanti i diritti fondamentali connesse all'uso della tecnologia di riconoscimento facciale. vi è anche un impatto potenziale per quanto concerne la non discriminazione e i diritti dei gruppi speciali, come i bambini, gli anziani e le persone con disabilità. l'uso della tecnologia non deve inoltre compromettere i diritti alla libertà di espressione, di associazione e di riunione. cfr. facial recognition technology: fundamental rights considerations in the context of law enforcement (tecnologia di riconoscimento facciale: considerazioni sui diritti fondamentali nell'ambito delle attività di polizia e giudiziarie), https://fra.europa.eu/en/publication/2019/facial-recognition .

[74] in particolare, ai sensi del GDPR, tale trattamento può essere effettuato solo per un numero limitato di motivi, principalmente per motivi di interesse pubblico rilevante. in tal caso, il trattamento deve essere effettuato sulla base del diritto dell'unione o degli stati membri, rispettare il requisito di proporzionalità e l'essenza del diritto alla protezione dei dati e prevedere appropriate misure di tutela. a norma della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, un simile trattamento deve essere strettamente necessario, autorizzato in linea di principio dal diritto dell'UE o degli stati membri e soggetto a garanzie adeguate.

Per affrontare eventuali preoccupazioni sociali relative all'uso dell'IA per tali fini in luoghi pubblici, e per evitare la frammentazione del mercato interno, la Commissione ha reso noto che avvierà al più presto un ampio dibattito europeo sulle circostanze specifiche che possano eventualmente giustificare tali usi, nonché sulle garanzie comuni".

Il quadro sino ad ora delineato mostra un'apertura sempre maggiore del diritto europeo all'innovazione e soprattutto alla volontà di voler regolare il fenomeno dell'Intelligenza artificiale al fine di armonizzare la tutela all'interno degli Stati membri.

Tuttavia, come avremo modo di vedere, la legislazione vigente non risulta adeguata alla tutela delle libertà fondamentali e tale inadeguatezza si è mostrata con tutta la sua intensità nella lotta alla pandemia Covid-19, ove le app di I.A impiegate per il monitoraggio e la prevenzione alla diffusione del virus sono state immesse sul mercato senza l'adeguamento della legislazione positiva, sia nazionale che europea ma solo con alcune prescrizioni generali fornite dalla Commissione.

1.5 L'approccio italiano nella regolazione dell'intelligenza artificiale alla luce delle linee guida del libro bianco dell'UE

Al fine di allinearsi con le politiche europee in materia di Intelligenza Artificiale, è stata pubblicata dal Ministero dello Sviluppo Economico una proposta di strategia italiana elaborata dal Gruppo di Esperti MISE sull'intelligenza artificiale.

Il programma in esame deve ispirarsi a cinque "principi guida"[75] tra cui quello di creare un sistema di Intelligenza artificiale antropocentrico:

---

qualunque trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica sarebbe soggetto alla carta dei diritti fondamentali dell'unione europea, in quanto rappresenterebbe un'eccezione a un divieto stabilito dal diritto dell'UE.

[75] Ministero Dello Sviluppo Economico, Proposte Per Una Strategia Italiana Per L'intelligenza Artificiale, Https://Www.Mise.Gov.It/Images/Stories/Documenti/Proposte_Per_Una_Strategia_Italiana_Ai.Pdf, (22 Maggio 2022), In Cui Si Specifica Che: 1*)Innanzitutto, L'ia Italiana È Un'ia Europea. Come Noto, Nell'ambito Della Strategia Europea Per L'ia, La Commissione Europea Ha Pubblicato, Lo Scorso 21 Aprile, La Proposta Di Regolamento Dell'intelligenza Artificiale, Che Tratteggia Il Primo Quadro Giuridico Europeo Sul Tema E Che, Inter Alia, Definisce L'approccio Di Base Che Deve Caratterizzare L'azione Degli Stati Membri, Condiviso Anche Dal Nostro Programma: I Governi Nazionali Devono Agire In Maniera Coordinata, Armonizzando Le Loro Politiche Di Implementazione Dell'ia, Affinché L'europa Tutta Diventi Maggiormente Competitiva.*

2)L'Italia Sarà Un Polo Globale Di Ricerca Ed Innovazione Dell'ia: Per Un Ecosistema IA All'avanguardia, È Essenziale Che L'italia Investi Nella Ricerca E Nello Sviluppo. A Tal Fine, Il Programma Individua Le Fonti Di Investimento, Europee E Nazionali, Per Sostenere I Progetti.

3) L'IA Italiana Sarà Antropocentrica, Affidabile E Sostenibile: Lo Sviluppo IA Deve Essere Incentrato Sull'inclusione Economica E Sociale, Sui Diritti Umani E Sulla Sostenibilità Ambientale. L'Italia Aderisce Alle "Linee Guida Etiche Per Un Programma Di Orientamento E Attuazione Affidabile Dell'ia" Definite Dall' High Level Expert Group On AI.

4) Le Aziende Italiane Diventeranno Leader Nella Ricerca, Nello Sviluppo E Nell'innovazione Dell'ia: Le Imprese Private – Insieme Alle Comunità Di Ricerca, Ai Centri Di Trasferimento Tecnologico E Alla Pubblica Amministrazione – Figurano Tra I Principali Protagonisti Della Trasformazione Digitale; Pertanto, Devono Adottare Soluzioni Di Intelligenza Artificiale Ed Essere Messe In Condizioni Di Farlo.

5) Le Pubbliche Amministrazioni Italiane Governeranno L'ia E Governeranno Con L'ia: "Govern AI And Govern With AI", Questa La Formula Che Sintetizza Il Principio Che Deve Ispirare L'azione Della P.A. Da Un Lato, Governare L'ia Per Attenuarne I Potenziali

"L'intelligenza artificiale italiana sarà antropocentrica, affidabile e sostenibile. Le tecnologie non devono solamente promuovere la crescita economica ma assicurare che essa sia inclusiva e sostenibile, in linea con i principi contenuti nell'articolo 3 della Costituzione italiana e negli obiettivi di sviluppo sostenibile delle Nazioni Unite. Ciò significa che lo sviluppo dell'IA deve essere incentrato sull'inclusione economica e sociale, sui diritti umani e sulla sostenibilità ambientale. L'IA deve essere progettata e implementata in modo responsabile e trasparente, affinché possa rispondere alle sfide della società garantendo sicurezza in tutti i settori. A tal fine, l'Italia aderisce alle "Linee guida etiche per un programma di orientamento e attuazione affidabile dell'IA" definito dall'High Level Expert Group on A".

Dopo aver elencato i principi guida, la proposta strategica italiana elenca i sei obiettivi che il Programma si propone di perseguire, al fine di creare un sistema IA che sfrutti al massimo i punti di forza che l'Italia possiede.

I punti cardine del programma governativo ruotano essenzialmente intorno a sei obiettivi primari, i quali si identificano nella volontà di rafforzare la ricerca nel campo dell'IA, prediligendo un approccio multidisciplinare volto soprattutto a costruire un sistema unitario di ricerca capace di ridurre la frammentazione della stessa e aiutandola a raggiungere obbiettivi sempre più ambiziosi e, inoltre, sviluppare e adottare un'IA antropocentrica ed affidabile andando soprattutto delle normative e del limiti che siano in linea con i profili etici individuati in sede unitaria.

Altro punto cardine è quello aumentare l'innovazione basata sull'IA e lo sviluppo della tecnologia di IA, trasferendo i risultati della ricerca sul mercato, promuovendo investimenti industriali e facilitando l'adozione di applicazioni IA anche nelle PMI cercando, inoltre, di sviluppare politiche e servizi basati sull'IA nel settore pubblico, per una P.A. più efficiente e, anch'essa, competitiva.

Infine, il programma cerca di creare, trattenere ed attrarre ricercatori di IA in Italia, in tutti i livelli di istruzione, prestando una maggiore attenzione alla valorizzazione della diversità ed evitando divari di genere[76] e ciò al fine di consentire uno sviluppo tecnologico omogeneo e competitivo in questo nuovo campo di ricerca.

Il programma elaborato dallo Stato italiano risulta essere coerente ed allineato con la strategia contenuta nel Libro Bianco dell'Unione Europa in materia di intelligenza artificiale ma i recenti fatti di cronaca dovuti all'emergenza sanitaria COVID-19 hanno di fatto accelerato

Rischi, Seguendo Le Linee Guida Etiche Di Cui Al Punto 1.3.; Dall'altro, Utilizzare Le Applicazioni IA Per Migliorare I Propri Processi Interni, Attraverso Un Uso Responsabile Dei Dati E Delle Nuove Tecnologie.

[76] Ministero Dello Sviluppo Economico, Op Cit P. 35

l’utilizzo dell’Intelligenza artificiale in campi sensibilissimi e poco regolamentati quali quello medico e sanitario.

Nel settore medico e sanitario, infatti, l’utilizzo dell’Intelligenza artificiale può rilevare in due ambiti precisi: il settore diagnostico e chirurgico e quello inerente trattamento dei dati sanitari.

Nel settore diagnostico e chirurgico l’utilizzo dell’intelligenza artificiale pone il particolare problema di individuare gli elementi essenziali della responsabilità civile in caso di cooperazione tra intelligenza umana e artificiale e, il problema oggi più attuale è quello di verificare se le attuali norme sulla responsabilità civile siano applicabili alla c.d. chirurgia robotica.

Il settore inerente al trattamento dei dati personali è il più articolato e complesso poiché non solo è strettamente collegato al concetto sfuggevole e poco definito di privacy ma anche perché la regolamentazione è caratterizzata dalla compresenza di norme nazionali, europee e internazionali e, pertanto, l’indagine si dovrà ora concentrare nell’analisi dell’evoluzione del diritto alla privacy con la conseguente tutela fornita dalla Convenzioni internazionali e dal GDPR europeo in caso di trattamento illecito dei dati sanitari.

Tale analisi è fondamentale al fine di poter verificare nel capitolo finale se l’utilizzo dell’Intelligenza Artificiale durante la prima fase della pandemia Covid-19 ha rispettato i diritti fondamentali ovvero se il trattamento illegittimo dei dati sanitari ha configurato una possibile ipotesi di responsabilità civile in capo al Ministero della Salute, designato quale Titolare del trattamento per i Big Data raccolti dall’ App *“Immuni”*.

Capitolo 2

Dalla privacy alla protezione dei dati personali sensibili e sensibilissimi

2.1 Privacy: storia ed evoluzione del diritto alla riservatezza

La nozione di privacy, e il correlativo diritto alla riservatezza, ha radici antiche ed ha assunto un significato diverso a seconda dell'epoca storica che si prende in considerazione.

Come analizzato dallo studioso Sergio Niger nella sua opera *"Le nuove dimensioni della privacy*: *dal diritto alla riservatezza alla protezione dei dati personali"*[77]*: Gli antichi greci ritenevano fondamentale, quasi un dovere, per i propri cittadini maschi, la partecipazione alla vita pubblica ; essi riconoscevano anche la necessità per ognuno di avere una sfera privata, ma si trattava dell'ambito strettamente limitato all'espletamento dei propri bisogni e delle proprie necessità, vicino alla fondamentale bios politikos*[78].

La polis tutelava come sacri i confini della proprietà ma a fondamento di ciò non vi era il rispetto della proprietà privata bensì il fatto che senza una casa un uomo non poteva partecipare agli affari della città[79],e pertanto, la privacy *finiva* per essere considerata come un concetto fine a sé stesso, ossia come la vita che si svolgeva nel contesto sociale, e tutti coloro che non erano impegnati nella vita della polis venivano visti come soggetti asociali che si sottraevano ai loro obblighi e doveri morali[80].

Nel contesto ellenico, infatti, la tutela della sfera personale dell'individuo era avvertita come un diritto funzionale alla partecipazione della vita e non come diritto assoluto, intangibile, inderogabile e solo nell'età medievale, il termine privato divenne sinonimo di familiare.

In quell'epoca, infatti, la vita privata era basata sulla fiducia reciproca che univa i membri del gruppo, dando luogo, quindi, ad una vita familiare intesa in senso conviviale, ove non vi era spazio per l'individualità.

---

[77] Niger S., Le Nuove Dimensioni Della Privacy: Dal Diritto Alla Riservatezza Alla Protezione Dei Dati Personali, Cedam, Padova 2006, P. 1-354

[78] Arendt H., Vita activa. La condizione umana, trad. it. di Finzi S, Bompiani, Milano, 2017, pp. 1-448: «un uomo che vivesse solo una vita privata e che, come lo schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano» … Di tutte le attività necessarie e presenti nelle comunità umane, solo due erano stimate politiche e costitutive di quello che Aristotele chiamò il bios politikos, cioè l'azione (praxis) e il discorso (lexis), da cui trae origine il dominio degli affari umani […], dal quale ogni cosa meramente necessaria o utile è rigorosamente esclusa»

[79] Niger S. op cit.

[80] Fabris F., Il diritto alla privacy tra passato, presente e futuro, in Tigor: rivista di scienze della comunicazione – A.I (2009) n.2 (luglio-dicembre), p.95: la privacy finiva per essere considerata come "fine a sé stessa, come vita spesa fuori dal mondo comune, acquisiva una connotazione quasi antisociale e, tanto che «lo stesso Platone riteneva che in una società ideale non vi fosse alcun bisogno di una sfera privata in cui l'individuo potesse rifugiarsi. Questo bisogno veniva visto come un pretesto per sottrarsi agli obblighi etici e sociali

Con la feudalizzazione il potere pubblico si frammenta e si cominciano a creare i primi sistemi familiari, basi sul rispetto e sul legame familiare e , a differenza dei periodi precedenti, la privacy comincia ad avere una dimensione più ristretta e non collegata alla vita publica[81].

Lo studioso Mumford nella sua opera del 1967 ha osservato che in tale contesto sociale cominciò a svilupparsi il concetto di intimità intesa quale intimità durante tutti gli aspetti della vita quotidiana e, questo desiderio di intimità segnò l'inizio di quella visione individualista che ancora oggi caratterizza il concetto di privacy[82].

Secondo lo studioso Ariès tra gli elementi che contribuirono all'evoluzione di un concetto di privacy similare a quello moderno, furono la progressiva costruzione dello stato moderno e lo sviluppo dell'alfabetizzazione[83].

Per lo studioso Niger i secoli XVIII e XIX rappresenterebbero l'età aurea del privato, in cui si precisano parole e le nozioni si affinano[84] ed infatti, proprio in tale periodo, due giovani avvocati di Boston, Samuel Warren e Louis Brandeis, hanno elaborato il concetto *right to privacy*[85], ovvero quella che noi definiremmo la prima nozione di privacy in ambito giuridico.

Nel "*The Right to Privacy*", Warren e Brandeis *indicarono thoughts, sentiments and emotions*, come i beni da tutelare giuridicamente in capo ad ogni individuo.

L'opera in esame rappresenta una pietra miliare in materia di privacy in quanto è la prima monografia giuridica a riconoscere l'esistenza di un autonomo diritto alla privacy; prima di allora, le esigenze di tutela della vita privata, seppur avvertite a livello sociale, faticavano a trovare riconoscimento giuridico, incappando nelle ostilità di quella parte della dottrina ancora

[81] Aries P., Duby G , La Vita Privata Dall'impero Romano All'anno Mille, Editori Laterza, Bari, 2001, P.10.: con la feudalizzazione si assiste a uno sbriciolamento che finisce col disseminare i diritti del potere pubblico, di casa in casa, col trasformarsi di ogni grande casa in un piccolo stato sovrano dove si esercita un potere che, pur essendo contenuto in una cornice ristretta, pur essendosi infiltrato in seno alla dimora, conserva nondimeno il suo carattere originale che è pubblico»«…attorno ai termini che esprimono a quest'epoca la nozione di privacy c'è in effetti una costellazione di altri termini che arricchiscono questa nozione. soffermiamoci su uno di questi, *commendatio,* parola chiave, in verità poiché definisce l'entrare in quella relazione su cui si costruiva la concordia nell'interno dei gruppi privati. come tradurre? con quest'atto un individuo si affida, affida la sua persona, si lega al capo di un gruppo e attraverso di lui, a tutti coloro che formano il gruppo, con un legame affettivo molto potente che la lingua volgare e la lingua dotta chiamano amicizia e che costituisce il cemento di tutti gli ordinamenti interni: da tali rapporti è strutturata un'entità sociale riparata da una chiusura protettiva contro la legge, la cui tendenza è ad espandersi, a insinuarsi; quando il potere esteriore riesce a farlo, manifesta la sua potenza mediante un simbolismo di penetrazione»,.

[82] Mumford L., La Cultura Delle Città, Trad. It. Di E. E M. Labò, Giulio Enaudi Editore Milano 2007, P. 53 «Il Primo Mutamento Radicale […] Destinato Ad Infrangere La Forma Della Casa Abitazione Medievale Fu Lo Sviluppo Del Senso Di Intimità»:: "… Intimità durante il sonno; intimità durante i pasti; intimità nel rituale religioso e sociale, intimità nel pensiero.. questo fatto segna la fine delle reciproche relazioni sociali fra i ranghi superiori e quelli inferiori del regime feudale: relazioni che avevano mitigato la sua oppressione. Il desiderio di intimità segnò l'inizio di quel nuovo schieramento di classi che era destinato a finire nella lotta di classe senza quartiere e nelle rivendicazioni individualistiche di un periodo posteriore"

[83] Aries P., Duby G, op cit.

[84] Niger S., op cit p.38 cit.

[85] Warren S., Brandeis L. D., The Right To Privacy, In Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), Pp. 193-220.

fortemente propensa a ricondurle all'interno delle logiche di diversi diritti, quali il diritto alla reputazione e all'onore.

Secondo la teoria dei giuristi in esame, la privacy veniva a coincidere con uno spazio della vita, quasi fisico, dal quale il soggetto aveva un diritto di tenere esclusi gli altri, a loro volta tenuti a rispettarne l'individualità e ciò si traduceva nel diritto dei singoli alla riservatezza, o alla "tutela dell'intimità privata", rispetto a quelle circostanze e vicende intrinsecamente personali e familiari che non avevano per i terzi un interesse socialmente apprezzabile[86].

L'intento di Warren e Brandeis è stato quello di offrire protezione, attraverso la tutela del diritto alla privacy, agli aspetti più intimi e spirituali dell'uomo e, nella loro prospettiva, si abbandonano le logiche materiali ed utilitaristiche per tutelare non solo il valore preminente della proprietà privata ma, anzitutto, quello supremo della inviolabilità personale[87].

Il saggio in esame ha il pregio di criticare la teoria previgente e denunciare l'inadeguatezza degli schemi giuridici fino ad allora utilizzati poiché l'intromissione fisica e materiale non rappresenta più la sola condizione per la violazione del diritto alla riservatezza ma la privacy si tutela per il valore intrinseco che il suo titolare gli affida.

Il taglio evolutivo proposto da Warren e Brandeis appare maggiormente interessante ed euristicamente utile poiché, nel porre l'accento sulle nuove esigenze della società e nell'aprirsi alle novità delle trasformazioni indotte dai più recenti ricavati tecnologici, la tesi evita di inoltrarsi nella (vana) ricerca filosofica dell'essenza dell'istituto.

D'altro canto, sul piano descrittivo, l'approccio di Warren e Brandeis chiarisce il modo in cui l'ordinamento giuridico, quanto meno nel caso del sistema nordamericano di common law, si è venuto trasformando; infatti, quando Warren e Brandeis propongono le definizioni dell'istituto come diritto ad essere lasciati indisturbati (…) il loro scopo non è certo quello di esaurire, ma di illustrare, alcune delle peculiari caratteristiche del diritto.[88]

In sostanza, per Warren e Brandeis il diritto alla privacy è un diritto unitario e la sua violazione dove essere configurata come un illecito civile (tort).

[86] Timiani M., Un contributo allo studio sul diritto alla riservatezza, in Rivista di studi parlamentari e di politica costituzionale, n.176, 2012

[87] Rodotà S., Intervista Su Privacy E Libertà, (A Cura Di)Conti P., Laterza Edizioni, Roma-Bari, 2005, Pp. 8-9, Ove L'illustre Autore Afferma: "Proprio Il Divieto Di Ingresso Nello Spazio Altrui È Lo Snodo Culturale Legato Alla Vicenda Originaria Del Concetto Di Privacy, Di Un Ambito Che Appartiene Solo A Te E A Coloro Con I Quali Vuoi Condividerlo'. E' Il Diritto A Essere Lasciato Da Solo. La Vita Privata Veniva Quindi Tutelata Con La Logica Del Recinto."

[88] PAGALLO U., La tutela della privacy negli Stati Uniti d'America ed in Europa, Giuffrè Francis Lefebvre S,p.A,Milano, 2008, pp 1-258

Su posizioni diametralmente opposte si è posta la teoria elaborata da William Prosser nel suo saggio intitolato Privacy del 1960 il quale, durante uno studio sull'illecito civile, afferma che il diritto alla privacy ricomprende quattro tipi di lesioni di quattro differenti interessi della persona identificati in una intrusione irragionevole della sfera privata di un altro, nell' l'appropriazione del nome dell'altro o delle sue fattezze, in una notorietà data alla vita privata dell'altro senza ragione e in una notorietà che senza ragione piazzi un individuo in una falsa luce agli occhi del pubblico.[89]

La teoria di Prosser disconosce l'esistenza di un diritto alla privacy a sé stante e analizza come la violazione della privacy non dia vita ad un unico e nuovo illecito (tort), ma possa generare quattro diversi tipi di illecito a cui corrispondono tre distinti interessi accumunati esclusivamente dal diritto di escludere gli altri.

A seguito del noto scandalo denominato Watergate che portò alle dimissioni del presidente Nixon, nel 1970 fu emanato il Privacy Act che, ancora oggi, rappresenta un importante testo normativo di riferimento in materia di privacy.

La legge in esame è composta da un articolo, il § 552 del titolo quinto del Codice degli Stati Uniti, suddiviso in ventuno sottoparagrafi rubricati con lettere dell'alfabeto ed ha un ambito di applicazione assai circoscritto poiché disciplina la raccolta, la classificazione, l'uso delle informazioni solo da parte dell'organo pubblico.

Infine, occorre sottolineare il ruolo chiave che ha avuto la giurisprudenza in merito alla tutela della privacy, la quale ha applicato i principi elaborati «a situazioni profondamente differenti che vanno dal diritto del singolo ad impedire comportamenti intrusivi nella propria vita privata ad opera dei media, al diritto di aborto, alla libertà sessuale»[90].

Si giunge, pertanto, a parlare *di informational privacy* e di *decisional pivacy* le quali hanno come fulcro il riconoscimento e la garanzia del potere di autocontrollo in capo al singolo, ma nel primo caso si manifesta in una sorta di signoria sulle informazioni inerenti la propria persona, traducendosi in un limite non solo alla diffusione di indiscrezioni sulla vita privata, ma anche, più in generale, alla raccolta ed all'impiego arbitrario dei dati personali, mentre nella seconda declinazione la privacy diviene la libertà di autodeterminarsi rispetto alle scelte

[89] Cosi Prosser W,. Privacy, A Legal Analysis, In California Law Review, N.48, 1960, Pp. 383-423,: ""One who invades the right of privacy of another subject to liability for the resulting harm to the interest of the other. The right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another...; or (b) appropriation of the other's name or likeness...; or (c) unreasonable publicity given to the other's private life...; or (d) publicity that unreasonably places the other in a false light before the public

[90] Mantelero A., Il Costo Della Privacy Tra Valore Della Persona E Ragione D'impresa, Giuffrè Editore, Milano, 2007, Pp.1-344

personali, siano esse pertinenti alla procreazione, alla libertà sessuale o alla libertà di organizzazione [91].

Il concetto di *right to privacy* finisce per diventare un "contenitore concettuale", come lo chiama Mantelero, all'interno del quale confluiscono tutte le modalità di tutela della libertà personale garantite al singolo dallo Stato.[92]

2.2 Dal diritto alla privacy al diritto alla protezione dei dati personali in ambito internazionale

Il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, sebbene strettamente connessi, sono diritti distinti in quanto il primo, fa riferimento al diritto alla riservatezza delle informazioni personali e della propria vita privata ed è un principio utilizzato come strumento per tutelare la sfera intima del singolo individuo, volto ad impedire che le informazioni siano divulgate in assenza di specifica autorizzazione, mentre la protezione dei dati personali, è un sistema di trattamento degli stessi che identifica direttamente o indirettamente una persona.

Nel diritto internazionale in materia di diritti umani, il diritto alla vita privata, conosciuto nel diritto europeo come diritto al rispetto della vita privata, è stato sancito nella dichiarazione universale dei diritti dell'uomo (UDHR), adottata il 10 dicembre 1948, dall'Assemblea Generale delle Nazioni Unite.

La Dichiarazione Universale dei Diritti Umani del 1948 fu il primo Trattato che diede un riconoscimento alla dignità dell'essere umano, elaborando dei diritti inalienabili posti a fondamento della libertà, della giustizia e della pace nel mondo[93].

---

[91] Mantelero A.,op. cit. p.41.

[92] Fabris F.op cit.p.38

[93] Dichiarazione Universale dei Diritti Umani del 1948, nel cui preambolo si può leggere: "*Considerato che il riconoscimento della dignità inerente a tutti i membri della famiglia umana e dei loro diritti, uguali ed inalienabili, costituisce il fondamento della libertà, della giustizia e della pace nel mondo; Considerato che il disconoscimento e il disprezzo dei diritti umani hanno portato ad atti di barbarie che offendono la coscienza dell'umanità, e che l'avvento di un mondo in cui gli esseri umani godano della libertà di parola e di credo e della libertà dal timore e dal bisogno è stato proclamato come la più alta aspirazione dell'uomo; Considerato che è indispensabile che i diritti umani siano protetti da norme giuridiche, se si vuole evitare che l'uomo sia costretto a ricorrere, come ultima istanza, alla ribellione contro la tirannia e l'oppressione; Considerato che è indispensabile promuovere lo sviluppo di rapporti amichevoli tra le Nazioni; Considerato che i popoli delle Nazioni Unite hanno riaffermato nello Statuto la loro fede nei diritti umani fondamentali, nella dignità e nel valore della persona umana, nell'uguaglianza dei diritti dell'uomo e della donna, ed hanno deciso di promuovere il progresso sociale e un miglior tenore di vita in una maggiore libertà; Considerato che gli Stati membri si sono impegnati a perseguire, in cooperazione con le Nazioni Unite, il rispetto e l'osservanza universale dei diritti umani e delle libertà fondamentali; Considerato che una concezione comune di questi diritti e di questa libertà è della massima importanza per la piena realizzazione di questi impegni; L'ASSEMBLEA GENERALE proclama la presente dichiarazione universale dei diritti umani come ideale comune da raggiungersi da tutti i popoli e da tutte le Nazioni, al fine che ogni individuo ed ogni organo della società, avendo costantemente presente questa Dichiarazione, si sforzi di promuovere, con l'insegnamento e l'educazione, il rispetto di questi diritti e di queste libertà e di garantirne, mediante misure progressive di carattere nazionale e internazionale, l'universale ed effettivo riconoscimento e rispetto tanto fra i popoli degli stessi Stati membri, quanto fra quelli dei territori sottoposti alla loro giurisdizione*"

Nell'art. 12 del Trattato in esame viene tutelata la riservatezza di ogni individuo da possibili condotte intrusive e lesive di altri beni giuridici primari, come l'onore o la reputazione.

Poco dopo l'adozione di tale dichiarazione, anche l'Europa ha sancito questo diritto, nella Convenzione europea dei diritti dell'uomo (CEDU), un trattato giuridicamente vincolante per le parti contraenti redatto nel 1950, all'art. 8 della CEDU, il quale tutela il diritto alla riservatezza e al benessere della vita privata e familiare, configurati come beni giuridici di primaria importanza, ed è finalizzato alla tutela contro le ingerenze arbitrarie da parte di un'autorità pubblica.

La CEDU, infatti, stabilisce che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza e l'ingerenza di un'autorità pubblica in questo diritto è vietata, salvo i casi in cui sia prevista dalla legge, persegua interessi pubblici importanti e legittimi e sia necessaria in una società democratica.

Si tratta di un classico obbligo negativo, bilanciato con l'obbligo positivo degli Stati membri di garantire che i diritti previsti dall'articolo 8 CEDU siano rispettati anche tra privati: lo Stato deve tener conto del giusto equilibrio tra gli interessi concorrenti della persona e della collettività nel suo insieme.

Pochi anni più tardi, l'Organizzazione delle Nazioni Unite adottò la Convenzione internazionale sui diritti civili e politici che entro in vigore il 23/3/1976 che, nell'art 17, proibisce la sottoposizione di un individuo a illegittime interferenze nella vita privata o a offese all'onore o alla reputazione[94].

Dal diritto rispetto della vita privata e familiare, del domicilio e della corrispondenza si è sviluppato il diritto alla tutela dei dati personali, la cui protezione è stata inaugurata in Europa negli anni '70 con l'adozione di alcune normative, da parte di alcuni Stati, finalizzate a controllare il trattamento de dati personali da parte delle autorità pubbliche e delle grandi imprese, si pensi ad esempio al Land tedesco dell'Assia, il quale ha adottato nel 1970 la prima legge sulla protezione dei dati.

L'emergere delle nuove tecnologie ha determinato un crescente bisogno di norme più dettagliate per tutelare le persone fisiche, proteggendone in particolare i dati personali e, pertanto, a metà degli anni '70, il Comitato dei Ministri del Consiglio d'Europa ha adottato

[94] L'art 17 Della Convenzione Internazionale Sui Diritti Civili E Politici Dispone Che: ". Nessuno Può Essere Sottoposto Ad Interferenze Arbitrarie O Illegittime Nella Sua Vita Privata, Nella Sua Famiglia, Nella Sua Casa O Nella Sua Corrispondenza, Né A Illegittime Offese Al Suo Onore E Alla Sua Reputazione. 2. Ogni Individuo Ha Diritto Ad Essere Tutelato Dalla Legge Contro Tali Interferenze Od Offese".

varie risoluzioni in tale materia, facendo riferimento alla giurisprudenza elaborata della Corte Edu in relazione all'interpretazione dell'articolo 8 CEDU.

Nel 1981 è stata aperta la firma alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (cosiddetta Convenzione n. 108), la quale si applica a tutti i trattamenti di dati personali [95] effettuati sia nel settore privato che in quello pubblico, compresi quelli effettuati da autorità giudiziarie e di polizia.[96]

La Convenzione 108 mira non solo a proteggere gli individui dagli abusi che possono accompagnare il trattamento dei dati personali ma cerca di regolamentare i flussi transfrontalieri degli stessi e i principi su cui si fonda sono: la correttezza e la liceità della raccolta e del trattamento automatizzato dei dati, che devono essere raccolti e trattati per specifici scopi legittimi e, pertanto, essi non devono essere destinati a un uso incompatibile con tali scopi, né conservati oltre il tempo necessario.

La Convenzione 108, nel caso in cui lo Stato non possa offrire adeguate garanzie giuridiche, vieta il trattamento dei dati «sensibili», come la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale o il casellario giudiziale di un individuo e le eccezioni al suo rispetto sono possibili solo quando vi siano in gioco interessi superiori, quali la sicurezza o la difesa dello Stato; inoltre, la Convenzione 108 prevede la libera circolazione dei dati personali tra le parti contraenti ma impone alcune restrizioni su tali flussi verso paesi in cui la regolamentazione giuridica non conferisce una protezione equivalente.

Tutti gli Stati membri dell'UE hanno ratificato la Convenzione n. 108 e, nel 1999, essa è stata emendata per consentire all'Unione Europea di diventarne parte contraente; inoltre, la convenzione è aperta anche all'adesione di paesi extra- Ue e, ad oggi, ne fanno parte più di 50 paesi tra cui possiamo ricordare tutti gli Stati membri del Consiglio d'Europa (47 paesi), l'Uruguay, che è stato il primo paese extraeuropeo che vi ha aderito, il Senegal e la Tunisia.

A seguito dell'avvento della digitalizzazione, la Convenzione è stata oggetto di un processo di modernizzazione volto al rafforzamento della protezione della vita privata nel settore digitale e al consolidamento del meccanismo di attuazione della stessa; il processo di modernizzazione è stato completato il 18 aprile 2018 con l'adozione del protocollo di modifica

[95] Art. 4, Punto 2 Del Gdpr: Per Trattamento Dei Dati Personali Si Intende "Qualsiasi Operazione O Insieme Di Operazioni, Compiute Con O Senza L'ausilio Di Processi Automatizzati E Applicate A Dati Personali O Insiemi Di Dati Personali, Come La Raccolta, La Registrazione, L'organizzazione, La Strutturazione, La Conservazione, L'adattamento O La Modifica, L'estrazione, La Consultazione, L'uso, La Comunicazione Mediante Trasmissione, Diffusione O Qualsiasi Altra Forma Di Messa A Disposizione, Il Raffronto O L'interconnessione, La Limitazione, La Cancellazione O La Distruzione"

[96] Convenzione 108 del Consiglio d'Europa, (conosciuta anche come Convenzione di Strasburgo del 1981) il cui scopo è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)

(Protocollo CETS No. 223), il quale rafforza la sua posizione di strumento universale sul diritto in materia di protezione dei dati.

Nella nuova formulazione della Convenzione 108 si riaffermano e consolidano i principi generali e si prevedono nuovi diritti a vantaggio degli individui, ampliando, al contempo, le responsabilità delle entità preposte al trattamento dei dati personali e assicurando maggiore responsabilità.

Al fine di contrastare l'aumento dell'attività di profilazione nel mondo online, la Convenzione sancisce altresì il diritto dell'individuo a non essere assoggettato a decisioni fondate esclusivamente su trattamenti automatizzati e senza che siano prese in considerazione le sue opinioni.

L'Italia ha ratificato la nuova Convenzione 108 il 5 marzo del 2019.

2.3 IL DIRITTO DELL'UNIONE EUROPEA

2.3.1 L'evoluzione del diritto alla privacy nei Trattati Istitutivi

Il diritto dell'Unione europea si divide in diritto primario e diritto secondario o derivato.

A livello primario si ha il Trattato sull'Unione europea (TUE) e il trattato sul funzionamento dell'Unione europea (TFUE) che sono stati ratificati da tutti gli Stati membri dell'UE; a livello secondario, invece, si hanno i regolamenti, le direttive e le decisioni dell'UE, adottati dalle istituzioni, e che costituiscono il cosiddetto «diritto derivato».

L'evoluzione del diritto alla privacy nel contesto dell'Unione europea può essere riassunta in quattro fasi specifiche.

In una prima fase, i trattati originari delle Comunità europee non contenevano riferimenti ai diritti umani o alla loro protezione, in quanto, inizialmente, la Comunità Economica Europea era considerata un'organizzazione regionale volta all'integrazione economica e all'istituzione di un mercato comune.

I primi trattati istitutivi dell'UE, infatti, non prevedono competenze esplicite in materia di diritti fondamentali ma erano fondati sul principio di attribuzione, in virtù del quale l'UE agiva esclusivamente nei limiti delle competenze che le erano state attribuite dagli Stati membri.

La seconda fase si caratterizza per la produzione giurisprudenziale della Corte di Giustizia dell'Unione Europea, la quale è stata chiamata a pronunciarsi su cause relative a violazioni dei diritti umani in contesti rientranti nell'ambito di applicazione del diritto dell'UE.

La CGUE, interpretando i trattati, ha introdotto i diritti fondamentali nei cosiddetti principi generali del diritto europeo, i quali riflettono la protezione dei diritti umani garantiti dalle costituzioni nazionali e dai trattati sui diritti umani e elaborati sull'orientamento della stessa Corte di Giustizia e della Corte Edu.[97]

La terza fase coincide con la proclamazione nel 2000 della Carta dei diritti fondamentali dell'Unione europea (cd. Carta di Nizza) che incorpora la totalità dei diritti civili, politici, economici e sociali dei cittadini europei, sintetizzando le tradizioni costituzionali e gli obblighi internazionali comuni agli Stati membri.

I diritti descritti nella Carta sono suddivisi in sei titoli: dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia.

La Carta garantisce non solo il rispetto della vita privata e della vita familiare (articolo 7), ma stabilisce anche il diritto alla protezione dei dati di carattere personale (articolo 8), innalzando esplicitamente il livello di tale protezione a quello di un diritto fondamentale nell'ambito del diritto dell'UE.

La Carta di Nizza, dunque, non solo menziona esplicitamente, all'articolo 8, paragrafo 1, il diritto alla protezione dei dati, ma all'articolo 8, paragrafo 2, fa altresì riferimento ai principi fondamentali della protezione dei dati.

Gli articoli sopra citati devono essere letti alla luce degli articoli 51[98] e 52[99] della Carta di Nizza: l'art 51 CDFUE, infatti, limita l'ambito dell'applicazione dei diritti riconosciuti nella

[97] Tra le sentenze della Corte ricordiamo: Sentenza 12 Novembre 1969, Erich Stauder C. Città Di ULM – Sozialamt, Causa 29/69 https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A61969CJ0029 ; Sentenza 14 maggio 1974, J. Nold, Kohlen- und Baustoffgroβhandlung c. Commissione, causa 4/73, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A61973CJ0004 ; Sentenza 13 Dicembre 1979, Liselotte Hauer C. Land Rheinland – Pfalz, Causa C-44/79, https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A61979CJ0044 ; Sentenza 13 Luglio 1989, Hubert Wachauf C. Germania, Causa C-5/88, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A61988CJ0005; Sentenza 15 Maggio 1986, Marguerite Johnston C. Chief Constable Of The Royal Ulster Constabulary, Causa 222/84 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A61984CJ0222 (6 giugno 2022)

[98] Art 51 Cdfue: " Le Disposizioni Della Presente Carta Si Applicano Alle Istituzioni, Organi E Organismi Dell'unione Nel Rispetto Del Principio Di Sussidiarietà, Come Pure Agli Stati Membri Esclusivamente Nell'attuazione Del Diritto Dell'unione. Pertanto, I Suddetti Soggetti Rispettano I Diritti, Osservano I Principi E Ne Promuovono L'applicazione Secondo Le Rispettive Competenze E Nel Rispetto Dei Limiti Delle Competenze Conferite All'unione Nei Trattati. 2. La Presente Carta Non Estende L'ambito Di Applicazione Del Diritto Dell'unione Al Di Là Delle Competenze Dell'unione, Né Introduce Competenze Nuove O Compiti Nuovi Per L'unione, Né Modifica Le Competenze E I Compiti Definiti Nei Trattati"

[99] Art 52 Cdfue: Eventuali Limitazioni All'esercizio Dei Diritti E Delle Libertà Riconosciuti Dalla Presente Carta Devono Essere Previste Dalla Legge E Rispettare Il Contenuto Essenziale Di Detti Diritti E Libertà. Nel Rispetto Del Principio Di Proporzionalità, Possono Essere Apportate Limitazioni Solo Laddove Siano Necessarie E Rispondano Effettivamente A Finalità Di Interesse Generale Riconosciute Dall'unione O All'esigenza Di Proteggere I Diritti E Le Libertà Altrui. 2. I Diritti Riconosciuti Dalla Presente Carta Per I Quali I Trattati Prevedono Disposizioni Si Esercitano Alle Condizioni E Nei Limiti Dagli Stessi Definiti. 3. Laddove La Presente Carta Contenga Diritti Corrispondenti A Quelli Garantiti Dalla Convenzione Europea Per La Salvaguardia Dei Diritti Dell'uomo E Delle Libertà Fondamentali, Il Significato E La Portata Degli Stessi Sono Uguali A Quelli Conferiti Dalla Suddetta Convenzione. La Presente Disposizione Non Preclude Che Il Diritto Dell'unione Conceda Una Protezione Più Estesa. 4. Laddove La Presente Carta Riconosca I Diritti Fondamentali Quali Risultano Dalle Tradizioni Costituzionali Comuni Agli Stati Membri, Tali Diritti Sono Interpretati In Armonia Con Dette Tradizioni. 5. Le Disposizioni Della Presente Carta Che Contengono Dei Principi Possono Essere Attuate Da Atti

stessa alle istituzioni e agli organi dell'Unione, nel rispetto del principio di sussidiarietà, come pure agli Stati membri, esclusivamente, però, nell'attuazione del diritto dell'Unione.

Mentre, l'articolo 52, al paragrafo 1, stabilisce che le limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta e l'esercizio del diritto alla protezione dei dati personali, saranno ammissibili solo se:

• sono previste dalla legge: tale requisito implica che le limitazioni devono fondarsi su una base giuridica che sia adeguatamente accessibile e prevedibile, oltre a essere formulate con precisione sufficiente per consentire alle persone di conoscere i propri obblighi e regolare la propria condotta;

• rispettino il contenuto essenziale del diritto alla protezione dei dati: le limitazioni estese e invasive, tali da svuotare il diritto fondamentale del suo contenuto di base, non saranno giustificate, infatti, se il contenuto essenziale del diritto è pregiudicato, la limitazione dev'essere considerata illegittima senza che occorra valutare ulteriormente se essa risponda o meno a una finalità di interesse generale ovvero soddisfi i requisiti della necessità e della proporzionalità;

• siano necessarie, nel rispetto del principio di proporzionalità: una limitazione può essere necessaria qualora occorra adottare misure ai fini del raggiungimento dell'obiettivo di interesse generale perseguito; la CGUE applica un rigido criterio di necessità, sostenendo che «deroghe e restrizioni intervengono entro i limiti dello stretto necessario» e. se una limitazione è considerata strettamente necessaria, occorrerà anche valutare se sia proporzionata.

Il principio di proporzionalità esige che i vantaggi risultanti dalla limitazione debbano prevalere sugli svantaggi causati dalla stessa in relazione all'esercizio dei diritti fondamentali in questione;

• rispondano a finalità d'interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui: per essere giustificate, le eventuali limitazioni all'esercizio dei diritti riconosciuti dalla Carta dovranno anche rispondere effettivamente alle finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Legislativi E Esecutivi Adottati Da Istituzioni, Organi E Organismi Dell'unione E Da Atti Di Stati Membri Allorché Essi Danno Attuazione Al Diritto Dell'unione, Nell'esercizio Delle Loro Rispettive Competenze. Esse Possono Essere Invocate Dinanzi A Un Giudice Solo Ai Fini Dell'interpretazione E Del Controllo Di Legalità Di Detti Atti. 6. Si Tiene Pienamente Conto Delle Legislazioni E Prassi Nazionali, Come Specificato Nella Presente Carta. 7. I Giudici Dell'unione E Degli Stati Membri Tengono Nel Debito Conto Le Spiegazioni Elaborate Al Fine Di Fornire Orientamenti Per L'interpretazione Della Presente Carta

Gli obiettivi di interesse generale includono gli obiettivi sanciti dall'articolo 3 del trattato sull'Unione europea (TUE), quali la promozione della pace e del benessere dei suoi popoli, la giustizia e la protezione sociale, la creazione di uno spazio di libertà, sicurezza e giustizia in cui sia assicurata la libera circolazione delle persone, insieme a misure appropriate per quanto concerne la prevenzione della criminalità e la lotta contro quest'ultima, come pure altri obiettivi e interessi tutelati da disposizioni specifiche all'interno dei Trattati istitutivi;

L'art 51 e 52 CDFUE hanno rappresentato e rappresentano tutt'oggi un prezioso strumento d'interpretazione destinato a chiarire le disposizioni della Carta, hanno portata generale e devono essere sempre tenuti in considerazione qualora occorra interpretare o bilanciare i diritti fondamentali riconosciuti ai cittadini dell'Unione Europea.

La quarta fase coincide con l'adozione del trattato di Lisbona, avvenuta il 1° dicembre 2009, pietra miliare nello sviluppo della legislazione in materia di protezione dei dati poiché, nell'art 6 paragrafo 1 del TUE, l'Unione Europea ha elevato la Carta di Nizza allo status di documento legale vincolante a livello di diritto primario mentre, nell'art 16 TFUE ha previsto espressamente il diritto alla protezione dei dati personali.

L'articolo 16 TFUE[100] crea una nuova base giuridica, conferendo all'UE la competenza a legiferare in materia di protezione dei dati e ciò si identifica in uno sviluppo importante, poiché, come già analizzato, la legislazione dell'UE in materia di protezione dei dati personali era volta alla primaria tutela del mercato interno ed era mossa dalla necessità di ravvicinare le legislazioni nazionali al fine esclusivo di non ostacolare la libera circolazione dei dati nell'UE.

Occorre premettere che l'articolo 16 TFUE è stata la base giuridica per l'adozione della riforma globale delle norme in materia di protezione dei dati nel 2016, vale a dire, il regolamento generale sulla protezione dei dati e la direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali[101].

[100] L'art 16 Tfue, Infatti, Dispone Che: "1. ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. il parlamento europeo e il consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'unione, nonché da parte degli stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'unione, e le norme relative alla libera circolazione di tali dati. il rispetto di tali norme è soggetto al controllo di autorità indipendenti. le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'unione europea."

[101] AA. VV., Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018, Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, 2018 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_it.pdf , (07 giugno 2022)

2.3.2 L'evoluzione del diritto alla privacy nel diritto derivato dell'Unione Europea

A livello derivato, la tutela del diritto alla privacy e alla riservatezza è stata in primo luogo disciplinata dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, inerente alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (direttiva sulla tutela dei dati).

Con la direttiva 46 del 1995, il legislatore europeo ha inteso fissare un nucleo di regole e di criteri comuni al fine di garantire un'omogenea protezione dei dati delle persone nel territorio dell'Unione[102] e ciò in quanto, alcuni Stati membri avendo adottato delle leggi nazionali in materia di protezione dei dati, garantivano un livello di tutela diversificato all'interno del territorio europeo.

In tale contesto è sorta la necessità di armonizzare la legislazione positiva al fine di garantire un livello elevato di protezione e il libero flusso di dati personali tra i diversi Stati membri.

La direttiva in esame ha ribadito, in primo luogo, i principi di protezione dei dati già contemplati dalle legislazioni nazionali e dalla Convenzione n. 108 ed ha introdotto le autorità di controllo indipendenti al fine di migliorare l'osservanza delle norme sulla protezione dei dati.

La direttiva sulla tutela dei dati ha istituito nell'UE un sistema di protezione dei dati dettagliato e completo ma, non essendo direttamente applicabile, ha portato alla creazione di norme diversificate, le quali, a causa delle diverse definizioni e dei diversi livelli di attuazione e di severità delle sanzioni, hanno determinato uno squilibrio di tutela e, nei casi più gravi , un vero e proprio deficit di tutela all'interno di alcuni Stati membri.

Nel 2009 la Commissione ha effettuato una consultazione pubblica sul futuro quadro giuridico riguardante il diritto fondamentale alla protezione dei dati personali e la proposta di regolamento è stata pubblicata dalla Commissione nel gennaio 2012, la quale ha dato avvio ad un lungo iter legislativo di negoziazione tra il Parlamento europeo e il Consiglio dell'UE, sfociato nel 2016 con l'adozione regolamento generale sulla protezione dei dati (cd. GDPR), diventato poi pienamente applicabile il 25 maggio 2018.[103]

Il regolamento generale sulla protezione dei dati è direttamente applicabile all'interno di tutti gli Stati membri e, quest'ultimi, sono tenuti ad aggiornare le legislazioni nazionali vigenti in materia di protezione dei dati al fine di allinearsi integralmente ad esso.

[102] AA.VV. I Dati Personali Nel Diritto Privato Europeo, G. Giappichelli Editore, Torino 2019
[103] AA. VV., Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018 op cit. p. 50

Il regolamento rappresenta una poderosa opera di riorganizzazione e di riformulazione del diritto europeo sulla protezione dei dati personali ed ha un livello di generalizzazione adeguato a un testo normativo che mira a essere il perno, o ancor meglio la cornice, della legislazione europea in materia.

Nel compiere l'impresa della ridefinizione del diritto europeo sulla protezione dei dati personali, il GDPR non ha operato però delle scelte neutrali, in quanto non si è limitato a ricostruire il diritto vigente in chiave prevalentemente ricognitiva, come nella tradizione dei *Restatement*, ma ha compiuto scelte significative di politica del diritto[104], positivizzando numerosi principi elaborati in seno alla Corte Europea di Diritti dell'Uomo e alla Corte di Giustizia dell'Unione Europea.

La difficoltà di trovare un fondamento unitario al concetto di privacy ha suggerito di negare autonomia allo stesso e, il diritto alla riservatezza, è stato ricondotto ad altre nozioni fondamentali come quelle di solitudine, intimità e anonimato.

Le principali innovazioni apportate dal Regolamento 2016/679 che si rendono utili ai fini della presente ricerca sono i principi nella liceità nel trattamento dei dati personali, i «diritti dell'interessato» ma soprattutto occorre rilevare che il parametro legale è stato ampliato rispetto alla previgente normativa.

Per quanto attiene ai principi fondamentali, l'art. 5[105] reg. 2016/679 elenca una serie di principi che si applicano a tutti i trattamenti di dati personali: liceità del trattamento, correttezza del trattamento, trasparenza del trattamento, il principio di limitazione della finalità, il principio

[104]Piraino, F. Il Regolamento Generale Sulla Protezione Dei Dati Personali E I Diritti Dell'interessato. Le Nuove Leggi Civili Commentate, 40(2), Wolters Kluwer S.P.A , 2017 Pp. 369-409, Pag .375 In Nota N.16: ovviamente la natura ricognitiva del restatement e` un elemento soltanto tendenziale giacche´ il diritto statunitense e` vario, percorso com'è da soluzioni differenti da stato a stato, e non è infrequente che nella riorganizzazione si prediliga una soluzione minoritaria, in tal modo compiendo un giudizio di valore e non di fatto che produce un rinnovamento normativo. Sul Punto Cfr. AJANI G., PASA B, Diritto Comparato, Lezioni E Materiali, Giappichelli Editore, Torino, 2018 Pp. 1-424.

[105] Art 5 Reg. 2016/679: *I dati personali sono: (C39) a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati(«minimizzazione dei dati»);d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli percancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione,*
mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74)

di minimizzazione dei dati, il principio di esattezza dei dati, il principio della limitazione della conservazione, il principio della sicurezza dei dati e il principio di responsabilizzazione.

In relazione al principio della liceità del trattamento, il GDPR richiede il consenso dell'interessato, che deve essere volontario, consapevole, specifico e inequivocabile, e l'assenso a che i dati personali siano oggetto di trattamento deve essere manifestato mediante azione positiva, o un'altra base legittima prevista dalla legislazione in materia di protezione dei dati.

In relazione al principio di correttezza del trattamento, il GDPR disciplina principalmente la relazione tra il titolare del trattamento e l'interessato: i responsabili del trattamento dei dati dovrebbero informare gli interessati e il pubblico in generale del fatto che tratteranno i dati in modo lecito e trasparente con l'onere di essere in grado di dimostrare la conformità delle operazioni di trattamento alle disposizioni legislative vigenti.

I responsabili del trattamento dei dati dovrebbero, per quanto possibile, agire in modo da conformarsi prontamente alla volontà dell'interessato, specialmente quando il suo consenso costituisca la base giuridica del trattamento dei dati e, inoltre, tale principio è rivolto anche ai servizi Internet, i cui sistemi di trattamento dovrebbero essere tali da consentire agli interessati di comprendere realmente ciò che accade ai loro dati.

In relazione al principio di trasparenza del trattamento, il GDPR sancisce l'obbligo per il titolare del trattamento di adottare misure appropriate per tenere informati gli interessati sul modo in cui verranno utilizzati i dati: il responsabile del trattamento ha l'obbligo di fornire agli interessati le informazioni concernenti il nome e l'indirizzo del titolare del trattamento, la base giuridica, le finalità del trattamento, le categorie di dati trattati e i loro destinatari nonché i mezzi di tutele riconosciuti dall'ordinamento.

Tali informazioni possono essere fornite in qualsiasi forma purché essa sia presentata all'interessato in maniera corretta, efficace, facilmente accessibile e comprensibile sulla base del rispetto del principio di trasparenza, il quale si riferisce non solo alle informazioni fornite alla persona prima dell'inizio del trattamento e durante lo stesso, ma anche alle informazioni fornite agli interessati a seguito di una richiesta di accesso ai dati che li riguardano[106].

[106] AA. VV., Manuale Sul Diritto Europeo In Materia Di Protezione Dei Dati, Edizione 2018 Op Cit. P. 50, Principi Espressi Nella Causa Haralambie C. Romania, in cui il ricorrente aveva ottenuto l'accesso alle informazioni che lo riguardavano, conservate dall'organizzazione di servizi segreti, solo cinque anni dopo la sua richiesta. la corte edu ha ribadito che gli individui oggetto dei fascicoli personali tenuti dalle autorità pubbliche avevano un interesse vitale ad accedervi e le autorità avevano il dovere di mettere a disposizione una procedura efficace per ottenere l'accesso a tali informazioni; inoltre, la corte edu ha ritenuto che né la quantità di fascicoli trasmessi né le lacune del sistema di archivio giustificassero la violazione.

In base al diritto di accesso, l'interessato ha il diritto di ottenere, a sua richiesta, dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati che lo riguarda e, in tal caso, ha il diritto di conoscere quali dati saranno soggetti a tale trattamento.

Il diritto all'informazione prevede che le persone i cui dati verranno trattati debbano essere informate in maniera proattiva dai titolari o responsabili del trattamento circa le finalità, la durata, i mezzi di trattamento, oltre ad altri dettagli, prima dell'inizio dell'attività di trattamento.

Il principio in esame era già stato specificato dalla Corte di Giustizia dell'Unione Europea nella causa *Smaranda Bara e a. c. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală* (ANAF)[107].

Nella sentenza sopra citata, la CGUE è stata adita, in via pregiudiziale, al fine di stabilire se gli articoli 10, 11 e 13 della direttiva 95/46 debbano essere interpretati nel senso che essi ostano a misure nazionali che consentono a un'amministrazione pubblica di uno Stato membro di trasmettere dati personali a un'altra amministrazione pubblica, a fini di trattamento, senza che le persone interessate siano state informate né di tale trasmissione né del successivo trattamento.

La CGUE, nella sentenza in esame, ha statuito che : "*Gli articoli 10, 11 e 13 della 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, devono essere interpretati nel senso che essi ostano a misure nazionali, come quelle di cui trattasi nel procedimento principale, che consentono a un'amministrazione pubblica di uno Stato membro di trasmettere dati personali a un'altra amministrazione pubblica, a fini di trattamento, senza che le persone interessate siano state informate né di tale trasmissione né del successivo trattamento".*

La Corte di Giustizia dell'Unione Europea ha riconosciuto nella controversia *Smaranda Bara e a. c. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF*) la preminenza del diritto all'informazione del privato rispetto al trattamento congiunto dei dati da parte delle Autorità pubbliche.

In relazione al principio di limitazione della finalità, esso è uno dei principi fondamentali del diritto europeo in materia di protezione dei dati ed è strettamente connesso con la trasparenza, la prevedibilità e il controllo dell'utente, infatti, se lo scopo del trattamento è

[107] Sentenza 1° ottobre 2015, Smaranda Bara e a. c. Casa Naţională de Asigurări de Sănătate e a., Causa C-201/14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0201 , (20 giugno 2022)

sufficientemente specifico e chiaro, le persone sanno cosa aspettarsi e aumentano così la trasparenza e la certezza del diritto e, al tempo stesso, una chiara indicazione della finalità è importante per consentire agli interessati di esercitare efficacemente i loro diritti, come il diritto di opposizione al trattamento.

In base a questo principio, il trattamento di dati personali deve essere effettuato per una finalità specifica e ben definita e solo per scopi ulteriori e compatibili con la finalità iniziale[108], viceversa, il trattamento è illecito.

Al pari è illecito anche il trattamento dei dati personali senza finalità certa, basato unicamente sulla considerazione che tali dati potrebbero essere utili in un futuro, infatti ogni nuova finalità di trattamento dei dati che non sia compatibile con le finalità iniziali deve avere la propria base giuridica specifica e non può fondarsi sul fatto che i dati fossero stati inizialmente acquisiti o trattati per un'altra finalità legittima.[109]

In relazione al principio di minimizzazione dei dati, esso richiede che il trattamento dei dati deve essere limitato a quanto strettamente necessario per perseguire una finalità legittima e i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi; inoltre, il trattamento dei dati non deve interferire in modo sproporzionato con gli interessi, i diritti e le libertà in gioco.

Il principio di minimizzazione dei dati è stato oggetto della causa Corte Di Giustizia (Grande Sezione), 8 Aprile 2014, Cause Riunite C-293/12 E C-594/12, *Digital Rights Ireland*, ove la Corte è stata chiamata a pronunciarsi sulla validità della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE[110].

La High Court (Alta Corte, Irlanda) nonché il Verfassungsgerichtshof (Corte costituzionale, Austria) hanno chiesto alla Corte di giustizia di esaminare la validità della direttiva n. 2002/58/CE in relazione agli artt. 7 e 8 dalla Carta dei diritti fondamentali

[108] Art 5 Reg. 2016/679

[109] Il Regolamento generale sulla protezione dei dati e la Convenzione n. 108 modernizzata dichiarano che: "[l]'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici» dovrebbe a priori essere considerato compatibile con la finalità iniziale. Tuttavia, per l'ulteriore trattamento di dati personali devono essere previste garanzie adeguate, come l'anonimizzazione, la criptatura o la pseudonimizzazione dei dati e la limitazione dell'accesso ai dati".

[110] Sentenza della Corte, Grande Sezione, dell'8 aprile 2014, Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a., Cause riunite C-293/12 e C-594/12, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0293 (22 giugno 2022)

dell'Unione europea, ossia il diritto al rispetto della vita privata e il diritto alla protezione dei dati di carattere personale[111].

La Corte, analizzando la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, ha ritenuto che il legislatore dell'Unione, con l'adozione della direttiva sulla conservazione dei dati, abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità poiché essa non prevede alcun criterio oggettivo che consenta di garantire che le autorità nazionali competenti abbiano accesso ai dati e possano utilizzarli solamente per prevenire, accertare e perseguire penalmente reati che possano essere considerati, tenuto conto della portata e della gravità dell'ingerenza nei diritti fondamentali summenzionati, sufficientemente gravi da giustificare una simile ingerenza. Al contrario, la direttiva si limita a fare generico rinvio ai «reati gravi» definiti da ciascuno Stato membro nella propria legislazione nazionale.

Pertanto, la CGUE nella controversia in esame afferma il seguente principio di diritto: "*La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, è invalida*[112]."

La Corte di Giustizia ha riconosciuto che lo stesso legislatore europeo non ha fatto buon uso dei principi generali costruendo una norma che per la sua genericità non avrebbe mai tutelato i cittadini comunitari e, pertanto, e ha dichiarato invalida la direttiva 2006/24/CE,

In relazione al principio di esattezza dei dati, esso impone al titolare del trattamento, in tutte le operazioni di trattamento, di cancellare o rettificare tempestivamente i dati inesatti ovvero di controllare costantemente o aggiornare i dati al fine di garantirne l'esattezza.

Nella causa CGUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer del 7 maggio 2009*, la Corte di Giustizia dell'Unione Europea è stata chiamata a fornire una pronuncia pregiudiziale sull'interpretazione dell'art. 12, lett. a), della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela

[111] Sentenza,Digital Rights Ireland Ltd, Op. Cit. P.55 "la corte rileva, anzitutto, che i dati da conservare consentono, in particolare, 1) di sapere con quale persona e con quale mezzo un abbonato o un utente registrato ha comunicato, 2) di determinare il momento della comunicazione nonché il luogo da cui ha avuto origine e 3) di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con determinate persone in uno specifico periodo. tali dati, considerati congiuntamente, possono fornire indicazioni assai precise sulla vita privata dei soggetti i cui dati sono conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri o di diversa frequenza, le attività svolte, le relazioni sociali e gli ambienti sociali frequentati. la corte ritiene che la direttiva, imponendo la conservazione di tali dati e consentendovi l'accesso alle autorità nazionali competenti, si ingerisca in modo particolarmente grave nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. inoltre, il fatto che la conservazione ed il successivo utilizzo dei dati avvengano senza che l'abbonato o l'utente registrato ne siano informati può ingenerare negli interessati la sensazione che la loro vita privata sia oggetto di costante sorveglianza."

[112] ibidem, punto 73

delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione in merito alla richiesta rivolta da un cittadino olandese all'amministrazione comunale della città di Amsterdam, di informare lo stesso circa l'identità delle persone alle quali l'amministrazione comunale aveva trasmesso nei due anni precedenti informazioni che lo riguardavano, nonché il contenuto dei dati comunicati.[113]

La CGUE ha dichiarato che il diritto al rispetto della vita privata implica che la persona interessata possa assicurarsi che i suoi dati personali siano trattati in modo corretto e lecito, ossia che i dati di base che la riguardano siano corretti e vengano inviati a destinatari autorizzati. La CGUE ha fatto riferimento al preambolo della direttiva sulla protezione dei dati, il quale afferma che gli interessati devono godere del diritto di accesso ai propri dati personali per poter verificare la loro esattezza.

Vi sono anche casi in cui l'aggiornamento dei dati archiviati è proibito per legge, perché la finalità della conservazione dei dati è principalmente quella di documentare eventi come uno «scatto storico», si pensi ad esempio alle cartelle cliniche, e altri casi in cui il controllo regolare dell'esattezza dei dati, fra cui l'aggiornamento, costituisce una necessità assoluta a causa del potenziale danno per l'interessato qualora i dati dovessero rimanere inesatti.

In relazione al principio della limitazione della conservazione, esso disciplina la cancellazione o l'anonimizzatine dei dati raccolti non appena questi non siano più necessari alle finalità per cui sono stati raccolti, infatti l'art 5 paragrafo 1, lettera e) del Regolamento

[113] Sentenza 7 Maggio 2009, College Van Burgemeester En Wethouders Van Rotterdam/M.E.E. Rijkeboer, C-553/07, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62007CA0553 (22 giungo 2022) , punti 23-29: *con lettera del 26 ottobre 2005, il sig. rijkeboer ha chiesto al college di informarlo di tutti i casi in cui informazioni che lo riguardano, provenienti dall'amministrazione comunale, erano state comunicate a terzi nei due anni precedenti la sua richiesta. egli voleva conoscere l'identità di tali persone ed il contenuto delle informazioni loro trasmesse. il sig. Rijkeboer, che si era trasferito in un altro comune, voleva in particolare sapere a chi fosse stato comunicato il suo vecchio indirizzo. Con decisioni del 27 ottobre e 29 novembre 2005, il college ha accolto solo parzialmente tale richiesta comunicandogli, conformemente all'art. 103, n. 1, della Wet Gba, unicamente le informazioni relative all'anno precedente la sua richiesta. le comunicazioni di dati vengono registrate ai sensi del «Logisch Ontwerp Gba». si tratta di un sistema automatizzato, creato dal Ministerie Van Binnenlandse Zaken En Koninkrijkrelaties (ministero degli interni e delle relazioni all'interno del regno [dei paesi bassi]). dalla domanda di pronuncia pregiudiziale risulta che i dati richiesti dal sig. rijkeboer, anteriori all'anno precedente la sua richiesta, sono stati automaticamente cancellati, ciò che sarebbe conforme all'art. 110 della Wet Gba. il sig. Rijkeboer ha depositato un reclamo presso il college avverso il rifiuto di comunicargli informazioni sui destinatari a cui erano stati comunicati dati che lo riguardano anteriormente all'anno precedente la sua richiesta. dopo che tale reclamo era stato respinto con decisione del 13 febbraio 2006, il sig. Rijkeboer ha proposto un ricorso dinanzi al Rechtbank Rotterdam. tale giudice ha accolto il ricorso ritenendo la limitazione del diritto ad essere informato dei dati comunicati a destinatari all'anno precedente la richiesta, quale prevista all'art. 103, n. 1, della Wet Gba, non compatibile con l'art. 12 della direttiva. esso ha anche ritenuto non applicabili le eccezioni di cui all'art. 13 di tale direttiva. il college ha impugnato tale sentenza dinanzi al raad van state. tale giudice ha rilevato che l'art. 12 della direttiva, relativo al diritto di accesso ai dati, non stabilisce alcun termine per l'esercizio del diritto. esso ritiene, nutrendo però dubbi al riguardo, che tale articolo non vieti tuttavia necessariamente al legislatore nazionale di limitare nel tempo il diritto della persona interessata ad essere informata dei destinatari a cui vengono trasmessi suoi dati personali. alla luce di quanto sopra, il raad van state ha deciso di sospendere il procedimento e di sottoporre alla corte la seguente questione pregiudiziale: «se la limitazione, prevista dalla legge, della comunicazione dei dati all'anno precedente la relativa richiesta sia compatibile con l'art. 12, (...) lett. a), della [direttiva], eventualmente interpretato in combinato disposto con l'art. 6, n. 1, lett. e), della citata direttiva e con il principio di proporzionalità».*"

2016/679, dispone che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Caso emblematico in merito alla violazione del principio di limitazione della conservazione dei dati è stato S. *e Marper c. Regno Unito (cause riunite ricc. nn. 30562/04 e 30566/04 del 4 dicembre 2008)*[114] in cui la Corte Europea dei Diritti dell'Uomo è stata chiamata a valutare la compatibilità con l'art. 8 della Convenzione le modalità di conservazione di campioni e dati previste dal National DNA Database del Regno Unito, il quale ammette la conservazione illimitata di dati biologici anche di cittadini innocenti.

Nella causa *S. e Marper*, la Corte EDU ha stabilito che la conservazione per una durata indeterminata delle impronte digitali, dei campioni cellulari e dei profili di DNA dei due ricorrenti era sproporzionata e non necessaria in una società democratica, considerando che le azioni penali promosse contro entrambi i ricorrenti si erano concluse, rispettivamente, con l'assoluzione e il non luogo a procedere.

In relazione al principio della sicurezza dei dati, esso richiede che, nel trattare dati personali, siano messe in atto misure tecniche o organizzative adeguate a proteggere i dati da accesso, uso, modifica, divulgazione, perdita, distruzione o danno accidentali, non autorizzati o illegali.

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, prevede all'art 32[115] che, nell'attuazione di tali misure, il titolare del trattamento e il

[114] Sentenza 4 dicembre 2008, S. e Marper c. Regno Unito, cause riunite ricc. nn. 30562/04 e 30566/04, Corte Edu, in Biodiritto, Unverità di Trento, https://www.biodiritto.org/Biolaw-pedia/Giurisprudenza/Corte-Europea-dei-Diritti-dell-Uomo-S.-Marper-v.-UK-limite-alla-conservazione-dei-dati-genetici, (22 giugno 2022): due cittadini inglesi, accusati in due distinti processi per rapina e violenza sessuale, erano stati sottoposti al prelievo di materiale biologico, sulla base della legislazione inglese che prevedeva il prelievo coattivo di campioni di soggetti indagati, condannati o semplicemente sospettati per la commissione di un reato. i campioni prelevati e i profili genetici da essi estratti erano destinati a conservazione illimitata nel database nazionale e nonostante le ripetute richieste da parte dei ricorrenti, giudicati innocenti, non era avvenuta la cancellazione.

[115] Articolo 32, Regolamento (UE) 2016/679 , Sicurezza del trattamento (C83): *"1. Tenendo 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"*

responsabile del trattamento, tengano 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 e, a seconda delle circostanze specifiche di ciascun caso, e impone di adottare delle misure tecniche adeguate come, ad esempio, la pseudonimizzazione e la cifratura[116] dei dati personali.

L'art 25 del Regolamento (UE) 2016/679, rubricato "*Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita",* fa esplicito riferimento alla pseudonimizzazione come esempio di misura tecnica e organizzativa adeguata, che i titolari del trattamento dovrebbero mettere in atto per rispettare i principi di protezione dei dati e per integrare le necessarie garanzie[117] e l'adesione a un codice di condotta approvato o a un meccanismo di certificazione approvato può contribuire a dimostrare la conformità al requisito della sicurezza del trattamento e, in caso di violazione, il titolare del trattamento deve notificare, senza ingiustificato ritardo, all'autorità di controllo competente, la violazione che presenti un rischio per i diritti e le libertà delle persone fisiche[118]

Infine, il principio di responsabilizzazione richiede da parte dei titolari e dei responsabili del trattamento di adottare attivamente e in modo permanente misure finalizzate alla promozione e alla salvaguardia della protezione dei dati nelle attività di trattamento.

I titolari e i responsabili del trattamento sono responsabili della conformità alla normativa in materia di protezione dei dati nell'ambito delle operazioni di trattamento e dei rispettivi obblighi e devono essere in grado di dimostrare in qualsiasi momento agli interessati, al

---

[116] AA. VV., Manuale Sul Diritto Europeo In Materia Di Protezione Dei Dati, Edizione 2018 Op Cit. P. 50; A Pag. 147 "pseudonimizzare i dati significa sostituire con uno pseudonimo gli attributi, contenuti nei dati personali, che consentono di identificare l'interessato, e conservare tali attributi separatamente, sulla base di misure tecniche o organizzative. il processo di pseudonimizzazione non deve essere confuso con il processo di anonimizzazione, in cui viene spezzato ogni nesso che permette l'identificazione della persona; la cifratura, invece, è essenzialmente quel processo che rende un determinato dato incomprensibile, al fine di garantire la sua confidenzialità. i concetti alla base di questo processo sono l'informazione da proteggere, l'algoritmo di cifratura, il crittogramma (cypher-text) e un valore segreto definito chiave (key). la crittografia dovrebbe garantire che, senza conoscere la chiave, non si possa mai avere la possibilità di ottenere il messaggio in chiaro da cui proviene il crittogramma.

[117] Art 25 Del Regolamento (UE) 2016/679: " 1. tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati. 2.: "il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. in particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. 3. un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo."

[118] Regolamento (UE) 2016/679, articolo 33, paragrafo 1.

pubblico in generale e alle autorità di controllo che essi operano in conformità delle disposizioni sulla protezione dei dati.

I responsabili del trattamento devono rispettare alcuni obblighi strettamente legati alla responsabilità quali, ad esempio, tenere un registro delle attività di trattamento, in determinate situazioni, designare il responsabile della protezione dei dati, che è coinvolto in tutte le questioni connesse alla protezione dei dati personali, svolgere valutazioni d'impatto sulla protezione dei dati per i tipi di trattamento che presentano un rischio elevato per i diritti e le libertà delle persone fisiche, garantire la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita, prevedere modalità e procedure per l'esercizio dei diritti degli interessati, aderire a codici di condotta approvati o a meccanismi di certificazione[119].

In relazione al parametro legale, il legislatore europeo ha individuato una gamma di basi giuridiche dalle quali far dipende la liceità del trattamento agli artt. 6 e 9 reg. 2016/679[120]e, infatti, affinché i dati personali siano «trattati in modo lecito, corretto e trasparente», il trattamento deve essere conforme a uno dei legittimi presupposti per il trattamento dei dati, elencati all'articolo 6, per i dati personali non sensibili, e all'articolo 9, per le categorie particolari di dati (o dati sensibilissimi).

L'art. 6 reg. 2016/679 delinea un quadro ampio ed eterogeneo di basi giuridiche del trattamento che riguarda: il consenso dell'interessato per una o più specifiche finalità; il carattere necessario del trattamento all'esecuzione di un contratto di cui sia parte l'interessato o allo svolgimento della fase precontrattuale; il carattere necessario del trattamento all'adempimento di un obbligo legale imposto al titolare dal diritto dell'Unione europea o dal diritto dello Stato membro cui egli è assoggettato; il carattere necessario del trattamento alla salvaguardia degli interessi vitali dell'interessato o di altra persona fisica; il carattere necessario del trattamento all'assolvimento di un compito di interesse pubblico o connesso all'espletamento di una pubblica funzione di cui è investito il titolare sulla base del diritto dell'Unione europea o del diritto dello Stato membro cui egli è assoggettato; il carattere necessario del trattamento al perseguimento del legittimo interesse del titolare o di terzi, sempre che non prevalgano gli interessi, i diritti e le libertà fondamentali dell'interessato collegati alla protezione dei dati personali, specie se quest'ultimo sia un minore[121].

[119] Regolamento (UE) 2016/679, articoli 25, 30, 35, 37–39. Convenzione n. 108 modernizzata, articolo 10, paragrafo 2.e 3. articoli 12 e 24. E 40 e 42.

[120] Piraino, F. Il Regolamento Generale Sulla Protezione Dei Dati Personali E I Diritti Dell'interessato. Le Nuove Leggi Civili Commentate, 40(2), Wolters Kluwer S.P.A , 2017, pag 386 e ss

[121] Piraino, F, op. cit. p.60

Per quanto riguarda il consenso dell'interessato, esso è definito dall'art 4 n. 11 Regolamento (UE) 2016/679 che lo identifica come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento, esso deve essere basato su un apprezzamento e sulla comprensione dei fatti e delle implicazioni dell'azione della persona interessata per il consenso al trattamento e, pertanto, l'interessato deve ricevere, in modo chiaro e comprensibile, informazioni precise e complete su tutti gli aspetti rilevanti come la natura dei dati trattati, le finalità del trattamento, i destinatari di eventuali trasferimenti e i diritti dell'interessato.

Affinché il consenso sia prestato con cognizione di causa, le persone devono altresì essere consapevoli delle conseguenze del mancato consenso al trattamento e, per essere valido, deve essere anche specifico alla finalità del trattamento e manifestato in maniera inequivocabile e, pertanto, non dovrebbero sussistere dubbi ragionevoli in merito al fatto che l'interessato volesse esprimere il proprio consenso al trattamento dei propri dati: l'inerzia dell'interessato non indicherà mai un consenso inequivocabile.[122]

Il Regolamento (UE) 2016/679 prevede, inoltre, una protezione specifica per i minori all'Articolo 8 in relazione ai servizi della società dell'informazione, in quanto tali soggetti «possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali[123].

L'interessato deve essere informato del diritto di revocare il consenso prima di prestarlo e può esercitare tale diritto a sua discrezione, senza alcun obbligo di motivazione e senza conseguenze negative salvo la cessazione di eventuali benefici derivanti dall'uso dei dati precedentemente concordato.

L'articolo 6, paragrafo 1, lettera b) e c), del GDPR fornisce due ulteriori basi per la liceità del trattamento dei dati personali: il primo nel caso in cui ciò necessario all'esecuzione di un contratto di cui l'interessato è parte, in cui devono essere ricompresi anche rapporti

[122] AA. VV., Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018, Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, 2018 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_it.pdf , (01 luglio 2022)

[123] Art 8, Regolamento (UE) 2016/679, *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (c38) :* 1. qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. gli stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13anni. 2. il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. 3. il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore

precontrattuali, il secondo nel caso in cui il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento e, l'obbligo legale può trovare la sua origine nel diritto dell'Unione o in quello dello Stato membro.

L'articolo 6, paragrafo 1, lettera d), del GDPR, dispone che il trattamento di dati personali è lecito se «è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica» mentre alla lettera e), del Regolamento si stabilisce che i dati personali possono essere trattati lecitamente se «è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

La lettera f) dell'articolo in esame stabilisce che i dati personali possono essere trattati in modo lecito se ciò «è *necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela [...]*».

Tuttavia, l'esistenza di un interesse legittimo deve essere attentamente valutata caso per caso e qualora venga individuato l'interesse legittimo del titolare del trattamento, esso dovrà essere bilanciato con diritti e le libertà fondamentali della persona interessata.

Nel caso *Valsts Policijas Rīgas Regiona pārvaldes Kārtības Policijas pārvaldE,* la CGUE ha stabilito tre condizioni cumulative che devono essere soddisfatte affinché il trattamento dei dati personali sia lecito sulla base del motivo del «legittimo interesse»: in primo luogo, il terzo a cui vengono comunicati i dati deve perseguire un interesse legittimo; in secondo luogo, il trattamento dei dati personali deve essere necessario per il perseguimento dell'interesse legittimo; in terzo luogo, i diritti e le libertà fondamentali dell'interessato non devono prevalere sugli interessi legittimi del titolare del trattamento o del terzo. La ponderazione degli interessi deve essere fatta caso per caso, tenendo conto di fattori quali la gravità della violazione dei diritti dell'interessato o addirittura, in determinate circostanze, l'età della persona[124].

l'art. 6, parr. 2 e 3, reg. 2016/679 consente, agli Stati membri di mantenere o di introdurre disposizioni più specifiche relative ai trattamenti di cui alle lett. c) ed e) volte a individuarne con maggiore precisione i requisiti specifici e le ulteriori misure destinate a integrare i requisiti della liceità e della correttezza e spetta sia al diritto dell'Unione europea che ai diritti nazionali individuare le basi giuridiche dei trattamenti legati al perseguimento di interessi generali, specificandone pure la finalità, con l'ulteriore possibilità di dettare disposizioni di dettaglio volte all'adeguamento della disciplina contenuta nel regolamento sul versante in relazione a la

[124] Sentenza 4 maggio 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA «Rīgas satiksme», C-13/16, https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62016CJ0013, (24 giugno 2022)

liceità del trattamento, della tipologia di dati da trattare, dell'individuazione della categoria degli interessati, dell'individuazione dei soggetti cui i dati possono essere comunicati e della finalità della comunicazione; delle limitazioni della finalità, dei periodi di conservazione dei dati e delle operazioni e procedure del trattamento, etc[125].

L'art 9 reg. 2016/679 disciplina il trattamento inerente a categorie particolari di dati personali tra cui sono ricompresi i dati inerenti all'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della stessa.[126].

In linea di principio il trattamento dei dati sensibili è vietato ma lo stesso art. 9 al paragrafo 2, contiene un elenco esaustivo di deroghe che costituiscono motivi legittimi per il trattamento di dati sensibili:

• il consenso dell'interessato al trattamento dei dati: tale consenso deve essere esplicito e l'Unione o lo Stato membro possono disporre che il divieto di trattamento per le categorie particolari non possa essere revocato dall'interessato.

• il trattamento è effettuato da un organismo che non persegue scopi di lucro e riveste carattere politico, filosofico, religioso o sindacale nel corso di attività legittime e riguarda solo i suoi (ex) membri o persone che hanno contatti regolari con esso per tali scopi;

• il trattamento riguarda dati personali esplicitamente resi pubblici dall'interessato;

• il trattamento è necessario:

a) per adempiere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato nel contesto dell'occupazione, della sicurezza sociale e della protezione sociale;

b) per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica (quando l'interessato non può prestare il proprio consenso);

c) per rivendicare, esercitare o difendere un diritto per via giudiziaria o quando i tribunali esercitano le loro funzioni giurisdizionali;

d) per finalità di medicina preventiva o di medicina del lavoro: per la «valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale

[125] Piraino, F, op. cit. p.60

[126] Art 9 Reg. 2016/679: 2. *Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (…)4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. (C8, C10, C41, C45, C53)*

ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità»;

e) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

f) per motivi di interesse pubblico nel settore della sanità pubblica;

g) per motivi di interesse pubblico rilevante.

Per trattare tali categorie particolari di dati un rapporto contrattuale con l'interessato non è visto come fondamento giuridico per il trattamento legittimo degli stessi, salvo il caso in cui il trattamento sia effettuato da un professionista della sanità vincolato dal segreto professionale.

Ai fini della presente analisi occorre porre l'attenzione sull'art 9 del Regolamento in esame, il quale fra i dati sensibili annovera anche quelli sanitari e afferma che gli essi in linea di principio non potrebbero essere trattati se non nei modi e nelle forme previste dal Regolamento UE 679/2016.

Tuttavia, il nuovo Regolamento ha introdotto numerose e sostanziali novità in materia di protezione dei dati personali, superando sotto diversi profili la Direttiva 95/46/CE e il D.lgs. 196/2003 (c.d. Codice privacy italiano).

Tra le novità di maggiore interesse vi è l'art. 6 REG. UE 679/2016, il quale non riconosce più un ruolo centrale al consenso dell'interessato[127] che ad oggi figura solo come una delle possibili alternative su cui il trattamento di dati personali può essere fondato.

[127] L'art. 26 (D.lgs. 30 giugno 2003, n. 196), disponeva che: "i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. 2. il garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare. 3. il comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del garante; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria. b-bis) dei dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis. 4. i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un

Nel caso in cui non vengano rispettate le prescrizioni e i principi sopra descritti il Regolamento europeo per la protezione dei dati personali (GDPR) e le normative nazionali prevedendo una serie di strumenti volti alla tutela dell'interessato in caso di trattamento illecito dei dati.

Gli strumenti di tutela azionabili dall'interessato in caso di trattamento illecito dei dati personali verranno analizzati nel prossimo capitolo nella sezione inerente al trattamento illecito dei dati sanitari.

prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. si applica la disposizione di cui all'articolo 82, comma 2; c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111. 5. i dati idonei a rivelare lo stato di salute non possono essere diffusi.

Capitolo 3

Intelligenza artificiale e responsabilità civile: la responsabilità civile in caso di cooperazione tra intelligenza umana e artificiale in ambito medico-sanitario e l'utilizzo dei big data nella lotta alla pandemia da covid-19

3.1 Applicazioni I.A. in campo medico e differenza con la robotica.

Prima di analizzare l'applicazione dell'Intelligenza Artificiale nel settore medico è indispensabile chiarire la differenza tra quest'ultima e la robotica poiché spesso questi due termini vengono impropriamente utilizzati come sinonimi.

Con il termine robotica si è soliti indicare quel settore dell'ingegneria che ha per oggetto lo studio e la realizzazione dei robot e che sviluppa metodi grazie ai quali i robot possono eseguire compiti specifici riproducendo in modo automatico il lavoro umano[128].

Un sistema robotico presenta quindi una struttura meccanica piuttosto complessa e articolata, basata su specifici modelli matematici tra cui, i principali approcci utilizzati per la programmazione di un robot, possiamo ricordare:

a) *Teaching-by-showing*: dove il robot viene guidato lungo un percorso e, grazie ad appositi sensori, apprende le posizioni raggiunte e, una volta programmato sarà in grado di ripetere autonomamente il movimento insegnato[129] con apprendimento sul campo.
b) *Robot-oriented*: dove il robot per l'apprendimento si basa su linguaggi di programmazione con strutture dati complesse, numerose variabili e diverse routine[130];
c) *Object-oriented*: dove il robot per l'apprendimento si basa su un linguaggio di programmazione orientato sugli oggetti e l'interazione attraverso uno scambio di messaggi.[131]

[128] Così, De Luca A, Monaco S, In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia Italiana - V Appendice (1994), Robotica, https://www.treccani.it/enciclopedia/robotica_%28Enciclopedia-Italiana%29/#:~:text=La%20r.,nei%20territori%20slavi%20dell'Impero. (20 luglio 2022)
[129] Rocco P., Fondamenti di robotica – Programmazione del moto, Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria, https://rocco.faculty.polimi.it/FDR/Programmazione%20del%20moto.pdf (20 luglio 2022) cfr Teaching one-to-one, in Cambridge University Press and Cambridge Assessment English, https://www.cambridgeenglish.org/Images/525581-teaching-one-to-one-part-1.pdf, (20 luglio 2022)
[130] Bock T., Linner T., Robot-Oriented Design, Design and Management Tools for the Deployment of Automation and Robotics in Construction, in Cambridge University Press, maggio 2015, p. 1-283
[131] ibidem

Uno dei primi campi di applicazione della robotica in medicina si è avuto nel settore della chirurgia, la quale, come la medicina in generale, è strettamente legata allo sviluppo tecnologico[132].

Viceversa, l'intelligenza artificiale è una disciplina appartenente all'informatica che si sostanzia nell'elaborazione di metodologie e tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, agli occhi di un osservatore comune sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana.

Come anticipato, le Intelligenze Artificiali sono programmate secondo tre tipologie principali di apprendimento che si distinguono nell'apprendimento per rinforzo, l'apprendimento non supervisionato e l'apprendimento supervisionato e i campi di applicazione dell'intelligenza artificiale sono sempre più numerosi e vanno dal mondo industriale all'ambito medico, passando per la sicurezza, il marketing e la comunicazione, il business management, la sicurezza informatica ecc.

Da ciò discende che non tutti i robot sono integrati dall'Intelligenza Artificiale, che replica le funzioni della mente umana, ma grazie alla robotica l'I.A. è in grado di migliorare i robot e aumentarne le capacità e le potenzialità come ad esempio il robot "Star" (Smart Tissue Autonomous Robot), progettato dalla Johns Hopkins University e specializzato nell'anastomosi dei tessuti molli, il quale attraverso un sistema a guida visiva e sofisticati algoritmi di intelligenza artificiale che ha eseguito un'intera operazione chirurgica senza l'assistenza umana.[133]

---

[132] il primo sistema di chirurgia robotica davvero utilizzabile in sala operatoria è del 1999, quando la Intuitive Surgical Inc., introdusse sul mercato il primo e unico sistema chirurgico robotizzato, denominato Da Vinci, in onore dello scienziato italiano.

[133] Saidi H., Opfermann M.K., Wei S. E Altri, Chirurgia Laparoscopica Robotica Autonoma Per Anastomosi Intestinale, In Science Robotics" Del 26 Gennaio 2022 Vol 7 , Edizione 62, https://www.science.org/doi/abs/10.1126/scirobotics.abj2908, (22 luglio 2022) i quali hanno affermato che: " la chirurgia robotica autonoma ha il potenziale per fornire efficacia, sicurezza e coerenza indipendentemente dall'abilità e dall'esperienza del singolo chirurgo. l'anastomosi autonoma è un compito di chirurgia dei tessuti molli impegnativo perché richiede intricate tecniche di imaging, tracciamento dei tessuti e pianificazione chirurgica, nonché un'esecuzione precisa tramite strategie di controllo altamente adattabili, spesso in ambienti non strutturati e deformabili. in ambito laparoscopico, tali interventi chirurgici sono ancora più impegnativi a causa della necessità di un'elevata manovrabilità e ripetibilità in condizioni di movimento e di vista. qui descriviamo una strategia autonoma potenziata per la chirurgia laparoscopica dei tessuti molli e dimostriamo l'anastomosi robotica dell'intestino tenue laparoscopica nei tessuti intestinali fantasma e in vivo. questa strategia autonoma avanzata consente all'operatore di selezionare tra piani chirurgici generati autonomamente e il robot esegue un'ampia gamma di attività in modo indipendente. utilizziamo quindi la nostra strategia autonoma avanzata per eseguire la chirurgia laparoscopica robotica autonoma in vivo per l'anastomosi intestinale su modelli suini per un periodo di sopravvivenza di 1 settimana. abbiamo confrontato i criteri di qualità dell'anastomosi, comprese le correzioni del posizionamento dell'ago, la spaziatura della sutura, la dimensione del morso della sutura, il tempo di completamento, la pervietà del lume e la pressione di perdita del sistema autonomo sviluppato, la chirurgia laparoscopica manuale e la chirurgia assistita da robot (ras). i dati provenienti da un modello fantasma indicano che il nostro sistema supera in termini di coerenza e accuratezza la tecnica manuale dei chirurghi esperti e la tecnica ras. questo è stato replicato anche nel modello in vivo."

Effettuata questa breve precisazione occorrerà ora verificare i campi medici in cui l'I. A. è stata impiegata e mettere in rilievo le criticità dal punto di vista giuridico.

In ambito diagnostico, i vari sistemi di Intelligenza Artificiale (IA) si stanno sviluppando repentinamente e numerosi studi hanno dimostrato l'utilità di questa tecnologia quale supporto dei medici e agli specialisti nel formulare diagnosi mediche.

Tuttavia, non potendo analizzare tutto l'ambito medico, la nostra ricerca si soffermerà ad analizzare in modo rapido l'applicazione dell'intelligenza Artificiale nel settore della radiologia, e in particolare lo studio sul sistema di deep learning CheXNeXt e il Deep Learning Assisted Detecting (DLAD), nel settore dell'oncologia ci si soffermerà ad analizzare l'applicazione dell'I.A nella lotta e prevenzione dei tumori al seno e il sistema di intelligenza artificiale *TRACE4BDensity* e ,infine, si analizzerà il settore della cardiologia.

3.1.1 L'intelligenza artificiale applicata nel settore della radiologia

Nel settore della Radiologia c'è una grande richiesta di sistemi che implementino tecniche di Intelligenza Artificiale poiché il carico di lavoro dei radiologi è in forte aumento e, inoltre, è cresciuto in modo significativo il numero delle immagini da interpretare per il singolo esame, producendo l'effetto di una refertazione sempre più complessa.

In questo scenario, le nuove tecniche di AI applicate alle principali attività radiologiche quali la scelta dell'esame, l'ottimizzazione dell'esame, il supporto alla diagnosi e alla refertazione e la guida nelle applicazioni interventistiche, qualora si dimostrino affidabili ed efficaci, potrebbero migliorare l'efficienza del radiologo, consentendogli di operare al meglio e in maggiore sicurezza.

Storicamente, le principali aree radiologiche nelle quali sono state applicate e utilizzate le tecniche d'intelligenza artificiale sono quattro e per ciascuna di esse sono stati sviluppati dei sistemi dedicati, i quali possono essere così elencati:

- **Computer-aided detection (cd. CADe**): che si sostanziano in sistemi di localizzazione delle regioni sospette in vari distretti anatomici quali, ad esempio, la mammella, il fegato, la prostata e il torace e le analizzano al fine di individuare delle specifiche manifestazioni di patologia.

In tali sistemi il data-processing utilizzato si compone di varie fasi: il pre-processing, la segmentazione, l'individuazione delle regioni d'interesse, l'estrazione di indicatori quantitativi

(cd. features), la loro analisi e la classificazione. Fino ad oggi sono stati utilizzati principalmente algoritmi di Machine Learning di tipo classico[134].

- **Computer-aided diagnosis (CADx):** che si sostanziano in sistemi per la diagnosi in grado di capire la natura benigna o maligna di un reperto radiologico, indicando nel paziente la presenza di una patologia; anche tale sistema si caratterizza per la presenza di varie fasi analogamente al CADe[135].

Tuttavia, i sistemi CADe e CADx, impiegati nel rilevamento e la diagnosi del cancro del polmone, hanno rilevato che i due sistemi devono operare separatamente in quanto: i sistemi CADe non rilevano le caratteristiche radiologiche dei tumori e i sistemi CADx non rilevano

---

[134] Firmino M, Giovani A., Morais H, ed altri- Computer-aided detection (CADe) and diagnosis (CADx) system for lung cancer with likelihood of malignancy, in BioMedical Engineering OnLine, https://biomedical-engineering-online.biomedcentral.com/articles/10.1186/s12938-015-0120-7 , (25 luglio 2022): "*a cade system for detection of pulmonary nodules usually consists of four main stages: segmentation of the lungs, detection of the candidate nodules, characteristics analysis and elimination of false positives. the segmentation of lung images serves to separate the region in study from other organs and tissues in radiological images. with the segmented images, a search is performed aiming to find abnormal structures present in the lungs, which may be nodules. then, the characteristics of the possible detected nodules are extracted. the main characteristics that are commonly used for detection of pulmonary nodules are: intensity values of pixels and morphological and texture analysis. finally, the candidate nodules are classified into nodules or non-nodules by the classifier. this final stage is very important, because it determines the final performance by removing non-nodules and maintaining real nodules*". **tradotto letteralmente** : ***"un sistema cade per il rilevamento dei noduli polmonari è solitamente costituito da quattro fasi principali: segmentazione dei polmoni, rilevamento dei noduli candidati, analisi delle caratteristiche ed eliminazione dei falsi positivi. la segmentazione delle immagini polmonari serve a separare la regione in studio da altri organi e tessuti nelle immagini radiologiche. con le immagini segmentate, viene eseguita una ricerca mirata a trovare strutture anormali presenti nei polmoni, che possono essere noduli. si estraggono quindi le caratteristiche dei possibili noduli rilevati. le principali caratteristiche comunemente utilizzate per la rilevazione dei noduli polmonari sono: i valori di intensità dei pixel e l'analisi morfologica e di tessitura. infine, i noduli candidati sono classificati in noduli o non noduli dal classificatore. questa fase finale è molto importante, perché determina la performance finale rimuovendo i non noduli e mantenendo i noduli reali***."

[135] Così Firmino M. e altri, op cit p.69 "*In general, CADx systems extract the characteristics of the images and use a classifier to measure the malignancy. Usually CADx systems for diagnosis of lung cancer are assessed through the ROC curve, more precisely through the area under the ROC curve (Az). A CADx system has been proposed by Shah et al. where they selected 31 characteristics and used logistic regression as classifier, reaching a value of Az 0.92 in distinguishing between 19 malignant nodules and 16 benign nodules, all solitary nodules. Way et al. developed a CADx system that used morphological characteristics, intensity values and surface characteristics. Using the LDC classifier (Linear Discriminant Classifier), Way et al. obtained a Az of 0.857 on the classification of 124 malignant nodules and 132 benign nodules in 152 patients. Suzuki et al. developed a neural network named MTANN to distinguish between benign and malignant nodules. Suzuki et al. reached a value of 0.88, being tested with 76 malignant nodules and 413 benign nodules. Lee et al developed a supervised learning system that made use of genetic algorithms and Linear Discriminant Analysis (LDA) for the analysis of 216 characteristics of the images and clinical history of patients. They obtained a Az of 0.889 when evaluated 62 malignant nodules and 63 benign nodules, all solitary nodules. Orozco et al. used 11 characteristics calculated from the wavelet transform and SVM as classifier. They obtained a Az of 0.805 being tested with 23 malignant nodules and 22 non-nodules*. **Tradotto letteralmente:** "***in generale, i sistemi cadx estraggono le caratteristiche delle immagini e utilizzano un classificatore per misurare la malignità. di solito lo sono i sistemi cadx per la diagnosi del cancro del polmone valutata attraverso la curva roc, più precisamente attraverso l'area sotto la curva roc (az). un sistema cadx è stato proposto da shah et al., dove hanno selezionato 31 caratteristiche e utilizzato la regressione logistica come classificatore, raggiungendo un valore di az 0,92 nel distinguere tra 19 noduli maligni e 16 noduli benigni, tutti noduli solitari. way et al. ha sviluppato un sistema cadx che utilizzava caratteristiche morfologiche, valori di intensità e caratteristiche della superficie. utilizzando il classificatore ldc (classificatore discriminante lineare), way et al. ha ottenuto un az di 0,857 sulla classificazione di 124 maligni noduli e 132 noduli benigni in 152 pazienti. suzuki et al. sviluppato un neurale rete denominata mtann per distinguere tra noduli benigni e maligni. suzuki et al. ha raggiunto un valore di 0,88, testato con 76 noduli maligni e 413 benigni noduli. lee et al hanno sviluppato un sistema di apprendimento supervisionato che ha fatto uso della genetica algoritmi e analisi discriminante lineare (lda) per l'analisi di 216 caratteristiche delle immagini e della storia clinica dei pazienti. hanno ottenuto un az di 0,889 quando hanno valutato 62 noduli maligni e 63 noduli benigni, tutti noduli solitari. orozzo et al. utilizzato 11 caratteristiche calcolate dalla trasformata wavelet e svm come classificatore. hanno ottenuto un az di 0,805 testando con 23 noduli maligni e 22 non noduli***."

noduli; inoltre, questi sistemi non sono ancora ampiamente utilizzati in ambito clinico poiché non hanno raggiunto buoni livelli di autonomia.[136]

- **Clinical decision support (CDS):** che si sostanziano in strumenti di supporto alla decisione clinica del medico; tali dispositivi sono idonei ad aiutare a seguire le linee guida e le migliori pratiche radiologiche da applicare al caso concreto, evitando così indagini inappropriate o inutili.

Il CDS fornisce a medici, pazienti o operatori sanitari conoscenze cliniche e informazioni specifiche al fine di aiutare il personale sanitario a prendere decisioni che migliorino la cura del paziente; inoltre, le informazioni sono abbinate ad una base di conoscenze cliniche e valutazioni specifiche del paziente stesso che permettono di formulare e comunicare le raccomandazioni in modo efficace e nei momenti più appropriati durante l'intero percorso clinico.[137]

---

[136] Ibidem: "*cade and cadx systems for lung cancer have been important areas of research in recent decades. however, these research areas are being worked on separately. according to fraioli et al. one of the main problems of cade systems for pulmonary nodules is that they detect the nodules but do not characterize them. thus, computer systems that only detect nodules are not enough for clinical application. currently, cade systems do not present the radiological characteristics of the tumor, resulting in lack of information for radiologists, and cadx systems do not detect tumor and do not have good levels of automation. this way, the new cad should incorporate into a single software a system for detection (cade) as well as diagnosis (cadx).* tradotto letterlamente: ***" i sistemi cade e cadx per il cancro del polmone sono stati importanti aree di ricerca in ultimi decenni. tuttavia, queste aree di ricerca vengono elaborate separatamente. secondo fraioli et al. uno dei problemi principali dei sistemi cade per la polmonite noduli è che rilevano i noduli ma non li caratterizzano. quindi,i sistemi che rilevano solo i noduli non sono sufficienti per l'applicazione clinica. attualmente, i sistemi cade non presentano le caratteristiche radiologiche del tumore, risultando mancanza di informazioni per i radiologi e i sistemi cadx non rilevano il tumore e non lo fanno avere buoni livelli di automazione. in questo modo, il nuovo cad dovrebbe incorporare in a software unico un sistema di rilevamento (cade) e diagnosi (cadx*) .

[137] Eichner J., e altri, "Challenges and Barriers to Clinical Decision Support (CDS) Design and Implementation Experienced in the Agency for Healthcare Research and Quality CDS Demonstrations", AHRQ National Resource Center for Health Information Technology, anno 2010, https://digital.ahrq.gov/sites/default/files/docs/page/CDS_challenges_and_barriers.pdf, (26 luglio 2022) nel quale si specifica che: "*to improve the quality of medical care in the united states, efforts are being made to increase the practice of evidence-based medicine through the use of clinical decision support (cds) systems. cds provides clinicians, patients, or caregivers with clinical knowledge and patientspecific information to help them make decisions that enhance patient care. the patient's information is matched to a clinical knowledge base, and patient-specific assessments or recommendations are then communicated effectively at appropriate times during patient care. some cds interventions include forms and templates for entering and documenting patient information, and alerts, reminders, and order sets for providing suggestions and other support. although cds interventions can be designed to be used by clinicians, patients, and informal caregivers, this report focuses on the use of cds interventions by clinicians to improve their clinical decisionmaking process. in addition, while cds interventions can be both paper and computer based, their application in the following projects is limited to electronic cds because of its greater capability for decision support. the use of cds systems offers many potential benefits. importantly, cds interventions can increase adherence to evidence-based medical knowledge and can reduce unnecessary variation in clinical practice. the process for development and implementation of cds systems can establish a standard knowledge structure that aligns with written evidence-based guidelines published by medical specialty societies or federal task forces, such as the u.s. preventive services task force (uspstf). cds systems can also assist with information management to support clinicians' decisionmaking abilities, reduce their mental workload, and improve clinical workflows.3 when well designed and implemented, cds systems have the potential to improve health care quality, and also to increase efficiency and reduce health care cost"* **. tradotto letteralmente**: "***per migliorare la qualità dell'assistenza medica negli stati uniti, si stanno compiendo sforzi per aumentare la pratica della medicina basata sull'evidenza attraverso l'uso del supporto alle decisioni cliniche (cds) sistemi. cds fornisce a medici, pazienti o operatori sanitari conoscenze cliniche e informazioni specifiche del paziente per aiutarli a prendere decisioni che migliorano la cura del paziente. le informazioni sono abbinate a una base di conoscenze cliniche e valutazioni specifiche del paziente o le raccomandazioni vengono quindi comunicate in modo efficace nei momenti appropriati durante la cura del paziente. alcuni interventi cds includono moduli e modelli per l'inserimento e la documentazione del paziente informazioni e avvisi, promemoria e set di ordini per fornire suggerimenti e altro supporto. sebbene gli interventi cds possano essere progettati per essere utilizzati da medici, pazienti e informali caregiver, questo rapporto si concentra sull'uso degli interventi cds da parte dei medici per migliorare il loro***

Tale strumento è utilizzato soprattutto negli Stati Uniti dove si stanno compiendo numerosi sforzi per aumentare la pratica della medicina basata sull'evidenza attraverso l'uso del supporto alle decisioni cliniche (CDS) sistemi.

- **Quantitative analysis tools**: che si sostanziano in strumenti di analisi che sono in grado di fornire differenti tipologie di features, grazie ai quali è possibile descrivere e identificare un reperto radiologico: lunghezza, forma, volume, intensità dei pixel ecc.

L'applicazione delle nuove reti neurali di *Deep Learning* ha rinnovato l'interesse verso questi strumenti che, in precedenza, erano poco utilizzati in quanto segnalavano un numero elevato di falsi positivi ma è stato dimostrato che i sistemi di Intelligenza Artificiale riescono ad essere più precisi nella diagnosi di alcuni radiologi che utilizzano per il loro lavoro il sistema di riconoscimento visuale per pattern[138]; infatti, quest'ultimi sono inevitabilmente soggetti a possibili pregiudizi, tra cui, ad esempio, la cosiddetta cecità attentiva (*inattentional blindness),* per la quale i soggetti focalizzati su specifici aspetti possono trascurare dati inaspettati anche se perfettamente visibili.

Su tale aspetto, Trafton Drew, un ricercatore presso la Harvard Medical School e il suo collaboratore Jeremy Wolfe, hanno applicato l'esperimento del gorilla invisibile[139] ad un gruppo di radiologi, i quali sono stati chiamati ad effettuare una diagnosi su una radiografia in cui lo stesso Trafton aveva nascosto l'immagine di un gorilla.

Nello Studio di Drew e Wolfe è stato dimostrato che l'83% dei radiologi non ha visto l'immagine del gorilla nelle radiografie che stava analizzando e questo perché i loro cervelli

processo decisionale clinico. inoltre, mentre gli interventi dei cds possono essere sia cartacei che computer based, la loro applicazione nei seguenti progetti è limitata ai cds elettronici perché della sua maggiore capacità di supporto alle decisioni. l'uso dei sistemi cds offre molti potenziali vantaggi. è importante sottolineare che gli interventi cds possono aumentare l'aderenza alle conoscenze mediche basate sull'evidenza e può ridurre le variazioni non necessarie nella pratica clinica. il processo di sviluppo e implementazione dei sistemi cds can stabilire una struttura di conoscenza standard che si allinea alle linee guida scritte basate sull'evidenza pubblicato da società di specialità mediche o task force federali, come la us preventive ask force dei servizi (uspstf). i sistemi cds possono anche aiutare con la gestione delle informazioni supportare le capacità decisionali dei medici, ridurre il loro carico di lavoro mentale e migliorare la clinica nei flussi di lavoro. se ben progettati e implementati, i sistemi cds hanno il potenziale per migliorare qualità dell'assistenza sanitaria, e anche per aumentare l'efficienza e ridurre i costi dell'assistenza sanitaria"

[138] Malizia A, Pattern Recognition Tecniche E Applicazion, in APPLICAZIONI- MONDO DIGITALE Vol n.2, giugno 2006, http://archivio-mondodigitale.aicanet.net/Rivista/06_numero_3/Malizia_p._40-50.pdf, (27 luglio 2022): Il pattern consiste nel riconoscimento automatico di oggetti (pattern) e la loro descrizione e classificazione.

[139] Chabris C e Simons D, Il gorilla invisibile. E altri modi in cui le nostre intenzioni ci ingannano, Il Sole 24 Ore, 2012 pp.1-332 L'esperimento È Stato Ideato Da Nel 1999 E I Due Psicologi Hanno Sottoposto Alcuni Soggetti Alla Visione Di Un Breve Filmato Nel Quale Un Gruppo Di Persone Giocava A Basket E Veniva Chiesto Loro Di Seguire Attentamente La Palla E Contare Il Numero Dei Passaggi Tra I Giocatori. Durante Il Filmato, Però Una Persona Travestita Da Gorilla Attraversava Il Campo Da Gioco, Si Fermava Tra I Giocatori, Salutava E Poi Spariva Dalla Parte Opposta. L'esperimento Mise In Luce Che Più Del 50% Degli Spettatori Non Si Erano Accorti Della Presenza Del Gorilla.

avevano inquadrato ciò che stavano facendo, ossia stavano cercando noduli cancerosi, non gorilla.[140]

Allo stesso esperimento è stato sottoposto CheXNeXt, un algoritmo di deep learning capace di rilevare contemporaneamente 14 malattie clinicamente importanti nelle radiografie del torace, da parte di alcuni studiosi, i cui risultati sono stati pubblica nell' articolo: "*Deep learning for chest radiograph diagnosis: a retrospective comparison of the CheXNeXt algorithm to practicing radiologists."*

In tale esperimento, è stato dimostrato che l'algoritmo di deep learning CheXNeXt ha ottenuto risultati simili ad un gruppo di 9 radiologi nella diagnostica di polmoniti, versamenti pleurici, masse polmonari, pneumotorace e noduli su semplici rx torace in antero-posteriore e, inoltre, a parità di efficacia diagnostica, il tempo medio di interpretazione delle 420 immagini del set di validazione è stato effettuato in 420 minuti dai radiologi umani e di soltanto 1,5 min. dall'algoritmo[141].

---

[140] Trafton D. e Wolfe J.: "Because even radiologists can lose a gorilla hiding in plain sight", in Heard on Morning Edition February 11, 20133, https://www.npr.org/sections/health-shots/2013/02/11/171409656/why-even-radiologists-can-miss-a-gorilla-hiding-in-plain-sight, (27 luglio 2022)

[141] Rajpurkar P. e altri, CheXNeXt: Deep learning for chest radiograph diagnosis, in Stanfor Dml Group, https://stanfordmlgroup.github.io/projects/chexnext/, (27 luglio 2022) : "*we developed chexnext, a convolutional neural network to concurrently detect the presence of 14 different pathologies, including pneumonia, pleural effusion, pulmonary masses, and nodules in frontal-view chest radiographs. chexnext was trained and internally validated on the chestx-ray dataset, with a held-out validation set consisting of 420 images, sampled to contain at least 50 cases of each of the original pathology labels. on this validation set, the majority vote of a panel of 3 board-certified cardiothoracic specialist radiologists served as reference standard. we compared chexnext's discriminative performance on the validation set to the performance of 9 radiologists using the area under the receiver operating characteristic curve (auc). the radiologists included 6 board-certified radiologists (average experience 12 years, range 4-28 years) and 3 senior radiology residents, from 3 academic institutions. we found that chexnext achieved radiologist-level performance on 11 pathologies and did not achieve radiologist-level performance on 3 pathologies. the radiologists achieved statistically significantly higher auc performance on cardiomegaly, emphysema, and hiatal hernia, with aucs of 0.888 (95% confidence interval [ci] 0.863-0.910), 0.911 (95% ci 0.866-0.947), and 0.985 (95% ci 0.974-0.991), respectively, whereas chexnext's aucs were 0.831 (95% ci 0.790-0.870), 0.704 (95% ci 0.567-0.833), and 0.851 (95% ci 0.785-0.909), respectively. chexnext performed better than radiologists in detecting atelectasis, with an auc of 0.862 (95% ci 0.825-0.895), statistically significantly higher than radiologists' auc of 0.808 (95% ci 0.777-0.838); there were no statistically significant differences in aucs for the other 10 pathologies. the average time to interpret the 420 images in the validation set was substantially longer for the radiologists (240 minutes) than for chexnext (1.5 minutes). the main limitations of our study are that neither chexnext nor the radiologists were permitted to use patient history or review prior examinations and that evaluation was limited to a dataset from a single institution";* **tradotto letteralmente**: "***abbiamo sviluppato chexnext, una rete neurale convoluzionale per rilevare contemporaneamente la presenza di 14 diverse patologie, tra cui polmonite, versamento pleurico, masse polmonari e noduli nelle radiografie del torace in vista frontale. chexnext è stato addestrato e convalidato internamente sul set di dati chestx-ray8, con un set di convalida sospeso composto da 420 immagini, campionate per contenere almeno 50 casi di ciascuna delle etichette originali della patologia. su questo set di validazione, il voto di maggioranza di un panel di 3 radiologi specialisti cardiotoracici certificati dal consiglio è servito come standard di riferimento. abbiamo confrontato le prestazioni discriminative di chexnext sul set di validazione con le prestazioni di 9 radiologi utilizzando l'area sotto la curva caratteristica operativa del ricevitore (auc). i radiologi includevano 6 radiologi certificati dal consiglio (esperienza media 12 anni, range 4-28 anni) e 3 specializzandi in radiologia senior, provenienti da 3 istituzioni accademiche. abbiamo scoperto che chexnext ha ottenuto prestazioni a livello di radiologo su 11 patologie e non ha ottenuto prestazioni a livello di radiologo su 3 patologie. i radiologi hanno ottenuto prestazioni auc statisticamente significativamente più elevate su cardiomegalia, enfisema ed ernia iatale, con auc di 0,888 (intervallo di confidenza 95% [ci] 0,863-0,910), 0,911 (ic 95% 0,866-0,947) e 0,985 (ic 95% 0,974-0,991), rispettivamente, mentre le auc di chexnext erano 0,831 (ic 95% 0,790-0,870), 0,704 (ic 95% 0,567-0,833) e 0,851 (ic 95% 0,785-0,909), rispettivamente. chexnext ha ottenuto risultati migliori rispetto ai radiologi nel rilevare l'atelettasia, con un'auc di 0,862 (ic 95% 0,825-0,895),***

I principali limiti emersi dallo studio sopra citato, attiene al fatto che né CheXNeXt né i radiologi potevano utilizzare l'anamnesi del paziente oppure rivedere gli esami precedenti e ciò ha comportato che la valutazione finale fosse limitata a un set di dati di una singola istituzione e, pertanto, non consentiva di dare un quadro clinico globale e adatto alle singole esigenze del caso in esame.

Sempre nel settore della Radiologia nel 2019 *il Journal of the American Medical Association* ha pubblicato un importante studio di alcuni ricercatori sudcoreani sull' applicazione di un sistema di intelligenza artificiale tipo Deep Learning Assisted Detecting (DLAD) alla diagnostica radiologica.

In questo lavoro, i ricercatori coreani hanno sviluppato un algoritmo diagnostico in grado di riconoscere 4 importanti gruppi di malattie respiratorie sulla base della semplice radiografia toracica standard ed hanno utilizzato, come base di addestramento del sistema di IA, 54221 radiografie normali di 47917 individui e 35613 immagini patologiche di 14102 individui[142].

L'algoritmo interpretativo, creato sulla base di questi dati, è stato quindi testato su 486 radiografie toraciche normali e 529 patologiche provenienti da 5 diversi centri diagnostici e, le medesime radiografie sono state anche interpretate da tre gruppi di medici di diversa specializzazione.

Lo studio ha dimostrato come l'algoritmo diagnostico del sistema di intelligenza artificiale DLAD è stato più accurato nella diagnosi rispetto a tutti i gruppi medici di confronto e, infatti, il DLAD si è dimostrato superiore agli esperti tanto nella individuazione di RX

statisticamente significativamente superiore all'auc dei radiologi di 0,808 (ic 95% 0,777-0,838); non ci sono state differenze statisticamente significative nelle auc per le altre 10 patologie. il tempo medio per interpretare le 420 immagini nel set di validazione è stato sostanzialmente più lungo per i radiologi (240 minuti) rispetto a chexnext (1,5 minuti).

[142] Hwang EJ, Park S, Park CM e altre, Development and validation of a deep learning-based automated detection algorithm for major thoracic diseases on chest radiographs, in JAMA NetworkOpen 2019, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2728630, (30 luglio 2022): "*this diagnostic study developed a deep learning–based algorithm using single-center data collected between november 1, 2016, and january 31, 2017. the algorithm was externally validated with multicenter data collected between may 1 and july 31, 2018. a total of 54 221 chest radiographs with normal findings from 47 917 individuals (21 556 men and 26 361 women; mean [sd] age, 51 [16] years) and 35 613 chest radiographs with abnormal findings from 14 102 individuals (8373 men and 5729 women; mean [sd] age, 62 [15] years) were used to develop the algorithm. a total of 486 chest radiographs with normal results and 529 with abnormal results (1 from each participant; 628 men and 387 women; mean [sd] age, 53 [18] years) from 5 institutions were used for external validation. fifteen physicians, including nonradiology physicians, board-certified radiologists, and thoracic radiologists, participated in observer performance testing. data were analyzed in august 2018.*", **tradotto letteralmente**: "***questo studio diagnostico ha sviluppato un algoritmo basato sull'apprendimento profondo utilizzando dati a centro singolo raccolti tra il 1 novembre 2016 e il 31 gennaio 2017. l'algoritmo è stato convalidato esternamente con dati multicentrici raccolti tra il 1 maggio e il 31 luglio 2018. un totale di 54 221 radiografie del torace con reperti normali da 47917 individui (21556 uomini e 26361 donne; età media [sd], 51 [16] anni) e 35613 radiografie del torace con reperti anormali da 14102 individui (8373 uomini e 5729 donne; media [sd] età, 62 [15] anni) sono stati utilizzati per sviluppare l'algoritmo. un totale di 486 radiografie del torace con risultati normali e 529 con risultati anormali (1 da ciascun partecipante; 628 uomini e 387 donne; età media [sd], 53 [18] anni) da 5 istituti sono stati utilizzati per la convalida esterna. quindici medici, inclusi medici non radiologici, radiologi certificati dal consiglio di amministrazione e radiologi toracici, hanno partecipato al test delle prestazioni dell'osservatore. i dati sono stati analizzati ad agosto 2018***"

patologiche (983 corrette su 1000, mentre gli umani oscillavano tra 814 e 932 con $p < 0,05$) quanto, nella localizzazione corretta delle lesioni, il DLASD ha localizzato le lesioni 985 volte su 1000, mentre i medici oscillavano tra 781 e 907[143], con una differenza di quasi 100 lesioni.

3.1.2 Intelligenza artificiale e oncologia: l'applicazione dell'i.a. nella lotta e prevenzione dei tumori al seno

Un altro importante settore in cui sono proliferati gli studi dei sistemi di IA è lo screening mammografico, che, in chiave di prevenzione, si pone l'obiettivo di diagnosticare le neoplasie mammarie in fase precoce, ossia in assenza di segni evidenti di malattia, al fine di ottenere migliori risultati salvifici per i soggetti colpiti.

L'interpretazione delle mammografie è uno di quei settori caratterizzati da possibili falsi positivi e falsi negativi poiché la fisiologica densità radiologica mammaria può mascherare quella tumorale rendendo molto difficile una diagnosi precoce.

Tali difficoltà hanno sviluppato un grande interesse per la realizzazione di sistemi di intelligenza artificiale, in grado di migliorare le performance diagnostiche dei radiologi, e uno tra i più noti sistemi di intelligenza artificiale è stato sviluppato da Google che, secondo uno studio pubblicato sula rivista Nature[144], sarebbe in grado di ridurre i falsi positivi del 5,7% e

---

[143] Ibidem : "*the algorithm demonstrated a median (range) area under the curve of 0.979 (0.973-1.000) for image-wise classification and 0.972 (0.923-0.985) for lesion-wise localization; the algorithm demonstrated significantly higher performance than all 3 physician groups in both image-wise classification (0.983 vs 0.814-0.932; all p < .005) and lesion-wise localization (0.985 vs 0.781-0.907; all p < .001). significant improvements in both image-wise classification (0.814-0.932 to 0.904-0.958; all p < .005) and lesion-wise localization (0.781-0.907 to 0.873-0.938; all p < .001) were observed in all 3 physician groups with assistance of the algorithm.*"**tradotto letteralmente*: *"l'algoritmo ha dimostrato un'area mediana (intervallo) sotto la curva di 0,979 (0,973-1,000) per la classificazione dell'immagine e 0,972 (0,923-0,985) per la localizzazione della lesione; l'algoritmo ha dimostrato prestazioni significativamente più elevate rispetto a tutti e 3 i gruppi di medici sia nella classificazione dell'immagine (0,983 vs 0,814-0,932; tutti p < .005) che nella localizzazione della lesione (0,985 vs 0,781-0,907; tutti p < .001). miglioramenti significativi sia nella classificazione dell'immagine (da 0,814-0,932 a 0,904-0,958; tutti p < .005) che nella localizzazione della lesione (da 0,781-0,907 a 0,873-0,938; tutti p < .001) sono stati osservati in tutti e 3 i gruppi di medici con l'aiuto dell'algoritmo"***

[144] Mayer, McKinney S. e altri "International evaluation of an AI system for breast cancer screening", in Nature 2020, gennaio 2020, https://www.nature.com/articles/s41586-019-1799-6, (5 agosto 2022) : "*screening mammography aims to identify breast cancer at earlier stages of the disease, when treatment can be more successful1. despite the existence of screening programmes worldwide, the interpretation of mammograms is affected by high rates of false positives and false negatives2. here we present an artificial intelligence (ai) system that is capable of surpassing human experts in breast cancer prediction. to assess its performance in the clinical setting, we curated a large representative dataset from the uk and a large enriched dataset from the usa. we show an absolute reduction of 5.7% and 1.2% (usa and uk) in false positives and 9.4% and 2.7% in false negatives. we provide evidence of the ability of the system to generalize from the uk to the usa. in an independent study of six radiologists, the ai system outperformed all of the human readers: the area under the receiver operating characteristic curve (auc-roc) for the ai system was greater than the auc-roc for the average radiologist by an absolute margin of 11.5%. we ran a simulation in which the ai system participated in the double-reading process that is used in the uk, and found that the ai system maintained non-inferior performance and reduced the workload of the second reader by 88%. this robust assessment of the ai system paves the way for clinical trials to improve the accuracy and efficiency of breast cancer screening.*"**tradotto letteralmente***: ***"la mammografia di screening mira a identificare il cancro al seno nelle fasi iniziali della malattia, quando il trattamento può avere più successo1. nonostante l'esistenza di programmi di screening in tutto il mondo, l'interpretazione delle mammografie è influenzata da alti tassi di falsi positivi e falsi negativi2. qui presentiamo un sistema di intelligenza artificiale (ai) in grado di superare gli esperti umani nella previsione del cancro al seno. per valutare le sue prestazioni in ambito clinico, abbiamo curato un ampio set di dati rappresentativo dal regno unito e un ampio set di dati arricchito dagli stati uniti. mostriamo una riduzione assoluta del 5,7% e 1,2% (usa e regno unito) nei falsi positivi e del 9,4% e 2,7% nei falsi negativi. forniamo prove della capacità del sistema di***

1,2% e i falsi negativi del 9,4% e 2,7%, utilizzando rispettivamente database statunitensi e britannici.[145]

Anche nello studio in esame si cerca di dimostrare come l'I.A. sia più accurata dei radiologi, perché a differenza degli esseri umani, i computer non sono influenzati dalla stanchezza o dalle distrazioni della vita quotidiana, ma è stato rilevato che vi sono innumerevoli questioni aperte prima fra tutte, il consenso al trattamento dei dati sanitari personali ad opera di sistemi di intelligenza artificiale.

Nella lotta contro il carcinoma al seno la *DeepTrace Technologies*, una startup attiva nel campo delle applicazioni medicali dell'I.A., in collaborazione con un gruppo di ricercatori italiani dell'Università degli Studi di Milano, dell'IRCCS Policlinico San Donato e del Centro Diagnostico Italiano, hanno ideato un software di intelligenza artificiale (IA) denominato *TRACE4BDensity*, in grado di classificare in maniera coerente e accurata la densità del seno durante la mammografia.

Il lavoro è stato presentato sulla rivista scientifica '*Radiology: Artificial Intelligence'*, in cui gli autori hanno sviluppato retrospettivamente e convalidato esternamente un software per la classificazione BD basato su reti neurali convoluzionali da mammografie ottenute tra il 2017 e il 2020.

I ricercatori italiani hanno cercato di sviluppare un software per la classificazione della densità mammaria basato sul deep learning con reti neurali convoluzionali, al fine di creare un tipo sofisticato di intelligenza artificiale in grado di discernere modelli sottili nelle immagini che vadano oltre le capacità dell'occhio umano.

Il software di IA TRACE4BDensity è stato addestrato sotto la supervisione di sette radiologi esperti che hanno valutato visivamente 760 immagini mammografiche in modo

generalizzare dal regno unito agli stati uniti. in uno studio indipendente su sei radiologi, il sistema di intelligenza artificiale ha superato tutti i lettori umani: l'area sotto la curva caratteristica operativa del ricevitore (auc-roc) per il sistema di intelligenza artificiale era maggiore dell'auc-roc per il radiologo medio di un margine assoluto dell'11,5%. abbiamo eseguito una simulazione in cui il sistema di intelligenza artificiale ha partecipato al processo di doppia lettura utilizzato nel regno unito e abbiamo scoperto che il sistema di intelligenza artificiale manteneva prestazioni non inferiori e riduceva il carico di lavoro del secondo lettore dell'88%. *questa solida valutazione del sistema di intelligenza artificiale apre la strada a studi clinici per migliorare l'accuratezza e l'efficienza dello screening del cancro al seno.*

[145] Ibidem: "…per valutare le sue prestazioni in ambito clinico, abbiamo curato un ampio set di dati rappresentativo dal regno unito e un ampio set di dati arricchito dagli stati uniti. mostriamo una riduzione assoluta del 5,7% e 1,2% (usa e regno unito) nei falsi positivi e del 9,4% e 2,7% nei falsi negativi. forniamo prove della capacità del sistema di generalizzare dal regno unito agli stati uniti. in uno studio indipendente su sei radiologi, il sistema ai ha superato tutti i lettori umani: l'area sotto la curva caratteristica operativa del ricevitore (auc-roc) per il sistema all'era maggiore dell'auc-roc per il radiologo medio di un margine assoluto dell'11,5%. abbiamo eseguito una simulazione in cui il sistema di intelligenza artificiale ha partecipato al processo di doppia lettura utilizzato nel regno unito e abbiamo scoperto che il sistema di intelligenza artificiale manteneva prestazioni non inferiori e riduceva il carico di lavoro del secondo lettore dell'88%. questa solida valutazione del sistema di intelligenza artificiale apre la strada a studi clinici per migliorare l'accuratezza e l'efficienza dello screening del cancro al seno"

indipendente e, inoltre, la convalida esterna dello strumento è stata eseguita dai tre radiologi su un set di dati di 384 immagini mammografiche[146].

Lo studio in esame ha dimostrato che TRACE4BDensity ha un'accuratezza dell'89% nel distinguere tra tessuto mammario a bassa densità e tessuto mammario ad alta densità e ciò dà la possibilità di superare la riproducibilità non ottimale della classificazione visiva umana, permettendo un aiuto più concreto nel processo decisionale.

3.1.3. L' Intelligenza artificiale applicata al settore della cardiologia

Nel settore della cardiologia da decenni vengono utilizzati gli elettrocardiogrammi (ECG) con lettura automatica in cui i dati registrati vengono analizzati automaticamente da algoritmi computerizzati e interpretati dal medico.

Tuttavia, gli errori nell'accuratezza diagnostica di tali strumenti sono frequenti e un medico inesperto nella lettura di un ECG potrebbe non riconoscere degli errori di un'interpretazione automatica e, pertanto, mettere in pericolo la salute e la vita del paziente.

Per far fronte a tali problematiche negli ultimi anni alcuni ricercatori hanno cercato di utilizzare lo strumento di deep learning, in particolare utilizzando le reti neurali convoluzionali (CNN), per l'analisi delle immagini, al fine di poter creare un algoritmo che permetta un'interpretazione ecocardiografica completa.

---

[146] Magni V., Interlenghi M, altri "development and validation of an ai-driven mammographic breast density classification tool based on radiologist consensus, radiology, in artificial intelligence, https://pubs.rsna.org/doi/abs/10.1148/ryai.210199 , (5 agosto 2022) : "*mammographic breast density (bd) is commonly visually assessed using the breast imaging reporting and data system (bi-rads) four-category scale. to overcome inter- and intraobserver variability of visual assessment, the authors retrospectively developed and externally validated a software for bd classification based on convolutional neural networks from mammograms obtained between 2017 and 2020. the tool was trained using the majority bd category determined by seven board-certified radiologists who independently visually assessed 760 mediolateral oblique (mlo) images in 380 women (mean age, 57 years ± 6 [sd]) from center 1; this process mimicked training from a consensus of several human readers. external validation of the model was performed by the three radiologists whose bd assessment was closest to the majority (consensus) of the initial seven on a dataset of 384 mlo images in 197 women (mean age, 56 years ± 13) obtained from center 2. the model achieved an accuracy of 89.3% in distinguishing bi-rads a or b (nondense breasts) versus c or d (dense breasts) categories, with an agreement of 90.4% (178 of 197 mammograms) and a reliability of 0.807 (cohen κ) compared with the mode of the three readers. this study demonstrates accuracy and reliability of a fully automated software for bd classification*." **tradotto letteralmente:** "***la densità mammografica della mammella (bd) viene comunemente valutata visivamente utilizzando la scala a quattro categorie bi-rads (breast imaging reporting and data system). per superare la variabilità inter e intraosservatore della valutazione visiva, gli autori hanno sviluppato retrospettivamente e convalidato esternamente un software per la classificazione bd basato su reti neurali convoluzionali da mammografie ottenute tra il 2017 e il 2020. lo strumento è stato addestrato utilizzando la categoria bd maggioritaria determinata da sette board- radiologi certificati che hanno valutato visivamente in modo indipendente 760 immagini oblique mediolaterali (mlo) in 380 donne (età media, 57 anni ± 6 [sd]) dal centro 1; questo processo ha imitato la formazione da un consenso di diversi lettori umani. la convalida esterna del modello è stata eseguita dai tre radiologi la cui valutazione bd era più vicina alla maggioranza (consenso) dei sette iniziali su un set di dati di 384 immagini mlo in 197 donne (età media, 56 anni ± 13) ottenute dal centro 2. il modello ha ottenuto un'accuratezza dell'89,3% nel distinguere le categorie bi-rads aob (seni non densi) rispetto a c o d (seni densi), con un accordo del 90,4% (178 su 197 mammografie) e un'affidabilità di 0,807 (cohen κ) rispetto alla modalità dei tre lettori. questo studio dimostra l'accuratezza e l'affidabilità di un software completamente automatizzato per la classificazione bd".***

In un articolo pubblicato nel 2018 sulla rivista scientifica "*NPJ Digit Med*", intitolato: *" Fast and accurate view classification of echocardiograms using deep learning*" alcuni autori hanno addestrato una rete neurale convoluzionale per classificare simultaneamente 15 visualizzazioni standard (12 video, 3 immagini fisse) prese da 267 ecocardiogrammi transtoracici che hanno catturato una gamma di variazioni cliniche del mondo reale al fine di verificare se l'applicazione dell'algoritmo risultasse più reciso degli ecocardiografi certificati[147].

Nello studio in esame è stato dimostrato che l'utilizzo di reti neurali ha un alto grado di sensibilità, pari quasi al 93%, di specificità e pari al 90%, nella diagnostica delle sindromi coronariche acute, paragonabile a quelle dei cardiologi umani.

Nell'ambito dell'ecocardiografia, gli algoritmi hanno fornito risultati migliori rispetto a gruppi di cardiologi esperti e sono anche in grado di quantificare altri parametri quali ad esempio le stenosi vascolari e l'ischemia coronarica, evitando così misure invasive.

Tuttavia, tali sistemi sono ancora a livello sperimentale e rudimentale e, pertanto, ad oggi vengono ancora utilizzati gli elettrocardiogrammi con lettura automatica da parte di algoritmi computerizzati e interpretati dal medico.

3.2. La responsabilità civile nel codice civile del 1942 e la responsabilità del medico alla luce della legge n. 24 del 2017 (Cd. Legge Gelli-Bianco)

La tematica della responsabilità civile dell'intelligenza artificiale applicata all' ambito medico non può prescindere da una breve esposizione degli elementi fondamentali della responsabilità civile in generale e soprattutto dalle modifiche apportate dalla novella del 2017 in ambito di responsabilità medica.

[147] Madani A., Arnaout R., Mofrad M., " Fast And Accurate View Classification Of Echocardiograms Using Deep Learning", In Npj Digit med 2018, https://www.nature.com/articles/s41746-017-0013-1, (10 agosto 2022): "*…we trained a convolutional neural network to simultaneously classify 15 standard views (12 video, 3 still), based on labeled still images and videos from 267 transthoracic echocardiograms that captured a range of real-world clinical variation. our model classified among 12 video views with 97.8% overall test accuracy without overfitting. even on single low-resolution images, accuracy among 15 views was 91.7% vs. 70.2-84.0% for board-certified echocardiographers. data visualization experiments showed that the model recognizes similarities among related views and classifies using clinically relevant image features. our results provide a foundation for artificial intelligence-assisted echocardiographic interpretation"*. **traduzione letterale: "*abbiamo addestrato una rete neurale convoluzionale per classificare simultaneamente 15 visualizzazioni standard (12 video, 3 immagini fisse), sulla base di immagini fisse e video etichettati da 267 ecocardiogrammi transtoracici che hanno catturato una gamma di variazioni cliniche del mondo reale. il nostro modello è classificato tra 12 visualizzazioni video con una precisione complessiva del test del 97,8% senza overfitting. anche su singole immagini a bassa risoluzione, l'accuratezza tra 15 visualizzazioni è stata del 91,7% rispetto al 70,2-84,0% degli ecocardiografi certificati. gli esperimenti di visualizzazione dei dati hanno mostrato che il modello riconosce le somiglianze tra le viste correlate e classifica utilizzando caratteristiche dell'immagine clinicamente rilevanti. i nostri risultati forniscono una base per l'interpretazione ecocardiografica assistita dall'intelligenza artificiale."***

In via preliminare occorre evidenziare che la responsabilità civile si inserisce nell'ambito del sistema delle obbligazioni ai sensi del 1173 c.c., e il fatto illecito ne costituisce la sua fonte.

La Costituzione non ci offre un modello di responsabilità civile, ma il modello generale è contenuto nell'art 2043 c.c.[148], i cui elementi costituiti possono essere così riassunti:

- elemento oggettivo, articolato al suo interno in azione, nesso di causalità materiale e danno ingiusto;
- antigiuridicità: che si sostanzia nel comportamento non autorizzato dall'ordinamento giuridico e posto in essere dall'agente;
- elemento soggettivo, declinato nelle sue due forme dolo e colpa, la cui disciplina viene mutuata dal diritto penale, in particolare dall'art 43 cp[149], e modellata alla responsabilità civile.
- danno conseguenza 1223 c.c. che si identifica nelle conseguenze dirette e immediate del fatto illecito che possono essere sia di tipologia patrimoniale o, nei casi previsti dalla legge, non patrimoniale (cfr art. 2059 c.c.)

Nella vigenza dello Statuto albertino del 1865[150], la responsabilità civile è stata considerata e regolata quale responsabilità ancillare a quella penale e solo con il codice del 1942 fu introdotto un nuovo concetto di "danno ingiusto" che ha spostato il focus del risarcimento dal fatto storico alla lesione ingiusta subita dalla vittima.

Pertanto, la funzione della responsabilità civile, nel modello generale delineato dal 2043 cc, è di tipo compensativa: la finalità è quella di compensare il danneggiato per il danno subito e tale funzione è prevista al fine di concretizzare il cosiddetto principio dell'indifferenza, cioè porre il danneggiato nella posizione antecedente al fatto illecito.

La finalità compensativa giustifica il fatto della mancata tipizzazione dei comportamenti illeciti, cosa che invece avviene nel sistema penale, e ciò perché ai fini del risarcimento l'unico

[148] Art 2043 c.c.: "Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

[149] Art 43 cp dispone che : "Il delitto:

è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione;

è preterintenzionale, o oltre l'intenzione, quando dall'azione od omissione deriva un evento dannoso o pericoloso più grave di quello voluto dall'agente;

è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline.

La distinzione tra reato doloso e reato colposo, stabilita da questo articolo per i delitti, si applica altresì alle contravvenzioni, ogni qualvolta per queste la legge penale faccia dipendere da tale distinzione un qualsiasi effetto giuridico.

[150] il codice civile italiano del 1865 all'art.1151, disponeva: «Qualunque fatto dell'uomo che arreca danno ad altri, obbliga quello per colpa del quale è avvenuto, a risarcire il danno».

elemento rilevante è il cosiddetto danno ingiusto che, inizialmente si riteneva coincidesse solo con la lesione del diritto soggettivo assoluto mentre, ad oggi, la giurisprudenza, ampliando il campo di applicazione, utilizza lo strumento della responsabilità civile per tutelare tutte le situazioni giuridiche soggettive meritevoli di tutela, siano esse inerenti a diritti di credito, interessi legittimi ovvero situazioni di fatto rilevanti quali il possesso.

In merito alla finalità compensativa della responsabilità civile, occorre sottolineare che ad oggi essa non è più l'unica a rilevare, poiché come affermato dalla Cassazione, la responsabilità civile ha una funzione polivalente; infatti, le Sezioni Unite chiamate a pronunciarsi sulla possibilità di poter delibare una sentenza americana che riconosceva il risarcimento dei cd. *punitive damages*, con sentenza n. 16601 del 05/07/2017 hanno statuito che: "*Nel vigente ordinamento, alla responsabilità civile non è assegnato solo il compito di restaurare la sfera patrimoniale del soggetto che ha subito la lesione, poiché sono interne al sistema la funzione di deterrenza e quella sanzionatoria del responsabile civile. Non è, quindi, incompatibile con l'ordinamento italiano l'istituto di origine statunitense dei risarcimenti punitivi. Il riconoscimento di una sentenza straniera che contenga una pronuncia di tale genere deve, però, corrispondere alla condizione che essa sia stata resa nell'ordinamento straniero su basi normative che garantiscano la tipicità delle ipotesi di condanna, la prevedibilità della stessa e i limiti quantitativi, dovendosi avere riguardo, in sede di delibazione, unicamente agli effetti dell'atto straniero e alla loro compatibilità con l'ordine pubblico*"[151].

Nella responsabilità da fatto illecito – ex Art. 2043 C.C – l'onere della prova è posto a carico del danneggiato, il quale deve provare non solo il fatto doloso o colposo ma anche il danno ingiusto ed il nesso di causalità che intercorre tra l'azione o l'omissione e la lesione.

Oltre al modello generale di responsabilità civile delineato dall'art 2043 cc, sono presenti nel Codice civile e in leggi speciali ulteriori modelli di responsabilità civile che derogano al modello generale al fine di rispondere alla proliferazione delle fonti di rischio ed alla massificazione dei danni.

Le deroghe contenute in questi modelli attengono principalmente al criterio di imputazione del fatto, alla ripartizione dell'onere probatorio e all'elemento soggettivo e, inoltre, le responsabilità che ne derivano possono essere classificate in due grandi gruppi: responsabilità oggettive e responsabilità aggravate o soggettivamente presunte.

In relazione alla responsabilità oggettiva, questa ricorre nell'ipotesi in cui l'autore risponde dell'evento dannoso anche in assenza dell'elemento soggettivo poiché la ratio della

[151] Sentenza del 05 luglio 2017, Cassazione civile, Sezioni Unite, n. 16601, Normattiva, https://www.normattiva.it, (10 agosto 2022)

norma è quella di tutelare chi è esposto a rischi inevitabilmente indotti da alcune attività o cose, accollando tali rischi al soggetto che li immette in circolazione nella società.

Si pensi ad esempio all'art 2049 c.c. che disciplina la responsabilità del preponente per i danni cagionati a terzi dai suoi preposti nell'esercizio delle incombenze cui gli stessi sono adibiti; in tali norme, il legislatore costruisce un modello di responsabilità basato su un criterio di imputazione che prescinde totalmente dalla valutazione circa il carattere censurabile della condotta del soggetto responsabile[152].

In relazione alla cosiddetta responsabilità aggravata, il legislatore, invece, costruisce la fattispecie tenendo conto anche dell'elemento soggettivo della colpa, capovolgendo l'onere probatorio rispetto al modello generale: la colpa in capo al danneggiante è presunta e sarà onere dello stesso dover fornire la prova liberatoria relativa alla propria diligenza.

La ratio di tali fattispecie si rinviene nella presenza di fonti di rischio (beni o attività) la cui pericolosità è normalmente neutralizzata dall'agire diligente del loro controllore e, pertanto lo stesso prodursi del danno è indice di carenza di diligenza e ciò giustifica la presunzione di colpa.

Le ipotesi di responsabilità aggravata previste dal legislatore sono:

a) Art. 2047 c.c.[153] che prevede la responsabilità per il danno cagionato da persona incapace di intendere o di volere: in tali casi il risarcimento è dovuto da chi era incaricato alla sorveglianza dell'incapace, quali ad esempio i genitori del minore, il precettore e il maestro d'arte nei confronti di allievi e apprendisti.
   In tale tipologia di responsabilità la prova liberatoria consiste nella dimostrazione di non aver potuto impedire il fatto e, nel caso dei genitori, la prova liberatoria verrà arricchita dalla dimostrazione della consona educazione del minore.

[152] Ulteriori ipotesi previste nel Codice civile e in leggi speciali, quali il codice del consumo sono:
   a) Art.2053 c.c. che disciplina la responsabilità del proprietario di un edificio o di altra costruzione per i danni cagionati dalla loro rovina, salvo che provi che questa non è dovuta a difetto di manutenzione o a vizio di costruzione. Anche in questo caso il proprietario è chiamato a rispondere a prescindere dal carattere di colpevolezza, ma solo per il fatto di essere proprietario.
   b) Art.2054, co.4 che disciplina la responsabilità del conducente e del proprietario (o, in mancanza, dell'usufruttuario) di un veicolo senza guida di rotaie per i danni cagionati dalla circolazione del veicolo stesso, derivanti da vizi di costruzione.
   c) L'esercente di un impianto nucleare è responsabile per ogni danno cagionato alle persone o alle cose determinato da un incidente nucleare avvenuto nell'impianto o connesso allo stesso.
   d) Art.114 Codice del consumo, in relazione ai danni da prodotto difettoso, statuisce che il produttore è responsabile del danno cagionato dai difetti del prodotto

[153] Art 2047 cc: "In Caso Di Danno Cagionato Da Persona Incapace Di Intendere O Di Volere, Il Risarcimento È Dovuto Da Chi È Tenuto Alla Sorveglianza Dell'incapace, Salvo Che Provi Di Non Aver Potuto Impedire Il Fatto.
Nel Caso In Cui Il Danneggiato Non Abbia Potuto Ottenere Il Risarcimento Da Chi È Tenuto Alla Sorveglianza, Il Giudice, In Considerazione Delle Condizioni Economiche Delle Parti, Può Condannare L'autore Del Danno A Un'equa Indennità.

b) Art 2050 c.c.[154] che prevede la responsabilità per l'esercizio di attività pericolose: la norma si riferisce sia alle attività pericolose tipizzate, nel codice o in leggi speciali, sia a quelle che siano comunque tali per la loro attitudine a produrre un rischio e, l'esercente di un'attività pericolosa può liberarsi dalla responsabilità solo provando di aver adottato, in concreto, tutte le misure idonee ad evitare il danno.

   Per quanto attiene all'onere probatorio, la giurisprudenza ritiene che oltre alla prova negativa, consistente nell'adozione di tutte le misure idonee a scongiurare il danno, il danneggiante debba fornire anche la prova positiva della causa esterna, quale, ad esempio la prova di un fatto naturale, connotata dai caratteri di imprevedibilità, eccezionalità ed inevitabilità

   Infatti, nell'esercizio di un'attività pericolosa, la prevedibilità del danno è in re ipsa e il soggetto deve agire tenendo conto del pericolo per i terzi.

c) Art 2051[155]c.c. che prevede la responsabilità per il danno cagionato da cosa in custodia: la responsabilità del custode ricorre nel caso in cui vi siano contemporaneamente due requisiti: il primo è la custodia, che consiste nel rapporto che lega il custode alla cosa e postula l'effettivo potere sulla stessa, e cioè la sua disponibilità giuridica e materiale, con il conseguente potere di intervento su di essa[156], il secondo consiste nella derivazione del danno dalla cosa.

   Il legislatore prevede che il custode possa liberarsi dalla responsabilità connessa al danno provando che il danno è derivato da caso fortuito; tuttavia, nella prassi, la giurisprudenza ritiene che il custode, oltre alla prova negativa del caso fortutito, debba fornire anche la prova positiva della causa esterna, quale esempio la prova di un fatto naturale o del terzo, connotata dai caratteri di imprevedibilità, eccezionalità ed inevitabilità[157].

[154] Art 2050 Cc. Responsabilità Per L'esercizio Di Attività Pericolose: "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno"

[155] Art 2051 Cc: Danno Cagionato Da Cosa In Custodia: ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito

[156] Sentenza 9 Giugno 2010, Cassazione Civile N. 13881, Normattiva, https://www.normattiva.it

[157] Sentenza 30 Ottobre 2019, Cassazione Civile Ordinanza N. 27970, In , Normattiva, https://www.normattiva.it, : "il criterio di imputazione della responsabilità di cui all'art. 2051 c.c. ha carattere oggettivo, essendo sufficiente, per la sua configurazione, la dimostrazione da parte dell'attore del nesso di causalità tra la cosa in custodia ed il danno, mentre al custode spetta l'onere della prova liberatoria del caso fortuito, inteso come fattore che, in base ai principi della regolarità o adeguatezza causale, esclude il nesso eziologico tra cosa e danno, ed è comprensivo della condotta incauta della vittima, che assume rilievo ai fini del concorso di responsabilità ai sensi dell'art. 1227, comma 1, c.c., e deve essere graduata sulla base di un accertamento in ordine alla sua effettiva incidenza causale sull'evento dannoso, che può anche essere esclusiva."

d) Art 2052 c.c. che prevede la responsabilità per il danno cagionato da animali[158]: la responsabilità sussiste sia se l'animale è domestico sia se l'animale è da lavoro e, inoltre, è indifferente se esso sia sotto la sua custodia, sia smarrito o fuggito.
La prova liberatoria concessa dal legislatore consiste nella dimostrazione del caso fortuito benché la giurisprudenza richieda nella prassi anche la prova della causa esterna che sfugge al controllo del soggetto considerato responsabile.

Effettuata tale breve premessa, occorre ora analizzare una particolare forma di responsabilità civile: la responsabilità medica.

La responsabilità medica si inserisce nel più ampio filone della responsabilità professionale, che trova il suo fondamento normativo nel Capo II del titolo III del Libro V del Codice civile all'art. 2236 c.c[159]., il quale prevede la responsabilità del professionista solo nel caso in cui il danno sia stato prodotto da un comportamento sorretto da dolo o colpa grave.

Nelle obbligazioni inerenti all'esercizio di un'attività professionale, l'art 1176, comma 2, c.c.[160] richiede un tipo di diligenza specifica, differente da quella del "buon padre di famiglia" e parametrata al tipo di attività svolta; la proiezione di tale forma di diligenza nell'attività medica è identificata nella perizia, intesa quale conoscenza e applicazione di quel complesso di regole tecniche proprie della categoria professionale di appartenenza, le quali sono tese a circoscrivere l'àmbito del rischio consentito e, per l'effetto, l'àmbito di liceità dell'intervento medico.[161]

Nel quadro così delineato, si configura la fattispecie della colpa medica ogniqualvolta vi è una inosservanza e/o violazione da parte del sanitario delle specifiche regole cautelari di condotta proprie dell'agente modello del settore specialistico di riferimento, la quale può concretarsi sia in una condotta attiva che in una condotta omissiva; in quest'ultimo caso la condotta del sanitario si sostanzia nell'omissione delle cautele prescritte, da valutare anche con riferimento ai protocolli terapeutici standardizzati (cd. Linee guida).

---

[158] Art 2052 Cc: il proprietario di un animale o chi se ne serve per il tempo in cui lo ha in uso, è responsabile dei danni cagionati dall'animale, sia che fosse sotto la sua custodia, sia che fosse smarrito o fuggito, salvo che provi il caso fortuito

[159] Art 2236 C.C: "se la prestazione implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni, se non in caso di dolo o di colpa grave"

[160] Art 1176 , Co.2, Cc: "…nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata"

[161] Così, In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Vocabolario On Line,Perizia, https://www.treccani.it/vocabolario/perizia/#:~:text=Stima%20e%20giudizio%20espressi%20da,%2C%20di%20na%20scrittura%2C%20ecc.., (13 agosto 2022): stima e giudizio espressi da un perito, per determinare il valore commerciale di un bene (valore di p., il valore così accertato), l'autenticità e l'attribuzione di un'opera d'arte, di una scrittura, Ecc.

Prima della novella del 2017, la responsabilità medica veniva ricondotta al modello della responsabilità contrattuale grazie alla teoria del c.d. "*contatto sociale qualificato*[162]", la quale garantiva la risarcibilità della lesione di obblighi di protezione, obblighi autonomi rispetto al primario obbligo di prestazione sia dal punto di vista strutturale sia da quello della fonte.

Secondo la teoria del contatto sociale qualificato, la lesione, fonte dell'obbligazione risarcitoria, consisterebbe nella violazione degli obblighi di diligenza, il cui mancato rispetto determinerebbe la responsabilità per inadempimento di cui all' art. 1218 c.c..

Con la teoria del contatto sociale viene valorizzato il particolare rapporto giuridico "qualificato"[163] che viene ad instaurarsi tra il medico ed il paziente, il quale non può essere ricondotto nell'alveo dell'art. 2043 c.c.: il medico, infatti, non è un "*quisque de popolo*" sul quale graverebbe solo il generico dovere di *neminem laedere*, ma il rapporto giuridico che si instaura presuppone in capo al medico l'obbligato di tutelare la salute del paziente in virtù sia di precise disposizioni di legge che in virtù del contratto stipulato con l'azienda ospedaliera per il quale lavora.

La ricostruzione effettuata dalla sentenza a Sezioni Unite n. 589/99 è stata poi ribadita nella Sentenza a Sezioni Unite n. 577/2008, la quale si è occupata del riparto dell'onere probatorio tra medico e paziente.

La sentenza del 2008[164] ritiene applicabili anche alla responsabilità medica i principi in materia di prova dell'inadempimento espressi nella celebre pronuncia, sempre a sezioni unite, n. 13533/2001 secondo cui: "*Il creditore deve dare la prova della fonte negoziale o legale del suo diritto, limitandosi alla mera allegazione della circostanza dell'inadempimento della controparte, mentre il debitore è gravato dall'onere della prova del fatto estintivo, costituito dall'avvenuto adempimento*".

---

[162] Santoro A., La Responsabilità Da Contatto Sociale. Profili Pratici E Applicazioni Giurisprudenziali, Giuffrè, Milano 2012 Pp.1-228,; Ma Vedi Anche, Venosta F., "Contatto Sociale" E Affidamento, Giuffè, Milano 2021 Pp. 1-213: la teoria del contatto sciale è stata elaborata dalla dottrina italiana sulla scia della dottrina tedesca degli anni '40, che aveva ricondotto alla più ampia teoria dei "rapporti contrattuali di fatto" tutte quelle ipotesi di responsabilità da inadempimento di obbligazioni senza prestazioni o violazione di doveri preesistenti di collaborazione e di protezione sussistenti in assenza di un contratto.

[163] Sentenza 22 gennaio 1999, Cassazione Civile sez. n. 589, Normattiva, https://www.normattiva.it, : "l'obbligazione del medico dipendente dal servizio sanitario per responsabilità professionale nei confronti del paziente, ancorché non fondata sul contratto, ma sul "contatto sociale" ha natura contrattuale. consegue che relativamente a tale responsabilità i regimi della ripartizione dell'onere della prova, del grado della colpa e della prescrizione sono quelli tipici delle obbligazioni da contratto d'opera intellettuale professionale"; "…nei confronti del medico, dipendente ospedaliero, si configurerebbe pur sempre una responsabilità contrattuale nascente da "un'obbligazione senza prestazione ai confini tra contratto e torto", in quanto poiché sicuramente sul medico gravano gli obblighi di cura impostigli dall'arte che professa, il vincolo con il paziente esiste, nonostante non dia adito ad un obbligo di prestazione, e la violazione di esso si configura come culpa in non facendo, la quale dà origine a responsabilità contrattuale."

[164] Sentenza 11 gennaio 2008, Cassazione Civile Sezioni Unite n. 577, Normattiva, https://www.normattiva.it

Applicando tali principi alla ripartizione dell'onere probatorio nelle cause di responsabilità professionale medica, risulta che l'attore (paziente-danneggiato) deve limitarsi a provare l'esistenza del contratto (o il contatto sociale) e l'insorgenza o l'aggravamento della patologia ed allegare l'inadempimento del debitore astrattamente idoneo a provocare il danno lamentato, rimanendo a carico del debitore (medico-danneggiante), l'onere di dimostrare o che tale inadempimento non vi è stato o che, pur essendovi stato, non è stato causa del danno.

Tale ricostruzione è stata per molto tempo utilizzata dalla giurisprudenza sino all'entrata in vigore del decreto-legge n. 158 del 13 settembre 2012 (cd. Decreto Balduzzi), il quale, al fine di scongiurare l'attività medica difensiva ha escluso la rilevanza penale delle condotte connotate da colpa lieve, che si collochino all'interno dell'area segnata da linee guida o da virtuose pratiche mediche purché accreditate dalla comunità scientifica, ed ha affermato la risarcibilità del danno ex art 2043 cc..

Proprio il richiamo contenuto nell'art. 3 del decreto-legge Balduzzi all'art. 2043 c.c. ha riaperto il dibattito sulla natura giuridica della responsabilità del medico e in tale contesto si sono formati due diversi orientamenti.[165]

Un primo orientamento ha ritenuto che l'art 3 decreto-legge 158/2012 si rivolgerebbe solo alla qualificazione penalistica della responsabilità medica e non intaccherebbe la ricostruzione civilista, la quale sarebbe sempre configurata come responsabilità da contatto sociale qualificato che resterebbe disciplinata ai sensi dell'art. 1218 c.c.[166]

Un secondo orientamento ha, invece, ritenuto che con il decreto Baluzzi il legislatore avrebbe espressamente preso posizione sul tema, poiché la ratio della novella suggerisce di ricostruire la responsabilità del medico in termini aquiliani, «gettando alle ortiche l'utilizzabilità in concreto della teorica del contatto sociale».

Al fine di superare le profonde incertezze interpretative contenute nel decreto Balduzzi, il legislatore ha promulgato la legge n. 24/2017 (c.d. legge Gelli-Bianco)[167] che segna una

[165] Art 3 decreto-legge n. 158 del 13 settembre 2012 "l'esercente le professioni sanitarie che nello svolgimento della propria attività si attiene a linee guida e buone pratiche accreditate dalla comunità scientifica non risponde penalmente per colpa lieve. in tali casi resta comunque fermo l'obbligo di cui all'art. 2043 del codice civile. il giudice, anche nella determinazione del risarcimento del danno, tiene debitamente conto della condotta di cui al primo periodo.

[166] Sentenza 19 febbraio 2013, Cassazione Civile n. n. 4030. Normattiva, https://www.normattiva.it

[167] Art 7 legge 24/2017:" *la struttura sanitaria o sociosanitaria pubblica o privata che, nell'adempimento della propria obbligazione, si avvalga dell'opera di esercenti la professione sanitaria, anche se scelti dal paziente e ancorché non dipendenti della struttura stessa, risponde, ai sensi degli articoli 1218 e 1228 del codice civile, delle loro condotte dolose o colpose.*

2. la disposizione di cui al comma 1 si applica anche alle prestazioni sanitarie svolte in regime di libera professione intramuraria ovvero nell'ambito di attività di sperimentazione e di ricerca clinica ovvero in regime di convenzione con il servizio sanitario nazionale nonché attraverso la telemedicina.

3. l'esercente la professione sanitaria di cui ai commi 1 e 2 risponde del proprio operato ai sensi dell'articolo 2043 del codice civile, salvo che abbia agito nell'adempimento di obbligazione contrattuale assunta con il paziente. il giudice, nella determinazione del

decisa inversione di tendenza, attraverso il superamento della teoria del contatto sociale e l'affermazione della natura aquiliana della responsabilità dell'esercente la professione sanitaria che svolge la propria attività nell'ambito di una struttura sanitaria (cd. Medico strutturato), che risponde quindi ai sensi dell'art. 2043 c.c.

Brevemente, le novità introdotte dalla legge Gelli- Bianco in ambito medico attengono alla qualificazione della responsabilità come contrattuale per la struttura sanitaria e della responsabilità come civile per medico strutturato, nel rapporto con il paziente e, pertanto, trova applicazione il regime proprio di questi tipi di responsabilità, soprattutto per quanto concerne la ripartizione dell'onere della prova e la prescrizione.

La novella, infatti, qualificando come civile la responsabilità che sorge tra medico e paziente ha reso più gravoso per il danneggiato l'onere della prova: il paziente danneggiato dovrà provare il fatto illecito, il danno, il nesso causale tra il fatto e il danno, nonché la colpa o il dolo del danneggiante; mentre la responsabilità in capo alla struttura sanitaria rimane di tipo contrattuale[168] e il danneggiato dovrebbe provare solo l'inadempimento.

Occorre precisare che il paziente danneggiato non può rivolgersi immediatamente al giudice poiché la novella del 2017 subordina la procedura giudiziale o al preventivo espletamento di una consulenza tecnica preventiva in cui il C.T.U, nominato dal Tribunale ha il compito di accertare in via preliminare l'an e il quantum della responsabilità medica, nel rispetto del contraddittorio delle parti, o al procedimento di mediazione[169].

---

risarcimento del danno, tiene conto della condotta dell'esercente la professione sanitaria ai sensi dell'articolo 5 della presente legge e dell'articolo 590 sexies del codice penale, introdotto dall'articolo 6 della presente legge.
4. il danno conseguente all'attività della struttura sanitaria o sociosanitaria, pubblica o privata, e dell'esercente la professione sanitaria è risarcito sulla base delle tabelle di cui agli articoli 138 e 139 del codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209, integrate, ove necessario, con la procedura di cui al comma 1 del predetto articolo 138 e sulla base dei criteri di cui ai citati articoli, per tener conto delle fattispecie da esse non previste, afferenti alle attività di cui al presente articolo.
5. le disposizioni del presente articolo costituiscono norme imperative ai sensi del codice civile."

[168] le principali differenze tra la responsabilità contrattuale e quella extracontrattuale riguardano:
a) onere della prova, che è a carico del debitore-danneggiante nella responsabilità contrattuale, mentre spetta al danneggiato nella responsabilità extracontrattuale;
b) prescrizione dell'azione risarcitoria è decennale in caso di prescrizione responsabilità medica contrattuale, invece per extracontrattuale responsabilità medica prescrizione diventa quinquennale;
c) danno risarcibile, limitato a quello prevedibile nella responsabilità contrattuale, mentre potenzialmente illimitato nella responsabilità extracontrattuale.

[169] Art 8 l. 24/2017: " *chi intende esercitare un'azione innanzi al giudice civile relativa a una controversia di risarcimento del danno derivante da responsabilità sanitaria è tenuto preliminarmente a proporre ricorso ai sensi dell'articolo 696 bis del codice di procedura civile dinanzi al giudice competente.2. la presentazione del ricorso di cui al comma 1 costituisce condizione di procedibilità della domanda di risarcimento. è fatta salva la possibilità di esperire in alternativa il procedimento di mediazione ai sensi dell'articolo 5, comma 1-bis, del decreto legislativo 4 marzo 2010, n. 28. in tali casi non trova invece applicazione l'articolo 3 del decreto-legge 12 settembre 2014, n. 132, convertito, con modificazioni, dalla legge 10 novembre 2014, n. 162. l'improcedibilità deve essere eccepita dal convenuto, a pena di decadenza, o rilevata d'ufficio dal giudice, non oltre la prima udienza. il giudice, ove rilevi che il procedimento di cui all'articolo 696 bis del codice di procedura civile non è stato espletato ovvero che è iniziato ma non si è concluso, assegna alle parti il termine di quindici giorni per la presentazione dinanzi a sé dell'istanza di consulenza tecnica in via preventiva ovvero di completamento del procedimento.3. ove la conciliazione non riesca o il procedimento non si concluda entro*

Una volta esperita una di queste due procedure, il paziente potrà rivolgersi al giudice per ottenere il risarcimento del danno nei modi e nelle forme di cui agli articoli 702-bis e seguenti del codice di procedura civile e potrà convenire in giudizio la struttura sanitaria o sociosanitaria, pubblica o privata, la quale "risponderà, ai sensi degli articoli 1218 e 1228 del codice civile, delle loro condotte dolose o colpose" (art.7, comma 1, legge 24/2017), l'esercente la professione sanitaria, il quale "risponderà del proprio operato ai sensi dell'articolo 2043 del codice civile" (art.7, comma 2, legge 24/2017), l' esercente, nell'ipotesi in cui "abbia agito nell'adempimento di obbligazione contrattuale assunta con il paziente" (art.7, comma 3, legge 24/2017), l'impresa di assicurazione della struttura o dell'esercente "entro i limiti delle somme per le quali è stato stipulato il contratto di assicurazione" (art.12, comma 1, legge 24/2017).

Dal quadro sin qui delineato emerge che la responsabilità del medico nel nostro ordinamento è una responsabilità per colpa il cui rapporto di causalità, sia in ambito penale quanto in ambito civile, è regolato dall'art. 40 del Codice penale[170]e, pertanto, l'evento dovrà essere conseguenza dell'azione o dell'omissione del professionista.

Il successivo articolo 41cp[171] prevede, invece, le ipotesi in cui si verifica l'interruzione del nesso causale, ossia quando o sopravvenga un processo causale del tutto autonomo oppure quando l'iter causale sia caratterizzato da un percorso causale del tutto atipico, configurandosi come eccezionale ovvero imprevedibile.

Infine, per la dimostrazione della sussistenza del nesso causale nel diritto civile è sufficiente la causalità ordinaria secondo le leggi statistiche che rispondono alla regola

il termine perentorio di sei mesi dal deposito del ricorso, la domanda diviene procedibile e gli effetti della domanda sono salvi se, entro novanta giorni dal deposito della relazione o dalla scadenza del termine perentorio, è depositato, presso il giudice che ha trattato il procedimento di cui al comma 1, il ricorso di cui all'articolo 702 bis del codice di procedura civile. in tal caso il giudice fissa l'udienza di comparizione delle parti; si applicano gli articoli 702 bis e seguenti del codice di procedura civile.4. la partecipazione al procedimento di consulenza tecnica preventiva di cui al presente articolo, effettuato secondo il disposto dell'articolo 15 della presente legge, è obbligatoria per tutte le parti, comprese le imprese di assicurazione di cui all'articolo 10, che hanno l'obbligo di formulare l'offerta di risarcimento del danno ovvero comunicare i motivi per cui ritengono di non formularla. in caso di sentenza a favore del danneggiato, quando l'impresa di assicurazione non ha formulato l'offerta di risarcimento nell'ambito del procedimento di consulenza tecnica preventiva di cui ai commi precedenti, il giudice trasmette copia della sentenza all'istituto per la vigilanza sulle assicurazioni (ivass) per gli adempimenti di propria competenza. in caso di mancata partecipazione, il giudice, con il provvedimento che definisce il giudizio, condanna le parti che non hanno partecipato al pagamento delle spese di consulenza e di lite, indipendentemente dall'esito del giudizio, oltre che ad una pena pecuniaria, determinata equitativamente, in favore della parte che è comparsa alla conciliazione".

[170] Art 40 cp "nessuno può essere punito per un fatto previsto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende l'esistenza del reato non è conseguenza della sua azione od omissione" aggiungendo poi che "non impedire un evento, che sia l'obbligo giuridico di impedire, equivale a cagionarlo".

[171]Art 41 Cp : "il concorso di cause preesistenti o simultanee o sopravvenute, anche se indipendenti dall'azione od omissione del colpevole, non esclude il rapporto di causalità fra l'azione od omissione e l'evento" per poi aggiungere che solo le cause sopravvenute, in quanto inconoscibili e imprevedibili, "escludono il rapporto di causalità quando sono state da sole sufficienti a determinare l'evento" in quanto fattori eccezionali tali da modificare l'iter causale"

probatoria del "*più probabile che non*" mentre per la causalità penalistica la regola è quella "*dell'oltre ogni ragionevole dubbio*".

La condotta colposa del medico dovrà essere analizzata dal giudice ai sensi dall'art. 43 del Codice penale, il quale dispone che deve ritenersi colposo (o contro l'intenzione) un evento che, anche se previsto, non è voluto dall'agente ma che si verifica a causa di negligenza, imprudenza o imperizia oppure per inosservanza di leggi, regolamenti, ordini o discipline.

La condotta colposa del medico può esse sia generica, quando sia connotata da negligenza (ossia superficialità, trascuratezza, disattenzione). imprudenza o imperizia (ossia la scarsa preparazione professionale, insufficienti conoscenze tecniche o inesperienza), si specifica che si identifica con la violazione di norme che il medico non poteva ignorare e che era tenuto ad osservare poiché espressione di legge o di un'autorità pubblica/gerarchica, disciplinanti specifiche attività o il corretto svolgimento delle procedure sanitarie.

L'errore medico può rilevare nella fase diagnostica, in quella prognostica e nella fase terapeutica ma, ai fini della presente ricerca occorrerà approfondire l'errore diagnostico, il quale si identifica nel non corretto inquadramento diagnostico della patologia, come, ad esempio, quando il medico raccoglie i dati anamnestici in modo superficiale e non ha valorizzato o non ha rilevato una certa allarmante sintomatologia.

Infine, nel campo medico i principi inerenti alla responsabilità professionale si arricchiscono in caso équipe medica, ossia nel caso in cui vi sia una cooperazione finalizzata all'esecuzione della prestazione sanitaria sia essa organizzata gerarchicamente ovvero orizzontalmente.

Nel caso di equipe medica, la dottrina ha cercato di applicare il cosiddetto principio di affidamento, corollario del principio di personalità della responsabilità penale di cui all'art. 27 della Costituzione, che opera in relazione ad attività pericolose svolte da una pluralità di persone, permettendo a ciascun componente di essa di confidare nel fatto che il comportamento dell'altro è conforme alle regole di diligenza, prudenza e perizia.

Per quanto concerne lo specifico ambito della responsabilità medica, il principio di affidamento consente di perimetrare, entro certi limiti, la responsabilità del sanitario che operi all'interno di una equipe: risponde dell'azione o dell'omissione solo chi abbia commesso un errore riferibile alla propria specifica competenza medica, non potendo essere genericamente addebitata alla equipe operatoria, nel suo complesso, la responsabilità per gli errori commessi da uno dei suoi componenti, infatti, nell'ipotesi di operazione medica in equipe ciascun sanitario ha uno specifico compito e la verifica del nesso di causalità tra la condotta posta in

essere dal singolo medico, in violazione delle regole cautelari asseritamente violate, e l'evento, deve essere particolarmente stringente e compiuta con riguardo alla condotta ed al ruolo rivestito da ciascuno, non potendosi configurare aprioristicamente una responsabilità di gruppo[172] .

La giurisprudenza di legittimità ha cercato, soprattutto in campo penale, di raggiungere il delicato equilibrio tra il rispetto dell'obbligo di garanzia che grava su ciascun medico nei confronti del paziente, la tutela del principio di affidamento e il principio della responsabilità penale personale ex l'art 27 Costituzione.

L'evoluzione giurisprudenziale ha consentito di perimetrare la responsabilità penale ed ha permesso anche l'esonero dalla responsabilità del capo equipe, soggetto che per legge è titolare di una posizione di garanzia ed è quindi tenuto giuridicamente a controllare e ad impedire il verificarsi di un evento dannoso nei confronti del garantito, e che abbia legittimamente fatto affidamento sulla correttezza dell'operato di altro soggetto contitolare di una posizione di garanzia, nell'ipotesi in cui vi fosse una precisa suddivisione di ruoli e di mansioni.

Occorre ora verificare se tali principi siano applicabili nel caso in cui a cooperare con il medico non sia un altro specialista umano ma un'intelligenza artificiale.

3.2.1 Responsabilità civile in caso di cooperazione tra intelligenza umana e artificiale in ambito medico: la chirurgia robotica

Nel paragrafo precedente sono state analizzate le caratteristiche tipiche della responsabilità professionale per colpa, le quali possono ora essere così riassunte: a) autonomia delle decisioni; b) discrezionalità sulla prestazione da eseguire e sugli strumenti tecnici da utilizzare; c) personalità della prestazione[173].

Tuttavia occorre verificare se i principi sopra esposti vengano travolti nel caso in cui venga in rilievo una responsabilità per colpa oggettiva dell'utilizzatore dell'apparecchiatura dotata di intelligenza artificiale ovvero se venga in rilievo una la responsabilità soggettiva del professionista che deve necessariamente prende in considerazione la cooperazione di altre "intelligenze" nell'ambito della prestazione sanitaria al fine di poter delimitare le responsabilità degli operatori umani e artificiali e, soprattutto, occorre verificare se esistono dei criteri di ripartizione delle responsabilità tra chi adotta un sistema autonomo e tutti gli attori coinvolti

[172] Sentenza 12 febbraio 2019 Cassazione penale n.30626, Normattiva, https://www.normattiva.it; Sentenza 12 giugno 2019 Cassazione penale n. 3972 Normattiva, https://www.normattiva.it; Sentenza 21 novembre 2019 Cassazione penale n.49774, Normattiva, https://www.normattiva.it;

[173] Pasceri G. E Altri, Intelligenza Artificiale In Radiologia, Documento Sirm 2020, https://sirm.org/wp content/uploads/2021/04/317-Documento-SIRM-2020-Intelligenza-artificale-in-radiologia.pdf (20 agosto 2022)

nella sua realizzazione quali ad esempio il produttore dell'hardware, l'analista ideatore dell'algoritmo, il programmatore del software, il trainer, il soggetto adibito alla manutenzione del sistema etc.

Il punto di partenza nel valutare l'impatto che le tecnologie intelligenti esercitano sulle regole in punto di responsabilità è l'analisi delle regole contenute nel Codice civile e della legislazione speciale, tanto nei rapporti tra medico e paziente, quanto rispetto alla Struttura sanitaria che si avvale di beni integrati dall'I.A e che si troverà a dover gestire i rischi conseguenti al loro utilizzo.

Nel caso della chirurgia robotica, analizzata nei paragrafi precedenti, occorre premettere che ad oggi i robot chirurgici non sono autorizzati ad operare senza la supervisione di un medico, svolgendo perlopiù un'attività di supporto al personale sanitario e non un'attività autonoma.

Le barriere normative, etiche e legali imposte ai robot medici richiedono però un'attenta considerazione dei diversi livelli di autonomia degli stessi, nonché il contesto di utilizzo e, al fine di poter delimitare la responsabilità occorrerà prendere quale punto di partenza un studio scientifico pubblicato sulla rivista "*Science Robotics"* del 2017 in cui alcuni studiosi hanno distinto i robot sulla base della loro autonomia, costruendo una scala gerarchica che va dal livello 0, in cui i robot non hanno alcuna autonomia e rispondono e seguono il comando dell'utente umano, al livello 5 in cui il robot ha piena autonomia e non ha bisogno per svolgere sue funzioni dell'apporto umano[174].

[174] YANG G.Z. et al., Medical robotics—Regulatory, ethical, and legal considerations for increasing levels of autonomy, in Science Robotics, 2, 2017 https://www.science.org/doi/10.1126/scirobotics.aam8638 ; (20 agosto 2022) "*…level 0: no autonomy. this level includes tele-operated robots or prosthetic devices that respond to and follow the user's command. a surgical robot with motion scaling also fits this category because the output represents the surgeon's desired motion.*
level 1: robot assistance. the robot provides some mechanical guidance or assistance during a task while the human has continuous control of the system. examples include surgical robots with virtual fixtures (or active constraints) (2) and lower-limb devices with balance control.
level 2: task autonomy. the robot is autonomous for specific tasks initiated by a human. the difference from level 1 is that the operator has discrete, rather than continuous, control of the system. an example is surgical suturing (3)—the surgeon indicates where a running suture should be placed, and the robot performs the task autonomously while the surgeon monitors and intervenes as needed.
level 3: conditional autonomy. a system generates task strategies but relies on the human to select from among different strategies or to approve an autonomously selected strategy. this type of surgical robot can perform a task without close oversight. an active lower-limb prosthetic device can sense the wearer's desire to move and adjusts automatically without any direct attention from the wearer.
level 4: high autonomy. the robot can make medical decisions but under the supervision of a qualified doctor. a surgical analogy would be a robotic resident, who performs the surgery under the supervision of an attending surgeon.
level 5: full autonomy (no human needed). this is a "robotic surgeon" that can perform an entire surgery. this can be construed broadly as a system capable of all procedures performed by, say, a general surgeon. a robotic surgeon is currently in the realm of science fiction…" **tradotto letteralmente : *"livello 0: nessuna autonomia. questo livello include robot telecomandati o dispositivi protesici che rispondono e seguono il comando dell'utente. anche un robot chirurgico con ridimensionamento del movimento si adatta a questa categoria perché l'output rappresenta il movimento desiderato dal chirurgo.***

Riprendendo gli esempi fatti in precedenza possiamo ora affermare che il robot Da Vinci[175], che è un sistema non dotato di un software di Intelligenza Artificiale poiché controllato costantemente da remoto dal chirurgo di cui replica in modo stabile e attento i movimenti, si colloca al livello 0 mentre, il Robot Star (Smart Tissue Autonomous Robot) ideato dal gruppo di ingegneri e informatici della Università Johns Hopkins, che nel gennaio 2022 ha eseguito un intero intervento chirurgico su di un maiale senza l'assistenza di un chirurgo umano, si colloca al livello 5.

In tale contesto si può affermare che, per i sistemi che si collocano al livello 0, quale il robot Da Vinci, la responsabilità civile in relazione al malfunzionamento del robot chirurgico che provochi un danno ad un paziente varranno applicati i principi generali e, pertanto, il paziente potrà citare in giudizio esclusivamente il chirurgo ai sensi del 2043 cc se non vi è alcun rapporto contrattuale con il paziente, esclusivamente la struttura sanitaria ai sensi degli artt. 1218[176] e 1228[177] c.c. ovvero entrambi in concorso nel caso in cui non sussista alcun rapporto di subordinazione o di collaborazione tra clinica e sanitario.

Infatti, in tale ultimo caso sussiste comunque un collegamento tra i due contratti stipulati, l'uno tra il medico e il paziente, e l'altro tra il paziente e la casa di cura, contratti aventi a oggetto, il primo, prestazioni di natura professionale medica, comportanti l'obbligo di abile e diligente espletamento dell'attività professionale e, il secondo, avente ad oggetto la prestazione di servizi accessori di natura alberghiera, di natura infermieristica ovvero aventi a oggetto la concessione

livello 1: assistenza robot. il robot fornisce una guida meccanica o assistenza durante un'attività mentre l'essere umano ha il controllo continuo del sistema. gli esempi includono robot chirurgici con dispositivi virtuali (o vincoli attivi) (2) e dispositivi per gli arti inferiori con controllo dell'equilibrio.
livello 2: autonomia dei compiti. il robot è autonomo per compiti specifici avviati da un essere umano. la differenza rispetto al livello 1 è che l'operatore ha un controllo discreto, piuttosto che continuo, del sistema. un esempio è la sutura chirurgica (3): il chirurgo indica dove deve essere posizionata una sutura in esecuzione e il robot esegue il compito in modo autonomo mentre il chirurgo monitora e interviene secondo necessità.
livello 3: autonomia condizionata. un sistema genera strategie di attività ma fa affidamento sull'essere umano per scegliere tra diverse strategie o per approvare una strategia autonomamente selezionata. questo tipo di robot chirurgico può eseguire un'attività senza una stretta supervisione. un dispositivo protesico attivo dell'arto inferiore può percepire il desiderio di chi lo indossa di muoversi e si regola automaticamente senza alcuna attenzione diretta da parte di chi lo indossa.
livello 4: alta autonomia. il robot può prendere decisioni mediche ma sotto la supervisione di un medico qualificato. un'analogia chirurgica sarebbe un residente robotico, che esegue l'intervento chirurgico sotto la supervisione di un chirurgo.
livello 5: piena autonomia (nessun essere umano necessario). questo è un "chirurgo robotico" che può eseguire un intero intervento chirurgico. questo può essere interpretato in senso lato come un sistema capace di tutte le procedure eseguite, diciamo, da un chirurgo generale. un chirurgo robotico è attualmente nel regno della fantascienza..."

[175] il robot DA VINCI è molto utilizzato anche negli ospedali italiani ed impiegato in ambiti quali la chirurgia generale, chirurgia urologica chirurgia ginecologica (con particolare riferimento all'ambito oncologico) chirurgia vascolare e toracica.

[176] Art. 1218ccc "*il debitore che non esegue esattamente la prestazione dovuta e' tenuto al risarcimento del danno, se non prova che l'inadempimento o il ritardo e' stato determinato da impossibilità della prestazione derivante da causa a lui non imputabile*"

[177] Art 1228 Cc: "*salva diversa volontà delle parti, il debitore che nell'adempimento dell'obbligazione si vale dell'opera di terzi, risponde anche dei fatti dolosi o colposi di costoro*"

in godimento di macchinari sanitari, di attrezzi e di strutture edilizie specificamente destinate allo svolgimento di attività terapeutiche e/o chirurgiche[178].

Pertanto, è possibile individuare in capo al nosocomio e al personale medico ivi operante l'esistenza di un dovere di monitoraggio degli strumenti e dei macchinari adottati nell'erogazione della prestazione e tale dovere assume caratteri ancor più stringenti laddove nell'esecuzione dell'intervento il chirurgo si avvalga di un robot, il quale richiede una manutenzione e un controllo meticoloso.

Inoltre, il paziente danneggiato potrà anche invocare la responsabilità del produttore ai sensi degli art. 114 e ss. del Codice del consumo, il quale dispone che: "*Il produttore è responsabile del danno cagionato da difetti del suo prodotto"* e, a differenza del 2043 cc, sarà tenuto a provare il danno e l'esistenza del difetto, nonché il nesso di causalità tra il difetto ed il danno; viceversa, il produttore dovrà provare esclusivamente i fatti che escludono la sua responsabilità[179].

---

[178] Sentenza 13 gennaio 2015 Corte di Cassazione civile n. 280, Normattiva, https://www.normattiva.it ; la quale ha affermato che: " *…la giurisprudenza di questa corte, alla quale il collegio intende dare continuità, pacificamente ritiene che, in via di principio, pur quando manchi un rapporto di subordinazione o di collaborazione tra clinica e sanitario, sussiste comunque un collegamento tra i due contratti stipulati, l'uno tra il medico ed il paziente, e l'altro, tra il paziente e la casa di cura, contratti aventi ad oggetto, il primo, prestazioni di natura professionale medica, comportanti l'obbligo di abile e diligente espletamento dell'attività professionale (e, a volte, anche di raggiungimento di un determinato risultato) e, il secondo, prestazione di servizi accessori di natura alberghiera, di natura infermieristica ovvero aventi ad oggetto la concessione in godimento di macchinari sanitari, di attrezzi e di strutture edilizie specificamente destinate allo svolgimento di attività terapeutiche e/o chirurgiche.*
trattasi di collegamento, per così ontologico, che dal piano fattuale assume inevitabilmente rilevanza su quello giuridico, posto che di norma, l'individuazione della casa di cura dove il medico eseguirà la prestazione promessa costituisce parte fondamentale del contenuto del contratto stipulato tra il paziente e il professionista, nel senso che ciascun medico opera esclusivamente presso determinate cliniche e che, a sua volta, ciascuna casa di cura accetta solo i pazienti curati da determinati medici (confr. cass. civ. 14 giugno 2007, n. 13953). ne deriva che deve ritenersi consustanziale al dovere di diligente espletamento della prestazione l'obbligo del medico di accertarsi preventivamente che la casa di cura dove si appresta a operare sia pienamente idonea, sotto ogni profilo, ad offrire tutto ciò che serve per il sicuro e ottimale espletamento della propria attività; così come, reciprocamente la casa di cura e' obbligata a vigilare che chi si avvale della sua organizzazione sia abilitato all'esercizio della professione medica in generale e, in particolare, al compimento della specifica prestazione di volta in volta richiesta nel caso concreto. e tanto in applicazione del principio generale di cui all'articolo 1228 c.c., il quale comporta che il medico, come ogni debitore, e' responsabile dell'operato dei terzi della cui attività si avvale, così come la struttura risponde non solo dell'inadempimento delle obbligazioni su di essa tout court incombenti, ma anche dell'inadempimento della prestazione svolta dal sanitario, quale ausiliario necessario dell'organizzazione aziendale" (Confr. Cass. Civ. 26 Giugno 2012, N. 10616; Cass. Civ. 6 Giugno 2014, N. 12833; Cass. Civ. 14 Giugno 2007, N. 13953).

[179] AA.VV. I Contratti Del Consumatore, Giuffrè, Milano 2014, pp 1- 1526; Vecchione L., La responsabilità da prodotto difettoso e la garanzia di conformità, Key Editore, 2022 pp. 1- 150; da cui è possibile verificare che la differenza più significativa risiede nel fatto che nel codice del consumo il danneggiato non deve provare l'elemento soggettivo in quanto si tratta di una responsabilità "oggettiva". Inoltre, l'art 118 cod. cons dispone una serie di ipotesi in cui la responsabilità è esclusa:

a) ove il produttore non ha messo il prodotto in circolazione;
b) se il difetto che ha cagionato il danno non esisteva quando il produttore ha messo il prodotto in circolazione;
c) ove il produttore non ha fabbricato il prodotto per la vendita o per qualsiasi altra forma di distribuzione a titolo oneroso, né lo ha fabbricato o distribuito nell'esercizio della sua attività professionale;
d) se il difetto è dovuto alla conformità del prodotto a una norma giuridica imperativa o a un provvedimento vincolante;
e) ove lo stato delle conoscenze scientifiche e tecniche, al momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerare il prodotto come difettoso;
f) nel caso del produttore o fornitore di una parte componente o di una materia prima, se il difetto è interamente dovuto alla concezione del prodotto in cui è stata incorporata la parte o materia prima o alla conformità di questa alle istruzioni date dal produttore che la ha utilizzata.

La complessità dei robot costituiti da un insieme di elementi (i pezzi, i sensori IoT, gli algoritmi) crea, però, seri problemi in fase di applicabilità della normativa in materia di responsabilità del produttore, poiché la catena della responsabilità si potrebbe estendere al programmatore del software-algoritmo, all'assemblatore della macchina e anche a chi ha fornito ed immesso i dati nel robot ove questi siano compromessi o corrotti o comunque non certificati in termini di qualità.

Pertanto, non essendoci una disciplina come quella americana che differenzia la responsabilità per difetto di fabbrica nella quale si prescinde dalla colpa, la responsabilità del programmatore e la responsabilità per carenza di informazioni al consumatore, tale strada, seppur percorribile, diventerebbe molto ostica per il consumatore/danneggiato/paziente.

Viceversa, nel caso in cui venga ipoteticamente impiegato per l'intervento un robot quale Star, che si colloca invece al livello 5, i principi generali vigenti nel nostro ordinamento risulterebbero totalmente inadatti.

la responsabilità extracontrattuale del medico e contrattuale della struttura sanitaria, così come oggi regolata dalla legge Gelli- Bianco imporrebbe al danneggiato, che voglia ottenere un risarcimento a fronte di un danno alla salute causato dal medico che utilizzi gli strumenti dell'IA, rispettivamente, una *probatio diabolica*, per la natura opaca dello strumento utilizzato dal medico che non permette un'agevole individuazione di un nesso di causalità tra fatto e danno, e per quanto attiene alla struttura sanitaria, poiché essa non detiene l'assoluto controllo sul sistema, sarebbe difficile ipotizzare una responsabilità ex art 1218 c.c.[180] ma si dovrebbe piuttosto ipotizzare una possibile responsabilità ex art 2051 cc, che consentirebbe probabilmente di spostare sull'ente ospedaliero il rischio della causa ignota, che verrebbe a coincidere con l'impossibilità a fornire la causa del fortuito.

Fino a qualche anno fa l'utilizzo di robot o sistemi di diagnostica assolutamente indipendenti dal controllo umano sembravano identificare una realtà utopistica mentre, ad oggi, tale realtà sembra sempre più vicina e ne è prova l'esperimento della Università Johns Hopkins con il robot Star.

In tale contesto, l'evoluzione tecnologica in campo di intelligenza artificiale potrebbe scontrarsi con la carenza di normative ad hoc volte a tutelare il paziente umano dal possibile danno alla salute cagionato robot-medico integrato da intelligenze artificiali e totalmente autonomo.

[180] Colletti E., INTELLIGENZA ARTIFICIALE E ATTIVITÀ SANITARIA. PROFILI GIURIDICI DELL'UTILIZZO DELLA ROBOTICA IN MEDICINA, in Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente Vol. XIX 2021 pag. 214

Come analizzato nel primo capitolo, la Commissione Europea su richiesta specifica del Parlamento europeo ha reso nota una proposta di Regolamento ("*Regulation on a European approach for Artificial intelligence*") con l'obiettivo di plasmare la legislazione europea sull'intelligenza artificiale al fine di armonizzarla e caldeggiando l'innovazione, la sicurezza e la tutela dei diritti individuali al fine di individuare soluzioni giuridiche praticabili dinnanzi alla crescita e diffusione dell'utilizzo dei sistemi di IA in tutti i settori e, in particolare, in quello sanitario.

Il possibile adattamento della normativa vigente in materia di prodotto difettoso si rende necessaria poiché quando si analizza la natura del mezzo di IA, va tenuto sempre a mente che mentre l'automa svolge azioni comandate e controllate dell'uomo (cd. machine learning), il sistema di IA autonomo, o con sempre maggior grado di autonomia, è in grado di elaborare in maniera del tutto indipendente i dati che colleziona, e di agire nel contesto che lo circonda mettendo a sistema tali dati.

Pertanto, il comportamento che potrebbe attuare l'IA dopo i vari processi di apprendimento non è conoscibile dall'utilizzatore e neanche dallo stesso produttore o programmatore (cd. deep learning) e le azioni che potrebbero essere compiute sono difficilmente individuabili sia ex post che ex ante, poiché l'operatore può contare sulla relativa certezza del risultato che la macchina porterà a termine, ma non riuscirà ad individuare il "come" di quel procedimento[181].

Da ciò discende che un sistema caratterizzato da complessità, incompletezza, opacità, imprevedibilità, apertura e vulnerabilità[182] mette in crisi gli attuali modelli di responsabilità e, in particolare, quelli che si basano sul criterio di imputazione della colpa e sull'individuazione della stessa ai fini di responsabilità.

Come già anticipato non essendo individuabile il momento effettivo dell'errore o del difetto a causa della caratteristica dell'opacità che contraddistingue le I.A., non c'è modo di rinvenire il nesso di causalità tra fatto e danno e, ciò impedirebbe in concreto il risarcimento del danno.

Per fronteggiare tali problematiche, il Parlamento Europeo ha proposto di attribuire soggettività giuridica allo strumento di IA e alcuni studiosi ritengono praticabile tale possibilità in quanto si potrebbero considerare i robot integranti tecnologia avanzata come persone elettroniche, in grado di risarcire la vittima di qualsiasi danno che essi producano nell'esercizio

[181] Fusaro A., Quale Modello Di Responsabilità Per La Robotica Avanzata? Riflessioni A Margine Del Percorso Europeo, In NGCC, 2020, pag.1344 e ss.
[182] Salanitro U., Intelligenza Artificiale E Responsabilità: La Strategia Della Commissione Europea, In Riv. Dir. Civ., 2020, Pag.1247

delle loro azioni tramite l'istituzione e la dotazione un patrimonio separato, da riservare all'applicazione di IA e al precipuo scopo di risarcire il danno[183].

Aderendo a tale prospettiva, si potrebbe ipotizzare l'introduzione della figura giuridica e professionale del sanitario robotico, anch'esso membro dell'equipe medica con tutte le conseguenze già analizzate in caso di responsabilità, sia civile che penale, del medico umano o robotico membro dell'equipe.

Il tema della "personalità elettronica" evoca un duplice problema: il primo relativo ai doveri ed obblighi dell'Intelligenza Artificiale, ed al sé e come dotarla di personalità al fine di assicurarne la responsabilità diretta, con patrimonio separato, il secondo, attiene, invece, ai "diritti", o quantomeno alle tutele, da accordare all'I.A. medesima, se e quando, con l'autoapprendimento, avrà sviluppato un grado, ed un tipo, di intelligenza (prossima o meno alla "Intelligenza Generale") idonea a renderla meritevole di tutela, se non anche di personalità, secondo la sensibilità e la coscienza sociale nel frattempo maturate[184].

In relazione alla prima questione, alcuni autori ritengono che sia del tutto superfluo riconoscere all' I.A. la soggettività giuridica poiché sarebbe comunque possibile creare un patrimonio destinato da utilizzarsi per il risarcimento del danno commesso dal robot senza che lo stesso acquisisca una personalità giuridica autonoma rispetto a quella dell'operatore sanitario che lo utilizza[185].

In relazione alla seconda questione, essa è stata analizzata dal Professor Ugo Ruffolo in un suo articolo del 2020 intitolato: "*Il problema della "personalità elettronica*"[186], il quale partendo dalla considerazione che la "persona elettronica" potrebbe, sia comunicare che disporre con comunicazione (e "decisione") propria senza mediazioni "umane", ha affermato che il dibattito si dovrebbe focalizzare sulla possibilità o meno di effettuare una qualche equiparazione tra intelligenze artificiali evolute e quelle naturali.

Tuttavia, per raggiungere tale ultimo scopo si dovrebbe abbandonare una concezione antropomorfa e antropocentrica del "pensiero" e della "autocoscienza" e riconoscere la superiorità della capacità di ragionamento deduttivo della macchina rispetto a quello induttivo umano, ragionando pertanto in termini di causalità e non anche per inferenza.

Seppur tale questione è dotata di profili affascinanti che stimolano il ragionamento degli studiosi, lo stesso autore afferma che tali problemi, pur sembrando ancora lontani e astratti, in

[183] Pagallo U., Robotrust And Legal Responsibility, In Know Techn. Pol., Vol. 23, 2010, Pag 367-379;
[184] Ruffolo U. Il Problema Della "Personalità Elettronica", In Journal Of Ethics And Legal Technologies ,Volume 2(1), Aprile 2020 Pag. 76
[185] Finocchiaro G., Responsabilità e intelligenza artificiale, in Contr. e Imp., 2020, 729 ss
[186] Ruffolo U., op. cit. p.96

concreto non lo sono poiché taluni aspetti ad essi connessi sono già attuali e gli studi in ambito medico-chirurgico ne sono la prova.

3.3 Responsabilità civile in caso di violazione dei dati sanitari: le nuove frontiere dell'I.A e la lotta alla diffusione del covid-19

La responsabilità civile in ambito medico viene in rilievo anche quando occorre conciliare il diritto alla riservatezza sulle informazioni personali sanitarie con il diritto alla salute, il che richiede da parte degli operatori sanitari, da un lato, un'organizzazione efficiente e razionale delle informazioni concernenti l'anamnesi clinica personale dei pazienti, e dall'altro, la possibilità di intervenire tempestivamente con la prestazione medica.

I dati sanitari sono per loro natura dati sensibilissimi e il loro trattamento può rendere ostensibile lo stato di salute del soggetto e il GDPR, in chiave protettiva, richiede per il loro trattamento che vi sia il consenso preventivo del soggetto al quale le informazioni ineriscono, quando il trattamento riguardi dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato ovvero l' autorizzazione del Garante, se la finalità di tutela della salute riguarda un terzo o la collettività.

Il GDPR prevede che il consenso sia reso senza ritardo, successivamente alla prestazione medica di cui benefici tanto il titolare dei dati, quanto eventuali terzi, nelle situazioni di emergenza individuate all'art. 82 dello stesso, configurando un regime «attenuato» di esercizio del diritto alla protezione sui propri dati sanitari, legato alla sussistenza e al perdurare di una situazione di emergenza.

La necessità di bilanciare il diritto alla riservatezza del soggetto sui suoi dati sensibili sanitari con l'esigenza di conoscenza di tali dati da parte degli organismi preposti alla tutela sostanziale del diritto alla salute è stata avvertita, sia in Italia che nel resto del mondo, in occasione dello scoppio della pandemia Covid-19 e soprattutto a seguito della decisione di molti Stati di introdurre dei sistemi di contact tracing per contenere la diffusione dei contagi.

I sistemi sopra citati sono stati essenzialmente sviluppati tenendo conto della raccomandazione della Commissione in relazione all'impiego di app a sostegno della lotta alla pandemia di covid-19 (2020/C 124 I/01)[187].

La raccomandazione in esame riconosce che le applicazioni mobili di tracciamento potrebbero essere utili sia alle autorità che agli organismi operanti nel settore sanitario per orientare la loro attività di ricerca, di prevenzione, di monitoraggio, di prognosi, di trattamento

[187] Commissione Europea, COMUNICAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=DE (20 agosto 2022)

o di attenuazione delle malattie, agevolando in questo modo anche lo scambio di informazioni tra di essi.

Inoltre, la Commissione delinea un itinerario strategico per l'adozione, a livello europeo, di un pacchetto di misure (c.d "*Toolbox of practical measures*") che siano idonee a fronteggiare efficacemente (dal punto vista medico e tecnico) la situazione di emergenza e che saranno costantemente integrate dagli orientamenti della Commissione stessa alla luce delle soluzioni, delle questioni e dei suggerimenti prospettati nel tempo dai singoli Stati membri.

La raccomandazione in esame indica i principi ai quali l'intero processo di sviluppo della 'Toolbox' e l'utilizzo delle tecnologie e dei dati dovranno ispirarsi, primo tra questi il lecito trattamento dei dati personali e, in particolare, le misure adatte dagli Stati memebri dovranno garantire, senza eccezione alcuna, il rispetto dei diritti fondamentali e delle norme sulla riservatezza delle comunicazioni e sulla protezione dei dati personali e prevenire il rischio di stigmatizzazioni; inoltre, dovranno essere trattati dati di prossimità garantendo la loro forma anonima e aggregata e, solo in caso di rilevata positività al virus questi verranno trattati e condivisi per informare con modalità appropriate le persone entrate in contatto con la persona infetta, pur sempre garantendo loro l'anonimato.

La Commissione ritiene fondamentale il fatto che i dati personali siano trattati per il periodo di tempo strettamente necessario a combattere l'emergenza del sanitaria Covid- 19 e, per raggiungere tale fine, gli Stati membri potranno utilizzare i dati raccolti solo ed esclusivamente per questa finalità e, inoltre, dovranno verificare costantemente la necessità del trattamento ovvero la sua cessazione.

Compito degli Stati membri, dunque, sarà quello di individuare misure idonee a garantire l'eliminazione dei dati non più necessari con la sola eccezione che i dati raccolti abbiano un valore scientifico di pubblico interesse e a patto che la tutela di quest'ultimo non comprometta la tutela dei diritti fondamentali degli individui e ciò in linea con le disposizioni del GDPR.

Altri principi indispensabili attengono al fatto di adottare tutte le misure necessarie per impedire la reversibilità della anonimizzazione dei dati e dunque la riferibilità degli stessi ai singoli individui e le applicazioni dovranno soddisfare i requisiti informatici e tecnici per le tecnologie impiegate (ad esempio il Bluetooth Low Energy, che ha un raggio di azione limitato a pochi metri) e garantire la crittografia dei dati di prossimità raccolti e la conservazione degli stessi con alti livelli di sicurezza esclusivamente all'interno dei dispositivi mobili, nonché regolare l'accesso alla tecnologia, se necessario e al ricorrere di determinate condizioni, delle autorità sanitarie.

I principi elaborati da parte della Commissione Europea sono espressione dei più generali criteri di necessità, proporzionalità e adeguatezza dai quali le misure in discussione non possono in alcun caso discostarsi, sebbene il presupposto di liceità di queste ultime coincida con esigenze di sanità pubblica.

Le linee giuda sopra menzionate seppur coerenti con l'impianto codicistico del GDPR sono state attuate esclusivamente dai paesi europei mentre, come vedremo più avanti, le tutele che l'Europa considera minime per il rispetto delle libertà fondamentali vengono totalmente pretermesse in altre parti del mondo.

3.3.1. Il nuovo scenario della profilazione dei dati inerenti alla salute alla luce del Gdpr e della raccomandazione della Commissione Europea

In un recentissimo intervento del febbraio 2022 il Presidente del Garante per la protezione dei dati personali Pasquale Stanzione ha affermato: "*La pandemia ha dimostrato, emblematicamente, quanto stretto possa essere il legame tra salute (anche nella sua declinazione metaindividuale di sanità pubblica), privacy e digitale. Se il distanziamento fisico non è divenuto anche sociale lo dobbiamo, infatti, alla "potenza geometrica delle nuove tecnologie che hanno consentito di ricreare nello spazio virtuale persino il più fisico dei rapporti, ovvero quello tra medico e paziente, grazie alla telemedicina, ai consulti on-line, all'intelligenza artificiale, all'e-health più in generale. Nulla più della pandemia ha reso, dunque, evidente la duplice dimensione del diritto alla salute, quale prerogativa individuale ma anche interesse collettivo, da salvaguardare anche mediante un flusso informatico costante e capillare sulla condizione epidemica di ciascuno. Emerge, dunque, in maniera quantomai inequivoca la tensione che caratterizza i dati sanitari, meritevoli da un lato della massima protezione e riservatezza e, dall'altro, di una (sia pur circoscritta e calibrata) circolazione per esigenze di sanità pubblica.*[188]*"*.

Lo stralcio dell'intervento in esame mette in luce tutte le problematiche che si presentano nel passaggio dalla cd. "Società dell'informazione alla c.d. Società algoritmica[189]", ossia quella società in cui alla centralità dell'informazione si accompagna quella degli algoritmi eseguiti dai software che, in qualsiasi modo, elaborano o comunque adoperano l'informazione medesima, organizzando la società sulla base dei processi decisionali svolti da algoritmi, robot e agenti intelligenti[190], i quali costituiscono il principale intermediario per l'esercizio del potere.

[188] Presidente del Garante per la protezione dei dati personali, Sicurezza del dato sanitario e condivisione Intervento di Pasquale Stanzione, in Panorama, 18 febbraio 2022 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9747071 ; (21 agosto 2022)

[189] 13. Balkin, J., "The Three Laws of Robotics in the Age of Big Data", in Ohio State Law Journal, 78(5), 2017, pp. 1217-1241.

[190] Schuilenburg M., Peeters, R., The Algorithmic Society. Technology, Power, and Knowledge. Routledge, Londra 2021, pp. 1-214

Come già analizzato nel secondo capitolo, la prima compiuta concettualizzazione del diritto alla privacy si deve ai giuristi statunitensi, Samuel D. Warren e Louis D. Brandeis, i quali lo hanno teorizzato quale *right to be let alone* che tratteggia la sfera negativa della riservatezza, consistente nella pretesa di non subire ingerenze nel proprio ambito privato.

Accanto a tale visione negativa si è progressivamente affiancata la valorizzazione di una sfera positiva, consistente invece nella pretesa di controllo sui propri dati personali e che hanno fatto emergere un diritto sempre più finalizzato a rendere possibile la libera costruzione della personalità, l'autonomo strutturarsi dell'identità, la proiezione nella sfera privata dei principi fondamentali della democrazia[191].

Questa linea evolutiva ha trovato riscontro nella legislazione positiva dell'Unione Europea degli ultimi decenni (es. la direttiva 95/46/CE, seguita dal Regolamento (UE) 679/2016 General Data Protection Regulation, GDPR, o Regolamento Generale sulla Protezione dei Dati, RGPD) avente ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione all'interno dell'Unione Europea, al fine di evitare che il trattamento possa comunque comportare rischi per la libertà, la dignità e altri diritti.

Tuttavia, seppur in prima approssimazione la disciplina europea appare rigida e completa, in realtà nella Società algoritmica in cui la raccolta dei dati è certamente centrale, appare ormai desueta, poiché tale tipo di società, così come è stata teorizzata, è caratterizzata dall'elaborazione automatizzata, soprattutto su larga scala (cd. *Big Data*), che consente altresì l'automazione dei processi decisionali.

In dottrina, gli studi in materia di privacy e consenso[192] dimostrano la sussistenza di un divario fra l'attitudine a livello generale delle persone e la loro condotta concreta, configurando quello che a livello generale viene definito "*il paradosso della privacy"*, secondo cui le persone anche se pubblicamente dichiarano di attribuire una elevata importanza alla propria privacy, sono pronte a comunicare anche dati sensibili per piccoli sconti ovvero benefici minimi.

In tali contesti, l'impianto così come elaborato dal GDPR risulta non adattabile alla cosiddetta Società algoritmica in quanto, come già analizzato, il fulcro del Regolamento UE è il consenso informato dell'interessato, fornito sulla base delle finalità comunicate prima ancora che il trattamento abbia inizio mentre, nella società algoritmica i Big Data vengono spesso

[191] Rodotà, S., Il diritto di avere diritti, Laterza, Roma-Bari, 2012 pp. 1-444

[192] Casciaro G., Santise P., il consenso informato, Giuffrè Editore, Milano 2012 pp.1-390; Scagliarini S., La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio, Aracne, 2013 pp. 1-256; D'Acquisto G., Naldi M., Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza. Con Contenuto digitale per download e accesso on line (I diritti nella «rete» della rete), Giappichelli Editore, Torino 2017 pp.1-228 ed altri.

trattati con scopi definiti solo in termini generali e le finalità reali non vengono individuate e comunicate all'inizio del trattamento.

In ambito sanitario i dati che rilevano sono quelli inerenti alla salute (cd. dati sanitari[193]), i quali per espressa previsione legislativa non possono essere trattati, salvo particolari eccezioni previste dalla stessa norma[194] quali ad esempio motivi di interesse pubblico nel settore della sanità pubblica, come "la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici" e, in caso di violazione, l'art 83 GDPR prevede un severo regime sanzionatorio (sanzioni sino a venti milioni di euro o sino al quattro per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

Nel contesto sanitario una delle più grandi preoccupazioni attiene alla profilazione automatizzata delle persone fisiche svolta dai sistemi informatici poiché, essa costituisce al contempo una opportunità, in quanto consente di offrire prodotti e servizi sempre più personalizzati nell'ambito del mercato, ma anche un elevato rischio che consiste sostanzialmente nella creazione di profili utente che assegnano vere e proprie rappresentazioni digitali dell'identità che non tengono in considerazione la persona in quanto tale ma solo della sua profilazione.

Il fenomeno della profilazione tocca sempre più anche la sfera della salute sia per ciò che concerne la fornitura di servizi e prestazioni sanitarie in senso stretto, ivi inclusa la pratica clinica, sia in relazione a prodotti e servizi che, in un modo o nell'altro, incidono sull'ambito della salute ed effettuano trattamenti di dati sanitari, come, ad esempio, i diversi dispositivi indossabili quali gli smartwatch dotati di pulsossimetro o in grado di effettuare un elettrocardiogramma (i cui dati vengono poi sovente elaborati o memorizzati in cloud)[195].

[193] dell'art. 4 GDPR, per dati relativi alla salute si intendono "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute".

[194] l'art. 9, par. 1, GDPR dispone il divieto di " trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Infine, l'art. 9, par. 2, GDPR prevede diverse eccezioni al divieto appena menzionato, fra cui possono qui ricordarsi: il consenso; il rispetto della normativa in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; l'interesse vitale dell'interessato o di altra persona fisica; i dati resi manifestamente pubblici dall'interessato; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o l'esercizio di funzione giurisdizionale da parte di un'autorità giurisdizionale; i motivi di interesse pubblico se proporzionali rispetto alla finalità perseguita; la finalità di medicina preventiva o del lavoro o di valutazione della capacità lavorativa del dipendente, nonché la diagnosi, l'assistenza o terapia sanitaria o sociale, la gestione di sistemi e servizi sanitari o sociali (sulla base del diritto dell'Unione europea o nazionale o di un contratto con professionista della sanità); i motivi di interesse pubblico
nel settore della sanità pubblica, come "la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici".

[195] Fioriglio G., La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici, in Journal of Ethics and Legal Technologies, Volume 3, November 2021

L'identità digitale delle persone fisiche si è evoluta anche grazie alla c.d sanità digitale (sanità elettronica, eHealth), che consiste nell'impiego delle nuove tecnologie nel dominio sanitario al fine di migliorare l'accesso degli utenti all'assistenza medica, ridurre il rischio clinico, implementare l'efficacia e la sicurezza delle prestazioni erogate dal Servizio Sanitario Nazionale (SSN) ed intervenire sulle diseconomie della spesa sanitaria pubblica[196].

In Italia già con la Legge Stanca, l. n. 4 del 2004, il legislatore aveva gettato le basi normative per il riconoscimento del "diritto di accesso individuale alle tecnologie" quale diritto sociale strumentale al godimento delle libertà fondamentali a cui è susseguita una notevole proliferazione legislativa ed è stata creata anche la c.d. Amministrazione Digitale di cui, in materia sanitaria, la novella più rilevante è costituita dal c.d. Decreto Semplificazione del 2012 (d.l. n. 5 del 2012) reso operativo attraverso le misure attuative previste dal c.d. Decreto Crescita 2.0 (d.l. n. 179/2012), che ha avuto lo scopo di modernizzazione i rapporti tra pubblica amministrazione, cittadini ed imprese[197].

Con il decreto sopra citato sono stati introdotti nel sistema italiano quelli che sono stati definiti gli strumenti nevralgici del sistema di sanità digitale italiana, ossia il fascicolo sanitario elettronico (FSE) di cui all'art. 1226, la prescrizione medica digitale (c.d. ricetta dematerializzata) e la cartella clinica elettronica (CCE) ex art. 13 del d.l. n. 179 /2012[198].

---

[196] PIOGGIA A., La sanità italiana di fronte alla pandemia. Un banco di prova che offre una lezione per il futuro, in Dir. pubbl., 2020, 385 ss

[197] CARLONI E., Digitalizzazione e riforma dell'amministrazione: la nuova agenda, in Mastragostino F., Piperata G., Tubertini C. (a cura di), L'amministrazione che cambia. Fonti, regole e percorsi di una nuova stagione di riforme, in Quaderni della Spisa, Bologna, 2016, 267 ss

[198] Art. 13 Prescrizione medica e cartella clinica digitale: *1. Al fine di migliorare i servizi ai cittadini e rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerando la sostituzione delle prescrizioni mediche di farmaceutica e specialistica a carico del Servizio sanitario nazionale-SSN in formato cartaceo con le prescrizioni in formato elettronico, generate secondo le modalita' di cui al decreto del Ministero dell'economia e delle finanze in data 2 novembre 2011, pubblicato nella Gazzetta Ufficiale n. 264 del 12 novembre 2011, concernente la dematerializzazione della ricetta cartacea di cui all'articolo 11, comma 16, del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122, le regioni e le province autonome, entro 6 mesi dalla data di entrata in vigore del presente decreto-legge, provvedono alla graduale sostituzione delle prescrizioni in formato cartaceo con le equivalenti in formato elettronico, in percentuali che, in ogni caso, non dovranno risultare inferiori al 60 percento nel 2013, all'80 percento nel 2014 e ((al 90 per cento nel 2016)).*

2. Dal 1° gennaio 2014, le prescrizioni farmaceutiche generate in formato elettronico sono valide su tutto il territorio nazionale nel rispetto delle disposizioni che regolano i rapporti economici tra le regioni, le ASL e le strutture convenzionate che erogano prestazioni sanitarie, fatto salvo l'obbligo di compensazione tra regioni del rimborso di prescrizioni farmaceutiche relative a cittadini di regioni diverse da quelle di residenza. Con decreto del Ministro della salute, di concerto con il Ministro dell'economia e delle finanze, d'intesa con la Conferenza permanente per i rapporti Stato regioni e le province autonome di Trento e di Bolzano, sono definite le modalità di attuazione del presente comma. 3. I medici interessati dalle disposizioni organizzative delle regioni e delle province autonome di cui al comma 1, rilasciano le prescrizioni di farmaceutica e specialistica esclusivamente in formato elettronico. L'inosservanza di tale obbligo comporta l'applicazione di quanto previsto dall'articolo 55-septies, comma 4, del decreto legislativo 30 marzo 2001, n. 165. 3-bis. Al comma 4 dell'articolo 55-septies del decreto legislativo 30 marzo 2001, n.165, sono aggiunti i seguenti periodi: "Affinché' si configuri l'ipotesi di illecito disciplinare devono ricorrere sia l'elemento oggettivo dell'inosservanza all'obbligo di trasmissione, sia l'elemento soggettivo del dolo o della colpa. Le sanzioni sono applicate secondo criteri di gradualità e proporzionalità, secondo le previsioni degli accordi e dei contratti collettivi di riferimento". 4. Dal 1° gennaio 2014, il sistema per la tracciabilità delle confezioni dei farmaci erogate dal SSN basato su fustelle cartacee e' integrato, ai fini del rimborso delle quote a carico del SSN, da sistema basato su tecnologie digitali, secondo modalità stabilite con provvedimento dirigenziale del Ministero dell'economia e delle finanze, pubblicato nella Gazzetta Ufficiale, e rese note sul

Tuttavia, l'ambito della salute, inteso nel suo complesso, non riguarda solo quello medico-sanitario in senso stretto, e dunque le attività svolte dai professionisti e dagli operatori sanitari individualmente e/o nelle strutture sanitarie ma anche la l'evoluzione delle pratiche e degli studi sulla telemedicina[199] che hanno alimentato l'offerta di servizi e prodotti, anche altamente tecnologici, prima riservati esclusivamente agli operatori professionali.

In tale scenario si inserisce l'applicazione "Immuni" introdotta nel nostro ordinamento con art. 6, comma 1°, d.l. 30.4.2020, n. 28, convertito in l. 25.6.2020, n.70[200], consistente in un sistema di contact tracing volto a contenere la diffusione dei contagi da Covid-19.

---

sito del sistema informativo del progetto «Tessera sanitaria», di cui all'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e nel rispetto di quanto previsto dal Sistema di tracciabilità del farmaco del Ministero della salute. Resta fermo quanto previsto dal comma 8 dell'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326,in ordine ai soggetti abilitati alla trasmissione dei dati. 5. All'articolo 47-bis del decreto-legge 9 febbraio 2012, n. 5 convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35, dopo il comma 1 sono aggiunti in fine i seguenti: «1-bis. A decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche può essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche solo in forma digitale, nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82, e dal decreto legislativo 30 giugno 2003, n. 196. 1-ter. Le disposizioni del presente articolo si applicano anche alle strutture sanitarie private accreditate.».

[199] Magalini S., Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A , Enciclopedia Italiana - V Appendice (1995) Telemedicina, https://www.treccani.it/enciclopedia/telemedicina_%28Enciclopedia-Italiana%29/#:~:text=La%20t.,ove%20essi%20sono%20rispettivamente%20situati., (25 agosto 2022): Particolare applicazione della telematica che consente di inviare a distanza, utilizzando varie vie di comunicazione (collegamenti telefonici e radiofonici, satelliti, ecc.), più comunem. le linee telefoniche, informazioni di carattere sanitario (tracciati di elettrocardiogrammi, radiografie, ecografie, misure di temperatura e pressione arteriosa, cartelle cliniche) per rendere l'assistenza medica più rapida ed efficiente.

[200] Art. 6 : Sistema di allerta Covid-19: Al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanita' pubblica legate all'emergenza COVID-19, e' istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile. Il Ministero della salute, in qualita' di titolare del trattamento, si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, con i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e con i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonche' con l'Istituto superiore di sanita' e, anche per il tramite del Sistema Tessera Sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanita' pubblica e di cura. Le modalita' operative del sistema di allerta tramite la piattaforma informatica di cui al presente comma sono complementari alle ordinarie modalita' in uso nell'ambito del Servizio sanitario nazionale. Il Ministro della salute e il Ministro per gli affari regionali e le autonomie informano periodicamente la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano sullo stato di avanzamento del progetto.
2. Il Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'articolo 35 del Regolamento (UE) 2016/679, adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le liberta' degli interessati, sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 36, paragrafo 5, del medesimo Regolamento (UE) 2016/679 e dell'articolo 2-quinquiesdecies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, assicurando, in particolare, che: a) gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalita' e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati; b) per impostazione predefinita, in conformita' all'articolo 25 del Regolamento (UE) 2016/679, i dati personali raccolti dall'applicazione di cui al comma 1 siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, individuati secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonche' ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti; c) il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimita' dei dispositivi, resi anonimi oppure, ove cio' non sia possibile, pseudonimizzati; e' esclusa in ogni caso la geolocalizzazione dei singoli utenti; d)

3.3.2 L'utilizzo dei Big Data in italia per contrastare la diffusione del covid -19: "L'app. Immuni"

L'anno 2020 sarà ricordato come l'anno della pandemia COVID-19: il 31 dicembre 2019 è stato segnalato un gruppo di casi di polmonite a Wuhan, in Cina e poche settimane dopo è stata confermata la trasmissione da uomo a uomo.

Entro la fine di gennaio 2020, l'Organizzazione Mondiale della Sanità ha segnalato 7818 casi confermati in 18 paesi, con la maggioranza in Cina e l'infezione si è diffusa rapidamente in tutto il mondo, con un ampio focolaio precoce in Italia e, alla fine del 2020 c'erano stati 85 milioni di casi confermati, 1,8 milioni di morti e al fine di contrastare la diffusione del virus i Governi di tutto il mondo hanno introdotto divieti di movimento e distanziamento sociale senza precedenti**.**

Oltre alle misure di restrizione fisica sopra citate, gli Stati hanno elaborato nuove strategie di prevenzione utilizzando i sistemi di intelligenza artificiale che hanno avuto la funzione di trattare i Big Data al fine di controllare l'espansione della pandemia.

Sebbene il d.lgs. 196/2003 non sia stato del tutto abrogato dal GDPR (Reg. UE n. 679/16), in nessuna di queste fonti si rinviene un'accurata disciplina in materia di Big Data, poiché, entrambe, si occupano prevalentemente del trattamento del dato personale e della corretta autodeterminazione del singolo, che deve fornire il proprio consenso al trattamento del dato[201].

siano garantite su base permanente la riservatezza, l'integrita', la disponibilita' e la resilienza dei sistemi e dei servizi di trattamento nonche' misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento; e) i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata e' stabilita dal Ministero della salute e specificata nell'ambito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine; f) i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 possano essere esercitati anche con modalita' semplificate. 3. I dati raccolti attraverso l'applicazione di cui al comma 1 non possono essere trattati per finalita' diverse da quella di cui al medesimo comma 1, salva la possibilita' di utilizzo in forma aggregata o comunque anonima, per soli fini di sanita' pubblica, profilassi, statistici o di ricerca scientifica, ai sensi degli articoli 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679. 4. Il mancato utilizzo dell'applicazione di cui al comma 1 non comporta alcuna conseguenza pregiudizievole ed e' assicurato il rispetto del principio di parita' di trattamento. 5. La piattaforma di cui al comma 1 e' di titolarita' pubblica ed e' realizzata dal Commissario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite dalla societa' di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. I programmi informatici di titolarita' pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione di cui al medesimo comma 1 sono resi disponibili e rilasciati sotto licenza aperta ai sensi dell'articolo 69 del decreto legislativo 7 marzo 2005, n. 82. 6. L'utilizzo dell'applicazione e della piattaforma, nonché' ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi.

[201] CINQUE ALBA, Privacy, Big-Data E Contact Tracing: Il Delicato Equilibrio Fra Diritto Alla Riservatezza Ed Esigenze Di Tutela Della Salute, in La Nuova Giurisprudenza Civile Commentata, n. 4, 1 luglio 2021, p. 957, Wolters Kluwer S.p.A.

Neanche con il diffondersi della pandemia Covid 19 e con l'introduzione nel giugno 2020 dell'applicazione "Immuni", il legislatore si è occupato di delineare gli aspetti fondamentali della regolamentazione dell'uso dei Big Data e ciò ha prodotto un vero e proprio dibattito in relazione alla possibile violazione del diritto alla privacy e al trattamento dei dati personali sanitari.

Nella prima fase, infatti, il legislatore con Decreto-legge 14/2020, recante "*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19*", ha introdotto, all'art. 14, alcune semplificazioni per il trattamento di dati personali, ossia quelle che risultino necessari all'espletamento delle varie funzioni, sanitarie e non, attribuite nell'ambito dell'emergenza determinata dal diffondersi del COVID-19 da parte dei soggetti pubblici operanti nel Servizio nazionale di protezione civile, degli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, oltre che delle strutture pubbliche e private operanti nell'ambito del Servizio sanitario nazionale[202].

Successivamente, è stato emanato il decreto-legge 30 aprile 2020, n.28, recante "*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni etc*.", in cui si stabiliva che l'applicazione per il tracciamento dei contagi scelta dal Governo italiano avrebbe potuto essere acquisita, su base volontaria e gratuitamente, direttamente sui dispositivi Android ed Apple.

Prima di capire se le regole di responsabilità ad oggi delineate dalla normativa europea in materia di dati personali siano sufficienti a tutelare i diritti dei cittadini contro applicazioni di contact tracing che sono capaci di trattare i Big Data, occorrerà in primo luogo analizzare l'art. 6, comma 1°, d.l. 30.4.2020, n. 28, convertito in l. 25.6.2020, n.70, che ha introdotto tale nuova tecnologia nella lotta contro la diffusione dei contagi da Covid-19.

L'applicazione Immuni consiste in un'applicazione che può essere installata volontariamente su smartphone che permette di individuare tutti i soggetti con cui un individuo positivo al Covid-19 ha avuto contatti[203]e utilizza la tecnologia contact tracing via Bluetooth., e ciò perché la localizzazione tramite GPS è stata ritenuta troppo invasiva dalle linee giuda europee[204].

[202] Fontana M. La Minaccia Di Erosione Del Diritto Alla Riservatezza Ai Tempi Del Covid-19: La Reazione All'emergenza, In Teaching European Law And Life Sciences (Biotell) A.A. 2019-2020, Organizzato All'interno Del Modulo Jean Monnet "Biolaw: Teaching European Law And Life Sciences (Biotell)", Coordinato Presso L'università Di Trento Dai Docenti Carlo Casonato E Simone Penasa

[203] Camardi C., Tabarrini C., Contact Tracing Ed Emergenza Sanitaria. "Ordinario" E "Straordinario" Nella Disciplina Del Diritto Al Controllo Dei Dati Personali, In "Nuova Giurisprudenza Civile Commentata", 3, 2020, P. 32; Cuffaro V., D'orazio R, La Protezione Dei Dati Personali Ai Tempi Dell'epidemia, In "Corriere Giuridico", 6, 2020, P. 729; Corso S., Il Fascicolo Sanitario Elettronico Fra E-Health, Privacy Ed Emergenza Sanitaria, In "Responsabilità Medica", 4, 2020.;

[204] Finocchiaro G., Il Punto Sull'app Immuni: Bilanciamento Tra Diritti, In Medialaws.Eu, 09 Giugno 2020

L'applicazione nello specifico si fonda sulla tecnologia Bluetooth Low Energy[205] capace di mantenere i dati dell'utente sul dispositivo stesso, attribuendogli un codice identificativo temporaneo che varia costantemente e viene scambiato appunto via Bluetooth coi dispositivi vicini, i quali conservano in memoria le informazioni degli altri cellulari con cui sono entrati in contatto nella forma di codici anonimi crittografati; a questi sono poi associati dei "metadati che valutano il rischio di contagio, quest'ultima fase viene svolta localmente, direttamente sul singolo dispositivo[206].

Pertanto, nel caso in cui un soggetto che abbia scaricato l'applicazione e risulti essere positivo all'infezione gli verrà assegnato un codice di autorizzazione con il quale lo stesso potrà caricare su un server ministeriale il proprio codice anonimo, che tramite il server verrà poi ricavato dai dispositivi attraverso l'applicazione e, nel caso in cui, "Immuni" rilevi tra i codici nel proprio database il codice di un plausibile contagiato, ne invierà una notifica all'utente di quel dispositivo e anche al server dei sanitari, gestito dal ministero della Salute, ma con informazioni pseudonimizzate.

La cifratura e la pseudonomizzazione sono elementi importanti al fine di garantire la massima sicurezza e riservatezza e, inoltre, l'applicazione in esame utilizza un sistema decentralizzato e l'immissione di dati nel sistema è subordinato ad una scelta del tutto volontaria della persona contagiata.

Prima dell'emanazione dell' art. 1, lett. f), d.p.c.m. 18.10.2020, che ha modificato l' art. 3, comma 1°, d.p.c.m. 13.10.2020, non sussisteva l'obbligo in capo all'operatore sanitario, di assistere il paziente risultato positivo al Covid-19 nell'inserimento del codice chiave all'interno della piattaforma di contact tracing: il dato veniva caricato nella sezione inserimento dati l'app e quest'ultima generava un codice che veniva comunicato all'operatore sanitario e, quest'ultimo, doveva inviare il codice al centro dati.

In tutta questa operazione il paziente aveva circa due minuti per selezionare il tasto "verifica", consentendo all'applicazione di confermare la corrispondenza del codice inserito dall'utente e quello inserito dall'operatore sanitario e tale operazione permetteva all'applicazione di ricollegarsi alle chiavi identificative dell'utente consentendo al sistema di

[205] Ibidem: Il Bluetooth Low Energy (Bluetooth Le) è una tecnologia wireless personal area network progettata e commercializzata dal bluetooth special interest group (bluetooth sig) per nuove applicazioni nel settore dell'assistenza sanitaria, fitness, per la sicurezza, per l'industria dell'intrattenimento domestico e per le industrie automobilistiche e dell'automazione. rispetto al bluetooth "classico", il bluetooth low energy ha lo scopo di fornire un consumo energetico e un costo notevolmente ridotto, mantenendo un intervallo di comunicazione simile.

[206] FONTANA M., op cit. p. 111

inviare una notifica a tutti i soggetti venuti in contatto con quelle particolari chiavi identificative.

Il 1° giugno 2020 il Garante per la protezione dei dati personali ha autorizzato il Ministero della salute ad avviare il trattamento relativo al Sistema di allerta Covid-19 (app "Immuni") ed ha emanato una serie di misure volte a rafforzare la sicurezza dei dati delle persone che utilizzeranno l'applicazione; in particolare, il Garante ha richiesto che gli utenti siano informati adeguatamente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio e in merito alla previsione di poter di disattivare temporaneamente l'applicazione attraverso una funzione facilmente accessibile nella schermata principale.

Il Garante ha richiesto, inoltre, che i dati raccolti attraverso il sistema di allerta non possano essere trattati per finalità non previste dalla norma che istituisce l'app e il Governo dovrà anche essere garantita la trasparenza del trattamento a fini statistico-epidemiologici dei dati raccolti ed individuate le modalità più adeguate al fine proteggerli, evitando ogni forma di riassociazione a soggetti identificabili e adottando idonee misure di sicurezza e tecniche di anonimizzazione.

Il Garante , infine, ha specificato che il legislatore dovrà introdurre delle misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati ed ha sottolineato che il trattamento di dati personali raccolti attraverso la applicazione Immuni, da parte di soggetti non autorizzati, può determinare un trattamento di dati personali illecito, [207] cosi come affermato dal Comitato europeo per la protezione dei dati nella "Dichiarazione sul trattamento dei dati nel contesto dell'epidemia da Covid-19" del 19 marzo 2020 da parte dell'UE, la quale ha affermato che l'adozione di misure incidenti sul diritto alla vita personale e alla riservatezza è subordinata al rispetto delle disposizioni in materia di protezione dei dati, tra cui, in particolare, il GDPR e [208]la Direttiva e-privacy 2002/58/CE del Parlamento europeo e del Consiglio (c.d. Direttiva e-privacy), come modificata dalla Direttiva 2009/136/CE, che disciplina il trattamento dei dati personali e della vita privata nel settore delle telecomunicazioni.

Nel comunicato stampa del 10 agosto 2020, inerente alla proliferazione delle applicazioni di contact tracing da parte di istituzioni pubbliche e soggetti privati, il Garante ha fatto un espresso monito al legislatore, ricordando che l'emergenza COVID-19 non rappresenta

[207] Presidente del Garante per la protezione dei dati personali ,App "Immuni": via libera del Garante privacy, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356588 , (28 agosto 2022)
[208] Jelinek A., Dichiarazione sul trattamento dei dati nel contesto dell'epidemia di Covid-19 del 19 marzo 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_it_1.pdf. , (28 agosto 2022)

automaticamente, e di per sé, una base giuridica sufficiente volta a incidere su diritti e libertà costituzionalmente protette, legittimando trattamenti di dati particolarmente invasivi, quali appunto quelli atti a consentire il tracciamento dei contatti da parte di qualsiasi titolare pubblico o privato e, al contempo, ha ribadito che: *'' gli unici trattamenti di dati personali che, allo stato, possano vantare un'adeguata base giuridica, sono esclusivamente quelli che trovano il proprio fondamento in una norma di legge nazionale. Ogni altro trattamento finalizzato al contact tracing risulta pertanto privo di un'adeguata fonte giuridica legittimante e, pertanto, effettuato in violazione della normativa europea e nazionale in materia di protezione dei dati personali*[209] *''*.

Le criticità derivanti dal raccordo tra la normativa in materia di tutela della riservatezza e l'utilizzo di tecnologie basate sul tracciamento dei movimenti degli individui o sui dati sanitari, con particolare riguardo alle applicazioni di contact tracing, ha di fatto ridotto il c.d. nucleo duro della Costituzione e, pertanto, le misure compressive sarebbero costituzionalmente lecite solo se rispettose dei principi di necessità, proporzionalità, adeguatezza e idoneità.

La maggior parte degli autori che si sono interrogati sul punto, hanno analizzato la questione alla luce del c.d. principio di precauzione[210], il quale opera allorquando sussista incertezza in merito alla soluzione di questioni scientifiche complesse e dibattute in dottrina, imponendo l'adozione delle misure necessarie a tutelare la vita, la salute e l'ambiente nel caso in cui vi sia il dubbio, suffragato dall'incertezza scientifica, che tali beni possano essere compromessi[211].

Il principio di precauzione va tenuto distinto dal principio di prevenzione, che opera, invece, allorquando il livello di conoscenza scientifica non sia connotato dall'incertezza e sia possibile individuare con sufficiente precisione sia il rischio sia il possibile danno e, inoltre, il principio di precauzione si trova alla base della Parte IV del Codice del Consumo, che disciplina la normativa in materia di sicurezza e qualità dei prodotti anche se alcuni autori hanno riconosciuto la sua valenza applicativa anche in ambito contrattuale[212].

---

[209] Presidente del Garante per la protezione dei dati personali, Garante privacy su proliferazione app di contact tracing. Violano la privacy i trattamenti non coperti dalla normativa nazionale, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9447462 , (28 agosto 2022)

[210] 90. SANTISE M., Principio di precauzione e tecniche di gestione del rischio: lockdown o ripartenza?, in AA.VV., Diritto e Covid-19, a cura di CHIESI e Santise, Giappichelli Editore, Torino, 2020 , cit., 409-410,: gli studiosi hanno evidenziato che la tecnica del "rischio zero" utilizzata nel lockdown, mira a tutelare la salute pubblica e si contrappone alla tecnica della c.d. "immunità di gregge", che dà prevalenza agli interessi economici di un Paese, non operano un bilanciamento di opposti interessi, ma conferiscono a uno di essi un'importanza maggiore; PASQUINO, Il principio di precauzione ai tempi del CoViD-19 tra "rischio" ed "emergenza" , in BioLaw Journal, 2020, 597 ss.

[211] CINQUE ALBA, op. cit. p. 110

[212] DEL PRATO, Il principio di precauzione del diritto privato: spunti, in Liber amicorum per Francesco D. Busnelli. Il diritto civile tra principi e regole, Giuffrè, 2008, 545 ss

Nell'ambito della responsabilità extracontrattuale, la precauzione tende a sovrapporsi alla colpa e alla causalità e ciò rende difficile per il danneggiato di poter azionare gli strumenti di tutela riconosciuti nel nostro ordinamento.

3.3.3 Gli strumenti di tutela azionabili in caso di illecito trattamento dei dati

L'utilizzo delle applicazioni di contract tracing, quali "Immuni", hanno aperto il "vaso di Pandora" liberando tutti i timori umani, con la conseguenza che i soggetti predisposti alla tutela della privacy e al rispetto delle norme inerenti al trattamento dei dati sanitari, hanno cercato di scongiurare la possibilità che i governi degli Stati membri utilizzino l'Intelligenza Artificiale non solo per scopi politici e amministrativi legittimi, quale è la tutela della salute, ma anche per anticipare e controllare il comportamento dei cittadini in modi che limitano le libertà individuali e interferiscono con il processo democratico.

L'intelligenza artificiale e i Big Data, in combinazione con la disponibilità di ampie risorse informatiche da parte degli Stati possono portare alla profilazione degli individui, sulla base di dati riguardanti gli stessi e, per scongiurare tale situazione anche il GPDR, all' art 22, riconosce il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici sfavorevole per il cittadino comunitario.

Tale primo divieto, però, da solo non è sufficiente e, pertanto, nel caso in cui non vengano rispettate le prescrizioni e i principi riconosciuti dal Regolamento (analizzati nel capitolo secondo), l'Unione Europea e gli Stati membri hanno previsto una serie di strumenti per la tutela dell'interessato in caso di trattamento illecito dei dati.

Per quanto riguarda la tutela oggi apprestata dall'ordinamento italiano, si assiste ad una commistione tra diritto europeo e nazionale dal quale scaturiscono numerosi di mezzi di tutela, sia inibitoria- preventiva, sia sanzionatoria.

Il punto di partenza comune ad entrambi i sistemi giuridici attiene al fatto che per entrambi un trattamento non conforme alla normativa vigente determina innanzitutto l'impossibilità di utilizzare i dati raccolti e successivamente la possibilità per il cittadino di richiedere il risarcimento del danno.

Gli strumenti di tutela concessi all'interessato al fine di far valere i propri diritti si distinguono in preventivi, capaci di far cessare immediatamente la lesione, e risarcitori, capaci di ristorare il danneggiato dal danno subito ed essi possono essere così classificati:

a) **Istanza al titolare del trattamento:** l'interessato al trattamento che ritiene di aver subito una violazione dei suoi diritti può rivolgersi direttamente al titolare del trattamento o al responsabile per la sua tutela, senza particolari formalità.

Dopo aver inviato l'istanza, l'interessato dovrà ricevere una risposta entro 30 giorni, termine che può essere esteso a 60 giorni per particolari ragioni e che deve essere comunicato all'interessato nei primi 30 giorni.

In caso di mancata risposta ovvero in caso di risposta non soddisfacente, l'interessato potrà rivolgersi direttamente all'Autorità di controllo (Garante) o a quella giudiziaria.

b) Tutela amministrativa: regolata dall'art 140- bis[213] del Codice Privacy e dal Regolamento Europeo che permette all'interessato di rivolgersi all'autorità di controllo per la tutela dei propri diritti, in alternativa al giudice ordinario direttamente oppure a seguito di non accoglimento della richiesta rivolta al titolare del trattamento.

c) il Reclamo: l'interessato, di persona o a mezzo di avvocato o organismo di rappresentanza con specifico mandato, può presentare un reclamo all'autorità di controllo, col quale rappresenta una violazione della normativa in materia di protezione dei dati personali. Il reclamo (regolamentato dall'articolo 77 del GDPR e dagli artt. da 140-bis a 143 del Codice Privacy) deve contenere una serie di elementi quali l'indicazione dettagliata dei fatti e delle circostanze; l'indicazione delle norme del GDPR o delle leggi nazionali che si presumono violate; l'indicazione delle misure richieste e gli estremi identificativi del titolare o del responsabile del trattamento se conosciuti.

Il reclamo deve essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro dotato di apposita procura.

Il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata in caso di invio tramite raccomandata A/R, ovvero con firma digitale in caso di invio mediante posta elettronica certificata.

Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale nel corso del quale il Garante può ingiungere al titolare di fornire delle

[213] Articolo 140 Bis Codice Della Privacy (D.Lgs. 30 Giugno 2003, N. 196) Rubricato Forme Alternative Di Tutela: "*Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato può proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria.*
2. Il reclamo al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.
3. La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150."

informazioni, rivolgere avvertimenti sul fatto che i trattamenti possano verosimilmente violare le disposizioni normative, imporre limitazioni provvisorie.

Il procedimento in esame potrà portare all'adozione di vari provvedimenti o sanzioni cosi come indicati nell'articolo 58 GDPR[214] con i quali l'autorità di controllo prescrive le misure per rendere il trattamento conforme alle disposizioni di legge, oppure intima il blocco o il divieto del trattamento che risulti illecito o non corretto.

Avverso il provvedimento che decide sul reclamo è proponibile ricorso giurisdizionale al tribunale competente nel termine di 30 giorni dalla comunicazione del provvedimento.

d) la Segnalazione: l'interessato ovvero un terzo può segnalare al Garante una presunta violazione, fornendo solamente gli elementi di cui si è in possesso. Tale segnalazione non è vincolante per il Garante, il quale può decidere se avviare o meno indagini.

[214] Art. 58 Regolamento UE 2016/679, rubricato Poteri: " 1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti:
a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti; b)condurre indagini sotto forma di attività di revisione sulla protezione dei dati; c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7; d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento; e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri. 2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale. 3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti: a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36; b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali; c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare; d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5; e) accreditare gli organismi di certificazione a norma dell'articolo 43; f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5; g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d); h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b); j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47. 4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta. 5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso. 6. Ogni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 2 e 3. L'esercizio di tali poteri non pregiudica l'operatività effettiva del capo VII.

e) I Provvedimenti di urgenza: che prevedono il ricorso al giudice ordinario nei modi e nelle forme di cui all'art 700 c.p.c. nel caso in cui si riesca a provare occorre provare il fumus boni iuris, consistente nella probabilità di accoglimento della richiesta, e il periculum in mora, consistente nel concreto pericolo che nel tempo necessario ad ottenere una pronuncia giudiziale possano intervenire fatti irreparabili che impedirebbero l'applicazione di un eventuale giudizio favorevole.

f) La Tutela civile: in alternativa al reclamo al Garante, l'interessato può rivolgersi al giudice civile, e in particolare al tribunale del luogo dove il titolare del trattamento ha uno stabilimento oppure dove risiede l'interessato ai sensi dell'art. 79 GDPR.

La tutela civile è regolata dall'articolo 82 del GDPR che dispone: "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento". L'espressione utilizzata è riferita al danno patrimoniale e non patrimoniale*[215]"

Il soggetto danneggiato a seguito di un trattamento illecito dei suoi dati può ottenere il risarcimento di qualunque danno occorsogli derivante sia dalla condotta del titolare che del responsabile del trattamento ovvero dai saggetti eventualmente autorizzati dal titolare.

Il titolare del trattamento risponderà per il danno causato dal trattamento in violazione del Regolamento, mentre il responsabile risponderà solo del danno causato dal non corretto adempimento dei suoi obblighi specifici, o se ha agito in modo difforme rispetto alle istruzioni del titolare.

In quest'ottica si configura, in capo al titolare ed eventuali responsabili, una responsabilità oggettiva e solidale tra tutti i soggetti convolti nel trattamento così come specificato nel Considerando 146[216] e, in tale forma di responsabilità, si applica il principio del cumulo tra i

[215] Art 82, comma 1, GDPR

[216] Considerando 146 GDPR: "Il Titolare Del Trattamento O Il Responsabile Del Trattamento Dovrebbe Risarcire I Danni Cagionati A Una Persona Da Un Trattamento Non Conforme Al Presente Regolamento Ma Dovrebbe Essere Esonerato Da Tale Responsabilità Se Dimostra Che L'evento Dannoso Non Gli È In Alcun Modo Imputabile. Il Concetto Di Danno Dovrebbe Essere Interpretato In Senso Lato Alla Luce Della Giurisprudenza Della Corte Di Giustizia In Modo Tale Da Rispecchiare Pienamente Gli Obiettivi Del Presente Regolamento. Ciò Non Pregiudica Le Azioni Di Risarcimento Di Danni Derivanti Dalla Violazione Di Altre Norme Del Diritto Dell'unione O Degli Stati Membri. Un Trattamento Non Conforme Al Presente Regolamento Comprende Anche Il Trattamento Non Conforme Agli Atti Delegati E Agli Atti Di Esecuzione Adottati In Conformità Del Presente Regolamento E Alle Disposizioni Del Diritto Degli Stati Membri Che Specificano Disposizioni Del Presente Regolamento. Gli Interessati Dovrebbero Ottenere Pieno Ed Effettivo Risarcimento Per Il Danno Subito. Qualora I Titolari Del Trattamento O I Responsabili Del Trattamento Siano Coinvolti Nello Stesso Trattamento, Ogni Titolare Del Trattamento O Responsabile Del Trattamento Dovrebbe Rispondere Per La Totalità Del Danno. Tuttavia, Qualora Essi Siano Riuniti Negli Stessi Procedimenti Giudiziari Conformemente Al Diritto Degli Stati Membri, Il Risarcimento Può Essere Ripartito In Base Alla Responsabilità Che Ricade Su Ogni Titolare Del Trattamento O Responsabile Del Trattamento Per Il Danno Cagionato Dal Trattamento, A Condizione Che Sia Assicurato Il Pieno Ed Effettivo Risarcimento Dell'interessato Che Ha Subito Il Danno. Il Titolare Del Trattamento O Il Responsabile Del Trattamento Che Ha Pagato L'intero Risarcimento Del Danno Può Successivamente Proporre Un'azione Di Regresso Contro Altri Titolari Del Trattamento O Responsabili Del Trattamento Coinvolti Nello Stesso Trattamento

vari soggetti (art. 82. par. 4), per far sì che tutti i danneggiati ottengano sempre l'intero risarcimento del danno, potendo agire per l'intero danno indifferentemente contro uno qualsiasi dei soggetti tenuti solidalmente al risarcimento, indipendentemente da eventuali ripartizioni interne tra i danneggianti poiché, le eventuali clausole contrattuali di ripartizione del danno valgono solo nei rapporti interni tra i danneggianti, e il soggetto che ha provveduto a risarcire l'intero danno potrà agire in regresso contro gli altri soggetti per le quote di responsabilità; viceversa, la ripartizione delle quote di danno dovrà essere accertata giudizialmente.

Il GDPR precisa, nell'art 82, che eventuali delegati del titolare ovvero i soggetti da lui autorizzati, risponderanno solo nella misura dell'effettivo concorso alla causazione del danno, in base ai principi generali della responsabilità civile e sempre limitatamente nei rapporti interni con i soggetti tenuti al risarcimento.

Si delinea, inoltre, un regime differenziato nel caso in cui la violazione sia posta in essere nell'esercizio dell'attività d'impresa dal caso in cui la violazione sia perpetrata da persone fisiche che trattano i dati per scopi domestici o personali: se la violazione è realizzata da persone fisiche, giuridiche o altri enti che trattano dati per attività di impresa o professionale, esse sono soggette al regime speciale agevolato per l'interessato al trattamento tipizzato dall'art. 82 GDPR, con risarcimento del danno patrimoniale o non patrimoniale; viceversa, le persone fisiche, che trattano dati per scopi domestici o personali, sono soggette al regime ordinario di responsabilità aquiliana.

In quest'ultimo caso il ristoro dei pregiudizi non patrimoniali passa attraverso un preciso onere di allegazione e di prova che fa capo al soggetto che agisce in giudizio al fine di ottenere il risarcimento di tutti i pregiudizi subiti a causa dell'evento lesivo subito.

Occorre precisare che solo un organo giurisdizionale può condannare il titolare del trattamento illecito al risarcimento dei danni occorsi all'interessato e, pertanto, gli Stati membri devono designare l'organo deputato a tal compito incorrendo, in caso di violazione, alle sanzioni predisposte dai Trattati istitutivi a seguito della mancata attuazione del diritto europeo.

Il GDPR, inoltre, rafforza la posizione dell'interessato in ambito probatorio, il quale può limitarsi a provare la mera violazione dei principi e delle regole di condotta del GDPR mentre, ridimensiona quella del titolare del trattamento, il quale, in base al principio di responsabilizzazione, risponderà del rischio tipico di impresa.

Il titolare del trattamento per non incorrere in responsabilità dovrà dimostrare che l'evento dannoso non gli è in alcun modo imputabile e, pertanto, non potrà limitarsi alla prova negativa di non aver violato le norme (ossia essersi conformato ai precetti), ma dovrà fornire anche la

prova positiva di aver valutato autonomamente il rischio di impresa, purché tipico, cioè prevedibile, e attuato le misure organizzative e di sicurezza tali da eliminare o ridurre il rischio connesso alla sua attività.

Tali azioni possono essere anche esperite nel caso in cui le applicazioni di contact tracing violino le regole stabilite dal Reg. Ue 2016/679 per il trattamento dei dati sanitari.

A distanza di due anni dal lancio dell'applicazione si può osservare che, nonostante il clamore e la fiducia inziale, essa non ha soddisfatto lo scopo per il quale era stata progettata, perché, al fine di rispettare la normativa sulla privacy, l'inserimento dei dati è stato subordinato ad una articolata procedura che presupponeva la compartecipazione dell'operatore sanitario e dell'utente positivo e, in tale periodo, era facilmente prevedibile che gli operatori sanitari, impegnati ad affrontare in prima linea una crisi del tutto inedita, avrebbero potuto trascurare l'onere di assistere telefonicamente il paziente positivo nell'inserimento dei dati sull' app.

Alcuni autori hanno ritenuto che se l'applicazione fosse stata collegata a quella dell'Istituto Superiore della Sanità, a cui le A.S.L. distrettuali o regionali dovevano inviare i risultati dei test effettuati, l'applicazione avrebbe potuto riconoscere in modo automatico i casi di positività e, pertanto, svolgere la funzione per la quale era stata programmata, mentre la riservatezza e l'autodeterminazione del cittadino sarebbero stati tutelati dal carattere non obbligatorio della misura.

Richiamando il principio di precauzione, alcuni autori hanno affrontato la questione concernente la possibile violazione dello stesso, sia dal punto di vista pubblicistico che privatistico, da parte dello Stato italiano.

Dal punto di vista pubblicistico, alcuni autori hanno osservato che il principio di precauzione non è stato del tutto rispettato in quanto il legislatore italiano, non prevedendo una norma *ad hoc* che rendesse obbligatoria l'introduzione dei dati all'interno del sistema a*b origine*, non ha di fatto garantito il massimo livello di tutela alla sicurezza collettiva e alla salute dei consociati[217].

Dal punto di vista privatistico, gli stessi autori hanno messo la luce la possibile violazione del principio di precauzione da parte del Ministero della Salute, il quale, in forza dell'art. 6 del d.l. 30.4.2020, n. 28, conv. in l. 25.6.2020, n. 70, è stato individuato quale titolare del trattamento dei dati e, pertanto, era tenuto a rispettare tutti gli obblighi previsti dal GDPR in materia di trattamento dei dati personali (come ad esempio il dovere di adottare le «misure

[217] CINQUE ALBA, op cit. p.110

tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati).

Il Ministero della salute, quale Titolare del trattamento alla luce dell'odierna normativa, è sempre responsabile per i danni provocati dal trattamento dei dati che sia contrario alle disposizioni di legge e, pertanto, egli dovrà porre in essere tutte quelle attività di gestione e controllo, anche dal punto di vista organizzativo, dei dati sanitari raccolti dall'App. "Immuni".

A carico del titolare e del responsabile per il trattamento dei dati, infatti, vengono previsti degli specifici obblighi di condotta, come quello di c.d. accountability, che vengono in rilievo a prescindere dall'esistenza o meno di un rapporto contrattuale con il danneggiato e, l'obbligo in esame impone al titolare (o al responsabile del trattamento) l'adozione di una serie di accorgimenti e misure minime, la cui entità dipende dal contesto specifico e dal grado di responsabilizzazione raggiunto.

In tale ottica, il GDPR prevede un'ipotesi di responsabilità extracontrattuale da trattamento illecito dei dati con funzione non solo sanzionatoria ma anche preventiva perché il Titolare del trattamento deve, in primo luogo analizzare e valutare il rischio e deve prevedere degli strumenti volti alla gestione di quest'ultimo come, ad esempio, la pseudonimizzazione dei dati personali e la cifratura.

Nel caso in cui gli obblighi imposti dal GDPR non siano stati rispettati, l'art. 82 dello stesso, prevede la legittimazione ad agire in capo a colui che abbia subito un danno, ammettendo in tale accezione qualsiasi soggetto, anche qualora non direttamente interessato, purché dimostri di aver subito "un pregiudizio di natura diversa dal trattamento di dati personali altrui"[218].

Tuttavia, pur trattandosi di responsabilità civile, l'art 82 GDPR prevede al terzo paragrafo l'inversione dell'onere della prova, laddove stabilisce che "il Titolare o il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile[219]" anche in ragione delle conoscenze tecniche esistenti nel periodo storico in cui il prodotto è stato messo in commercio e utilizzato.

L'inversione dell'onere probatorio fa sì che il regime applicabile al caso concreto sia similare alle previsioni di natura probatoria al regime contrattuale ex art. 1218 c.c. onerando quindi il Titolare (o il Responsabile) del trattamento di fornire la prova della non imputabilità.

[218] Considerando n. 14 del GDPR il quale precisa che: " È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto"

[219] Art 82 GDPR

In buona sostanza, il carattere preventivo della disposizione assegna al titolare del trattamento l'obbligo di adottare tutte le misure adeguate ed efficaci affinché vengano rispettati i dettami di tutela per il trattamento dei dati, prevedendo l'obbligo in capo al Titolare di poter dimostrare la conformità delle attività di trattamento con il regolamento medesimo.

Azionando tale forma di tutela, il danneggiato potrà richiedere sia il danno patrimoniale (in tale caso dovrà limitarsi a fornire la prova del pregiudizio economico determinato in ragione della violazione del trattamento dei dati, identificato nel lucro cessante e nel danno emergente) sia il danno non patrimoniale che sarà sottoposto però alla dimostrazione del "danno conseguenza[220]".

Pertanto, alla luce della già menzionata normativa, il Ministero della salute è il soggetto deputato ad assumere decisioni in merito alle modalità di trattamento dei dati ed è responsabile per i danni cagionati da un trattamento contrastante con le disposizioni del GDPR (v. art. 82, comma 2°, GDPR) e, pertanto, sarà tenuto al risarcimento del danno qualora venga dimostrato il pregiudizio subito dal danneggiato.

Alcuni autori ritengono che la mancata previsione di una disposizione finalizzata ad assicurare il corretto inserimento dei dati nel sistema non possa essere considerata di per sé una condotta illecita, contrastante con il GDPR ma, occorre ricordare che, il Regolamento Generale sulla Protezione dei Dati stabilisce che il titolare del trattamento può essere sempre chiamato a rispondere per i danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri [221].

Alla luce di tali premesse, gli autori in esame richiamando il principio di precauzione (principio generale europeo, il quale come chiarito permette di adottare misure specificamente orientate a contrastare un pericolo per la salute umana anche in assenza di tutte le conoscenze

[220] Il danno-conseguenza è rappresentato dall'insieme delle conseguenze pregiudizievoli che la vittima dell'illecito civile ha sofferto a causa della lesione arrecata alla situazione giuridica della quale è titolare.

[221] Considerando n. 146 del GDPR chiarisce che: " Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento".

scientifiche necessarie) ritengono che la mancata tempestiva adozione da parte del titolare del trattamento di una norma volta a disciplinare il corretto e puntuale inserimento, all'interno del sistema, dei dati relativi ai pazienti infetti abbia integrato una condotta omissiva colposa, contrastante con il principio de quo[222].

Secondo tali studiosi la tesi sarebbe suffragata dalla considerazione che la mancata previsione di un sistema efficiente attraverso cui inserire i dati dei pazienti positivi al Covid-19 ha reso, *quoad effectum,* non pienamente funzionante per alcuni mesi un'applicazione per il cui sviluppo sono state devolute ingenti risorse pubbliche.

Tuttavia, gli stessi autori si rendono conto della difficoltà probatorie in capo al danneggiato, il quale dovrebbe fondare un'azione di responsabilità sulla violazione di un principio generale che ha un'ampia portata contenutistica e che difficilmente potrebbe attanagliarsi alle stringenti regole probatorie della responsabilità civile.

Ad oggi, non è ancora possibile stabilire se i dati raccolti dall'applicazione Immuni siano stati trattati nei modi e nelle forme stabilite dalla legge o se gli stessi continuano ancora oggi ad essere trattati; tuttavia, è possibile sin da ora affermare che se tali violazioni venissero riscontrate, il Ministero della salute potrebbe essere chiamato a rispondere della violazione in forza delle disposizioni del GDPR nel caso in cui il consociato riesca a superare le difficoltà probatorie.

Le problematiche suscitate dal ricorso alle nuove tecnologie e ai Big Data durante l'esperienza Covid- 19 non hanno riguardato solo l'Italia, infatti, in tutto il modo sono state sviluppate diverse soluzioni al fine di contrastare la diffusione della pandemia e, alcune di esse, sono state utilizzate per reperire informazioni non solo sanitarie.

3.4 L'utilizzo Dei Big Data Nel Panorama Internazionale Al Tempo Della Pandemia: Inghilterra, Cina, Di Singapore E Arabia Saudita

Come anticipato molti paesi europei e non hanno adottato diverse strategie al fine di contrastare la diffusione del virus e seppur le soluzioni adottate non sono state le stesse, esse presentano quasi sempre, un tratto comune: l'utilizzo delle tecnologie di contact tracing.

Non potendo ripercorrere tutte le diverse metodologie e tecniche utilizzate, la presente analisi si focalizzerà solo sulle tecnologie adottate in Inghilterra, Cina, Singapore e Arabia Saudita.

222 CINQUE ALBA, op. cit. p. 110

In relazione all'esperienza inglese, occorre precisare che tutte le misure adottate fino al 31 dicembre 2020 dal Governo inglese hanno dovuto tenere conto delle disposizioni del GDPR, il quale era ancora pienamente efficace nel territorio britannico.

Tuttavia, il 18 luglio 2022 il Parlamento inglese ha presentato il disegno di legge sulla protezione dei dati e l'informazione digitale e, ad oggi, il regime di protezione dei dati del Regno Unito è costituito dal Regolamento generale sulla protezione dei dati del Regno Unito (GDPR del Regno Unito), dal Regolamento sulla privacy e sulle comunicazioni elettroniche (PECR) e dal Data Protection Act 2018 (DPA).

I giuristi inglesi, con lo scoppio della pandemia hanno dovuto affrontate questioni simili ai giuristi italiani in merito alla protezione dei dati sanitari poiché nel marzo 2020 in Inghilterra vi era la piena operatività del GDPR.

Per fronteggiare la pandemia, il Regno Unito ha adottato un'applicazione chiamata NHS COVID-19, similare all'applicazione Immuni italiana, che, avvalendosi della tecnologia bluetooth per individuare persone infette entro un certo raggio, inviava una notifica agli altri utilizzatori dell'applicazione che si trovano nelle vicinanze del soggetto positivo al Covid-19.

A differenza dell'applicazione italiana, però, è stato stabilito dalla legislazione inglese che i dati caricati sull'applicazione NHS COVID-19 non potranno esse accessibili a nessun organo istituzionale e il Governo non potrà utilizzare i personal data raccolti per motivi di interesse generale[223].

Tale applicazione, infatti, è stata designata, in ossequio al principio di minimizzazione, per ridurre il più possibile il ricorso ai dati personali degli utenti[224].

In Inghilterra, inoltre, sono state utilizzate altre due applicazioni Covid Symptom Tracker, sviluppata dai ricercatori del King's College di Londra, e il Covid-19 Sounds, un' app sviluppata dai ricercatori dell'Università di Cambridge: la prima applicazione utilizza i dati sensibili e traccia i movimenti degli individui che hanno contratto l'infezione in tempo reale [225]e, la seconda ha il compito di raccoglie registrazioni di tosse, respiro e voci da parte di persone che presentano sintomi dell'infezione e di persone sane, al fine di costruire modelli predittivi e diagnosticare in tempi brevi i casi di COVID-19.

[223] NHS Covid19, v. https://covid19.nhs.uk.
[224] CINQUE ALBA, Privacy, Big-Data E Contact Tracing, op. cit. p. 110
[225] L'applicazione Symptom Tracker presuppone che gli utilizzatori registrino informazioni personali come il loro nome, il luogo di residenza, l'altezza, il peso ed ulteriori dati attinenti alle condizioni di salute degli utenti. Inoltre, è stata scaricata da oltre 750.000 persone.

Quest'ultima applicazione a differenza di quelle sin qui analizzate si avvale di un sistema di machine learning, che, attraverso la raccolta di dati sensibili e di registrazioni vocali, "allena" l'algoritmo ad individuare i soggetti che hanno contratto l'infezione in tempi brevi.

Le preoccupazioni inerenti alla tutela della privacy degli utilizzatori hanno indotto, il 7 maggio 2020, il Parlamento del Regno Unito a realizzare un progetto di legge relativo alla regolamentazione dell'applicazione e alla tutela dei dati personali e, al contempo, la Royal Society ha promosso il piano d'azione" DELVE[226]" (*Data Evaluation and Learning for Viral Epidemics)*, un'iniziativa che ricorrendo anche ai Big Data, persegue l'obiettivo di combattere la diffusione del Covid-19, attraverso la costituzione di un gruppo di ricerca multidisciplinare.

All'interno di tale iniziativa è stato presentato nel 2021 l'*ASMODEE* (*automatic selection of models and outlier detection for epidemics*) un nuovo algoritmo per il cambiamento di tendenza e il rilevamento di anomalie che unifica i due importanti caratteristiche di un sistema di allerta precoce: misurare le tendenze temporali nelle serie temporali di incidenza e rilevare anomalie recenti, conteggiando i casi eccezionalmente più elevati sulla base di dati recenti.

Il principale vantaggio dell'approccio in esame consiste nella possibilità di specificare una gamma di modelli candidati e selezionare automaticamente la migliore previsione (usando K ripetuti-fold cross-validation) o il modello fitting (usando AIC)[227].

Tuttavia, *l'ASMODEE,* seppur addestrato solo con i dati inerenti all'epidemia Covid-19, esso si caratterizza per una notevole flessibilità e il suo impiego può essere facilmente esteso ad altre malattie e contesti quali, ad esempio, per rilevare nuovi focolai di casi di Ebola in epidemie su larga scala come l'epidemia di Ebola nell'Africa occidentale.

Diversamente dai paesi europei Singapore, Cina e paesi arabi hanno realizzato delle strategie di contenimento più stringenti che si caratterizzano per una forte compressione di alcune libertà fondamentali dei cittadini.

Lo Stato di Singapore, infatti, ha fatto ricorso alla tecnologia di contact tracing al fine di contrastare la diffusione del Covid-19, predisponendo un sistema di tracciamento, denominato

[226] Il piano è finalizzato ad analizzare data nazionali ed internazionali al fine di determinare gli effetti di differenti misure e strategie, tenendo in considerazione i risultati di queste ultime in ambito economico e sociale. Lo scopo della raccolta dei dati è quello di fornire risposte strategiche da attuare sul territorio del Regno Unito per prevenire e rallentare la diffusione della pandemia.

[227] si tratta, infatti di un algoritmo che addestra un modello statistico su serie temporali di conteggio "univariato" per derivare limiti basati su un parametro alfa e tiene conto dell'andamento e della stagionalità e ridimensiona i conteggi anomali nella fascia di allenamento. Per evitare di rimanere intrappolati nelle tendenze recenti e quindi di perdere le epidemie, gli ultimi passaggi temporali vengono ignorati durante l'allenamento. Per un approfondimento si rinvia a: https://royalsocietypublishing.org/doi/10.1098/rstb.2020.0266

SafeEntry[228], che si basa sull'utilizzo di un QR Code identificativo che rinvia ad una pagina web e che richiede l'inserimento di alcuni dati, tra cui il nominativo e ulteriori informazioni personali del soggetto "scansionato" (numero di telefono, e-mail, stato di salute)[229].

Gli scanner deputati a leggere il QR Code sono stati istallati all'interno dei luoghi maggiormente frequentati e la raccolta dei dati ha permesso di ricostruire gli spostamenti di un soggetto infetto e di rintracciare le persone che hanno avuto contatti con i positivi al Covid-19.

Il Governo di Singapore, inoltre, si è avvalso anche di un'altra applicazione, che sfrutta la tecnologia bluetooth ed è scaricabile su base volontaria, chiamata *" Trace Together",* la quale ha la capacità di identificare le persone che hanno avuto contatti con un individuo infetto per più di trenta minuti, registrando l'incontro in una memoria temporanea criptata.

Il Governo di Singapore e soprattutto il Commissario per la protezione dei dati personali di Singapore (PDPC) hanno, in un primo tempo, affermato che tali misure erano idonee al rispetto del principio della riservatezza in quanto i dati sarebbero stati accessibili solo ai funzionari del Ministero della salute; tuttavia, era stato specificato che l'utilizzo e la divulgazione di dati personali rilevati senza un puntuale consenso dell'interessato risultavano legittime per fronteggiare l'emergenza sanitaria e tracciare i contatti.

Successivamente, il Governo di Singapore ha ammesso pubblicamente che i dati raccolti dall'app di tracing sono accessibili anche dalle forze dell'ordine per ragioni investigative, contraddicendo le precedenti rassicurazioni in materia di tutela dei dati personali.

Il Governo di Singapore, infatti, aveva precedentemente escluso esplicitamente che i dati sarebbero stati utilizzati per qualcosa di diverso dal tracciamento del virus ma, il 4 gennaio 2021 la disciplina in materia di trattamento dei dati degli utilizzatori di Trace Together è stata modificata[230] stabilendo espressamente che: "« *TraceTogether data may be used in circumstances where citizen safety and security is or has been affected. Authorised Police officers may invoke Criminal Procedure Code (CPC) powers to request users to upload their TraceTogether data for criminal investigations. The Singapore Police Force is empowered under the CPC to obtain any data, including TraceTogether data, for criminal investigations»*[231].

[228] SafeEntry è un sistema di check-in digitale nazionale che registra i dettagli identificativi delle persone (dati identificativi e numeri di cellulare) che visitano luoghi pubblici come centri commerciali e luoghi di lavoro, nonché aree di attività comuni. SafeEntry supporta e accelera gli sforzi di tracciamento dei contatti fornendo alle autorità un registro delle persone che visitano questi luoghi.
[229] CINQUE ALBA, Privacy, Big-Data E Contact Tracing, op. cit. p. 110
[230] Agenzia Governativa di Singapore, nelle TraceTogether Privacy Safeguards, https://www.tracetogether.gov.sg/
[231] Ibidem: "I dati di TraceTogether possono essere utilizzato in circostanze in cui la sicurezza e la sicurezza dei cittadini è o è stata pregiudicata. Gli agenti di polizia autorizzati possono invocare il codice di procedura penale (CPC) poteri di richiedere agli utenti di

Pertanto, estendendo la normativa penale in tale ambito, essa è applicabile a tutti i documenti, inclusi i dati digitali, su cui Singapore eserciti la propria competenza giurisdizionale e che siano funzionali e utili allo svolgimento delle indagini[232], comportando una aperta violazione del trattamento dei dati sanitari e personali come concepita a livello europeo.

In relazione all'esperienza cinese, la principale strategia attuata dalla Cina per contrastare la diffusione del Covid-19 sul territorio nazionale è consistita proprio nel ricorso alle tecnologie di contact tracing, tramite un sistema di mappatura, il c.d. Migration Big Data Platform che ha permesso di tracciare i movimenti di casi sospetti e dei viaggiatori in aree ad alto rischio, come ad esempio la regione di Wuhan[233].

La Cina si è avvalsa anche dell'applicazione WeChat e AliPay per determinare automaticamente, sulla base dei sintomi dichiarati, se l'utilizzatore dovesse sottoporsi a isolamento, e ciò è stato possibile tramite la registrazione volontaria dell'utente su una di queste app e la creazione di un Health Code il cui colore indica il potenziale stato di contagio[234].

La peculiarità del sistema di tracing cinese è che l'app si serve della tecnologia GPS per verificare che la quarantena non venga violata e una volta immesse le informazioni necessarie per la registrazione e per l'ottenimento del codice, i dati sono automaticamente trasmessi alle autorità di polizia e ogni cittadino che risulti avere avuto contatti con un infetto confermato doveva essere sottoposto ad una quarantena obbligatoria di almeno due settimane.

Inoltre, in Cina è legalmente fatto divieto ai soggetti infetti di allontanarsi dalla zona di quarantena ed essi sono tenuti a mantenere il distanziamento fisico anche nei confronti dei familiari, non appena venga ordinato loro da parte del centro medico locale e ad occuparsi dell'evoluzione della condizione di salute del soggetto in isolamento sono deputati alcuni funzionari del governo locale, che monitorano due volte al giorno per telefono la situazione del soggetto infetto[235].

In relazione all'esperienza dell'Arabia Saudita, la strategia realizzata per il contrasto alla diffusione del Covid-19 si basa sull'utilizzo dei Big Data con un approccio incentrato su una

caricare i propri dati TraceTogether per le indagini penali. Le forze di polizia di Singapore sono autorizzate ai sensi del CPC per ottenere qualsiasi dato, inclusi i dati di TraceTogether, per le indagini penali"

[232] l' art. 20 del Codice di procedura penale di Singapore dispone che qualsiasi documento, cartaceo o digitale, che sia ritenuto funzionale o utile allo svolgimento delle indagini deve essere esibito o consegnato all'agente di polizia ovvero al funzionario pubblico che lo richiede

[233] 27. CINQUE ALBA, Privacy, Big-Data E Contact Tracing: Il Delicato Equilibrio Fra Diritto Alla Riservatezza Ed Esigenze Di Tutela Della Salute, in La Nuova Giurisprudenza Civile Commentata, n. 4, 1 luglio 2021, Wolters Kluwer S.p.A.

[234] Il codice verde consente all'utente piena libertà di movimento; il codice giallo obbliga l'utente a una quarantena preventiva della durata di una settimana; il codice rosso fa insorgere, in capo all'utilizzatore, l'obbligo di rispettare una quarantena di quattordici giorni.

[235] 48. FONTANA M. La minaccia di erosione del diritto alla riservatezza ai tempi del Covid-19: la reazione all'emergenza, in Teaching European Law and Life Sciences (BioTell) a.a. 2019-2020 , pag 8

politica rigorosa di monitoraggio degli ingressi nel Paese e di individuazione mirata di soggetti infetti ricorrendo alla tecnologia di contact tracing.

Occorre premettere che, sebbene l'ordinamento saudita disponga di una legge generale che configura la privacy come un diritto connesso alla dignità dell'individuo, in essa manca una regolamentazione generale in materia di protezione dei dati personali, la cui tutela è assicurata da discipline di settore quale ad esempio l'Anti-Cyber Crime Law of 2007 (Royal Decree No. M/17) che mira a combattere i crimini informatici[236].

Inoltre, l'Arabia Saudita ha costituito la Saudi Data & A.I. Authority (SDAIA), organismo preposto allo sviluppo e al controllo dei data nazionali e all'incremento dello sviluppo delle tecnologie basate sull'I.A che, durante l'emergenza Covid-19, ha promosso congiuntamente con il Ministero della Salute progetto Saudi Covid-19 Index[237], che assolve il compito di analizzare e prevedere la diffusione del Covid-19 sul territorio nazionale[238].

La cooperazione tra questi due organi ha fatto sì che in Arabia Saudita venisse lanciata l'applicazione di contact tracing, chiamata " Tabaud", una tecnologia bluetooth che invia una notifica agli utilizzatori che si trovino nelle vicinanze di un soggetto infetto e li invita a sottoporsi a un esame naso-faringeo[239].

Il Ministro della Salute saudita ha reso obbligatorio per i cittadini di ritorno nel territorio nazionale l'utilizzo di un braccialetto elettronico, chiamato *" Tetammann bracelet*" finalizzato a vigilare sul rispetto dell'auto-isolamento da parte del cittadino proveniente da uno stato estero ed ha sviluppato un'applicazione mobile, la c.d. *" Tetammann app*", che persegue, anch'essa, lo scopo di vigilare sul rispetto dell'auto-isolamento[240].

---

[236] L'art 2 l'Anti-Cyber Crime Law of 2007 (Royal Decree No. M/17) dispone che: *" This Law aims at combating cyber crimes by identifying such crimes and determining their punishments to ensure the following:*
1. Enhancement of information security.
2. Protection of rights pertaining to the legitimate use of computers and information networks.
3. Protection of public Interest, morals, and common values.
4. Protection of national economy"
Tradotto letteralmente: Questa legge mira a combattere i crimini informatici identificando tali crimini e determinandone le sanzioni per garantire quanto segue:
1. Miglioramento della sicurezza delle informazioni.
2. Tutela dei diritti relativi all'uso legittimo dei computer e delle informazioni reti.
3. Tutela dell'interesse pubblico, della morale e dei valori comuni.
4. Tutela dell'economia nazionale"

[237] Saudi Covid, index, https://covid19.pemandu.org/Saudi%20Arabia , (30 agosto 2022) Il progetto ha lo scopo di coadiuvare gli organi del Governo ad affrontare la sfida posta dall'emergenza sanitaria attraverso l'adozione delle misure più efficaci e deterrenti.

[238] CINQUE ALBA, op. cit. p. 122

[239] ibidem

[240] idibem

Infine, i ricercatori del King Abdulaziz City for Science and Technology (KACST) hanno sviluppato una tecnologia che, avvalendosi dell'I.A. e dell'accesso ai Big Data, analizza la diffusione del Covid-19, simulando la mobilità degli individui all'interno delle città.

Gli stessi ricercatori hanno poi sviluppato anche una piattaforma per studiare la diffusione del Covid-19 attraverso l'utilizzo dei Big Data estrapolati da social media e da compagnie telefoniche, resi anonimi[241] e messi a disposizione della sanità saudita al fine di tracciare il raggio di diffusione del virus e pianificare una strategia contenitiva adeguata ed efficace.

[241] Dr. Moraga P., Unlocking Coronavirus' Secrets Through Cellphone Data And Social Media, In King Abdullah Umiversity Of Science And Technology, https://www.kaust.edu.sa/en/news/unlocking-the-secrets-of-coronavirus , (30 agosto 2022)

CONCLUSIONI

Il presente elaborato ha voluto mettere in rilievo la difficoltà della legislazione positiva, europea e nazionale, di regolare aspetti della vita quotidiana nel caso in cui l'essere umano venga a contatto con un'intelligenza artificiale.

L'analisi della tematica ha voluto offrire una panoramica delle riflessioni che possono essere svolte in tema di responsabilità civile dell'intelligenza artificiale, soffermandosi su un particolare settore, quale quello medico, in cui l'evoluzione dell'A.I presenta punti di contatto e frizione con due diritti fondamentali: il diritto alla salute e il diritto al corretto trattamento dei dati sanitari.

L'indagine ha mosso i suoi passi dall'evoluzione storica dell'intelligenza artificiale, ipotizzando quale "anno zero" il 1939, periodo in cui venne costruito "l'Atanasoff Berry Computer" (cd.ABC), ossia il primo computer digitale totalmente elettronico.

Successivamente, si è visto come l'evoluzione scientifica dell'Intelligenza Artificiale è stata influenzata da importanti studiosi, tra cui possiamo ricordare, Alan Turing che 1950 pubblicò, sulla rivista "Mind" uno dei primi articoli sull'intelligenza artificiale, dal titolo "*Computing machinery and intelligence",* John McCarthy che coniò il termine di "intelligenza artificiale" e nel 1956 ipotizzò la costruzione di una macchina in grado di simulare l'intelligenza umana, gli studiosi Warren McCulloch, Walter Pitts e lo psicologo americano Frank Rosenblatt, il quale progettò un modello base di reti neurali denominato " percettrone" in grado di apprendere ed elaborare le informazioni che venivano programmate.

L'analisi ha messo in rilievo la difficile evoluzione dell'Intelligenza Artificiale, caratterizzata da periodi di forte interesse scientifico e giuridico ed altri, definiti come "inverni dell'intelligenza artificiale", caratterizzati da numerosi fallimenti e disinteresse della ricerca scientifica in questo campo ma, come si è avuto modo di verificare, l'evoluzione in questo campo non si è mai arrestata tanto che negli anni '90 sono iniziati i primi studi complessi, finalizzati a far replicare alle macchine il ragionamento seguito dal cervello umano.

L'evoluzione scientifica dell'I.A., però, non è stata seguita dall'evoluzione normativa, infatti, le poche norme che si rinvengono sono state emanate in specifici settori quali la privacy e la responsabilità da prodotto difettoso e ciò è dovuto alla difficoltà di dare una definizione univoca all' "Intelligenza Artificiale" e ciò ha comportato l'ulteriore difficoltà di inquadrare questa nuova tecnologia nei sistemi e nei modelli classici del diritto.

L’indagine ha quindi preso come riferimento la definizione di l’Intelligenza Artificiale dell’Università di Stanford, che identifica l’I.A. come “*una scienza ovvero 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*”, ed ha analizzato i tre più importanti modelli di apprendimento: l’apprendimento per rinforzo, l’apprendimento non supervisionato e l’apprendimento supervisionato.

Successivamente, si è passati ad analizzare le regole etiche delineate Gruppo di lavoro AI4People, costituito su iniziativa dell’Unione Europea in tema di I.A., le quali hanno permesso nel febbraio del 2020 alla Commissione di presentare “il Libro Bianco sull'intelligenza artificiale”, un documento unico nel suo genere che ha posto l’Europa in una posizione di avanguardia nella regolamentazione del settore ed in cui vengono poste le basi per la tutela dei diritti dei consumatori e la promozione dell'innovazione nel campo dell'I.A

Nel libro bianco sull’intelligenza artificiale, l’Unione Europea ha cercato di porre le basi per un possibile equilibrio tra innovazione e protezione dei diritti e delle libertà individuali della persona prescrivendo delle possibili linee guida da seguire al fine di delineare il futuro quadro normativo, invitando, al contempo, il legislatore europeo a concentrarsi soprattutto sulla regolamentazione dei dati di addestramento, della tenuta dei dati e dei registri, delle informazioni da fornire agli utenti, della robustezza e della precisione dell’I.A. e del ruolo dell’uomo nella sorveglianza del sistema e ciò al sol fine di creare un ecosistema di fiducia per l’utilizzo dell’I.A. da parte dei produttori e dei consumatori.

Il quadro delineato dall’analisi svolta ha mostrato un’apertura sempre maggiore del diritto europeo all’innovazione e soprattutto alla volontà di voler regolare il fenomeno dell’Intelligenza artificiale, cercando di armonizzare la tutela all’interno di tutti gli Stati membri per poter raggiungere un livello normativo e di tutela parificato in tutto il territorio europeo.

Le linee giuda elaborate dalla Commissione Europea sono state recepite e poste a fondamento anche del programma elaborato dallo Stato italiano in tema di intelligenza artificiale che, nei primi mesi del 2020, ha pubblicato, tramite Ministero dello Sviluppo Economico, la proposta di strategia italiana elaborata dal Gruppo di Esperti MISE.

L’analisi si è poi spostata sul diritto alla privacy e sulla normativa vigente in tema di trattamento dei dati personali ed è stata analizzata la storia e l’evoluzione del diritto alla riservatezza in ambito internazionale, attraverso l’esame della Dichiarazione Universale dei Diritti Umani del 1948, la Convenzione europea dei diritti dell’uomo (cd. Cedu) e la Convenzione n. 108/1981 in merito alla protezione delle persone rispetto al trattamento

automatizzato di dati a carattere personale e, in ambito europeo attraverso l'evoluzione del diritto alla privacy nei Trattati Istitutivi e nel diritto derivato.

In tale contesto si è appurato che il settore dei dati personali risulta articolato e complesso poiché non solo è strettamente collegato al concetto sfuggevole di privacy ma anche perché la regolamentazione è caratterizzata dalla compresenza di norme nazionali, europee e internazionali

Tuttavia, è stato anche rilevato che il legislatore europeo già partire dai primi anni '90 ha cercato di dare una pronta tutela alle persone fisiche, emanando la direttiva 95/46/CE inerente al trattamento dei dati personali e alla libera circolazione di tali; il legislatore europeo, infatti, ha cercato di fissare un nucleo di regole e di criteri comuni al fine di garantire un'omogenea protezione dei dati delle persone nel territorio dell'Unione e ciò in quanto, alcuni Stati membri avendo già adottato delle leggi nazionali in materia di protezione dei dati, garantivano un livello di tutela diversificato all'interno del territorio europeo.

La Direttiva 95/46/CE è stata superata solo recentemente con l'emanazione del REG. UE 679/2016, entrato in vigore solo nel 2018, che tra le novità di maggiore interesse si annovera l'art. 6, il quale non riconosce più un ruolo centrale al consenso dell'interessato che, ad oggi, figura solo come una delle possibili alternative su cui il trattamento di dati personali può essere fondato.

Per quanto riguarda il settore medico, nel terzo capitolo l'approfondimento è stato compiuto in due ambiti specifici: il settore diagnostico e chirurgico, in cui si registra un crescente utilizzo dell'I.A. nella lotta alla prevenzione e alla cura di alcune malattie e quello inerente trattamento dei dati sanitari, il quale ha avuto un crescente interesse con lo scoppio della pandemia Covid-19.

Lo studio si è soffermato su questi due settori poiché nel settore diagnostico e chirurgico non vi sono delle norme specifiche in tema di responsabilità nel caso in cui il robot medico, integrato con l'I.A., collabori con il medico umano mentre nel settore del trattamento dei dati sensibili vi sono delle regole puntuali elaborate dal legislatore europeo per tutelare i cittadini.

Come rilevato, nel settore diagnostico e chirurgico l'utilizzo dell'intelligenza artificiale pone il particolare problema di individuare gli elementi essenziali della responsabilità civile in caso di cooperazione tra intelligenza umana e artificiale e la problematica più rilevante attiene alla verifica dell'adeguatezza del vigente impianto normativo alla nuova realtà che vede la cooperazione tra medico umano e medico robot in quel particolare settore che oggi viene denominato c.d. chirurgia robotica.

L’analisi ha preso quale punto di riferimento la considerazione che non tutti i robot sono integrati dall’Intelligenza Artificiale, ma che l’integrazione con l’I.A. permette ai robot di aumentarne le capacità e le potenzialità predittive come, ad esempio, il robot “Star” (Smart Tissue Autonomous Robot), progettato dalla Johns Hopkins University e specializzato nell’anastomosi dei tessuti molli, il quale attraverso un sistema a guida visiva e sofisticati algoritmi di intelligenza artificiale ha eseguito un’intera operazione chirurgica senza l’assistenza umana.

Tuttavia, non solo i robot sono impiegati nella cura e la prevenzione nel settore medico, infatti esistono numerose applicazioni dell’intelligenza Artificiale nel settore della radiologia, quali, ad esempio, il sistema di deep learning CheXNeXt e il Deep Learning Assisted Detecting (DLAD) il TRACE4BDensity, programmato per contribuire alla lotta contro i tumori al seno e, dall’analisi di tutte queste tecnologie si è potuto constatare che ad oggi la normativa italiana è in grado di tutelare i suoi cittadini solo in parte, perché la tutela è garantita nel caso in cui il danno venga provocato da sistemi che non hanno autonomia decisionale quale, ad esempio, il robot Da Vinci, (in tali casi, infatti, la responsabilità civile derivante dal malfunzionamento del robot chirurgico seguirà le normali regole della responsabilità civile, permettendo al paziente la possibilità di citare in giudizio il chirurgo ai sensi del 2043 cc e la struttura sanitaria ai sensi degli artt. 1218 e 1228 c.c., così come stabilito dalla legge Gelli Bianco, ovvero entrambi in concorso nel caso in cui non sussista alcun rapporto di subordinazione o di collaborazione tra clinica e sanitario); mentre, nel caso in cui venga ipoteticamente impiegato per l’intervento un robot quale Star, dotato di autonomia decisionale e in grado di svolgere il compito per il quale è programmato senza l’assistenza umana, i principi generali ad oggi vigenti nel nostro ordinamento risultano totalmente inadeguati.

Inoltre, la responsabilità medica, così come oggi regolata dalla legge Gelli- Bianco, imporrebbe al danneggiato che voglia ottenere un risarcimento una probatio diabolica perché, a causa natura opaca che caratterizza qualsiasi l’intelligenza artificiale, il danneggiato avrebbe serie difficoltà a dimostrare il nesso di causalità che collega il fatto al danno, mentre, in tema di responsabilità contrattuale sarebbe difficile ipotizzare una responsabilità ex art 1218 c.c. in capo alla struttura sanitaria la quale utilizza l’I.A. ma non né potrebbe ma controllare i processi di apprendimento.

Come meglio analizzato, si è anche ipotizzata la possibilità di riconosce all’I.A. un particolare status denominato “personalità elettronica” ma tale riconoscimento aprirebbe ulteriori problemi quali i diritti e le tutele da accordare all’I.A.

Il settore del trattamento dei dati risulta invece compiutamente regolato dal GDPR, il quale dispone una precisa disciplina in tema di trattamento dei dati sanitari e risarcimento per il trattamento illecito degli stessi.

L'entrata in vigore del GDPR, infatti, ha fatto sì che in Italia vi sia la compresenza di diversi strumenti per la tutela dell'interessato in caso di trattamento illecito dei dati: l' Istanza al titolare del trattamento che permette alla persona fisica di interagire direttamente con il titolare del trattamento al fine di far cessare l'illecito, la tutela amministrativa, regolata dall'art 140- bis del Codice Privacy, che non è stata abrogata con l'entrata in vigore del GDPR e che permette all'interessato di rivolgersi all'autorità di controllo per la tutela dei propri diritti, il reclamo, che permette all'interessato, di persona, a mezzo di avvocato o per mezzo di un organismo di rappresentanza con specifico mandato, di presentare un reclamo all'autorità di controllo, nei modi e nelle forme disciplinate dall'articolo 77 del GDPR e dagli artt. da 140-bis a 143 del Codice Privacy, la tutela civile quale strumento alternativo al reclamo al Garante ecc.…

L'analisi di tutti questi strumenti potrebbe far ritenere che, a livello europeo, il singolo cittadino sia tutelato a 360°, tuttavia il crescente utilizzo dell'Intelligenza artificiale ha rilevato che tali strumenti potrebbero non essere sufficienti in alcuni settori quale, ad esempio, quello medico- sanitario dove l'utilizzo dell'Intelligenza artificiale è sempre più crescente e l'esperienza Covid-19 ha mostrato sia la difficoltà di armonizzare il diritto al corretto trattamento dei dati sanitari con altri diritti e principi generali, sia che la disciplina oggi vigente difetta di un'accurata disciplina in materia di Big Data.

Analizzando le strategie di contrasto alla pandemia Covid-19 attuate dall'Italia e da altri paesi extra-europei è emerso che le applicazioni di *contant tracing* sono state utilizzate non solo per combattere la diffusione del Covid, ma alcuni Stati, quali Cina e Singapore, hanno utilizzato queste tecnologie per controllare il rispetto della quarantena ovvero hanno utilizzato i dati raccolti per ragioni investigative.

Apparentemente, sembra che la pandemia sia stata utilizzata da tutti gli Stati del modo per commercializzare prodotti programmati per processare innumerevoli quantità di dati, il cui reale utilizzo sarà rimesso esclusivamente all'etica di ciascun Governo, il quale potrà utilizzare "lecitamente" o meno il potere che deriva dalla conoscenza delle abitudini e dei dati dei cittadini.

Inoltre, algoritmi di IA, addestrati sui dati raccolti, possono essere utilizzati per amplificare il pregiudizio sociale sulla scorta di determinazioni algoritmiche inique e

discriminatorie e tale situazione nel settore pubblico potrebbe compromettere la dialettica politica tra governanti e governati.

I governi, infatti, potrebbero servirsi dell'intelligenza artificiale non solo per scopi politici e amministrativi legittimi ma anche per anticipare e controllare il comportamento dei cittadini in modo tale che le limitazioni della libertà individuale non siano percepibili ai consociati e, la manipolazione dell'opinione politica, basata sulla profilazione e l'invio di messaggi mirati, potrebbe condurre alla conformazione e all'appiattimento delle opinioni politiche nonché al deteriorando il dialogo pubblico.

La paura generata dal diffondersi della pandemia ha fatto sì che molti cittadini sacrificassero autonomamente i loro diritti fondamentali, autorizzando volontariamente il trattamento dei dati, senza, però, preoccuparsi delle possibili conseguenze del loro consenso.

In Italia, infatti, è stato emblematico il richiamo del Garante della privacy al Governo italiano di non utilizzare la pandemia come base legale per introdurre delle tecnologie volte a tracciare e profilare i comportamenti dei cittadini.

L'analisi ha, inoltre, dimostrato che seppur a livello europeo il dibattito circa lo sviluppo di nuove norme volte a regolare il rapporto uomo-macchina sia tra gli obbiettivi principali dell'Unione Europea, non si può non rilevare come la legislazione positiva avanzi molto lentamente rispetto ai nuovi approcci tecnologici e ciò comporta due ordini di problemi.

Il primo che attiene all'abuso dell'IA da parte dei governanti ovvero da parte di soggetti privati che utilizzino la nuova tecnologia per scopi illeciti, in quanto il deficit di regolazione produce sia un gap normativo di tutela sia la sfiducia nell'utilizzo di questa nuova tecnologia che potrebbe risultare determinare per la lotta e il contrasto alla diffusione di nuove malattie

Il secondo che attiene all'evoluzione tecnologica in senso stretto, in quanto il divario tra l'innovazione e il diritto, se non colmato, porterà inevitabilmente a all'arresto del progresso, poiché l'idea di un mondo in cui convivono "Intelligenze Artificiali" capaci di acquisire consapevolezza di sé e di poter rimpiazzare o superare l'uomo è un mondo che difficilmente potrebbe essere accettato dalla razza umana.

BIBLIOGRAFIA:

LIBRI E SAGGI

Aa.Vv. Intelligenza Artificiale Il Diritto, I Diritti, L'etica, Giuffrè Francis Lefebvre S.P.A, Milano, 2020 A Cura Di Ugo Ruffolo

Aa.Vv. I Dati Personali Nel Diritto Privato Europeo, G. Giappichelli Editore, Torino 2019

Aa. Vv., Manuale Sul Diritto Europeo In Materia Di Protezione Dei Dati, Edizione 2018, Agenzia Dell'unione Europea Per I Diritti Fondamentali E Consiglio D'europa, 2018

Aa.Vv. I Contratti Del Consumatore, Giuffrè, Milano 2014

Aa. Vv., Artificial Intelligence: Short Histoy, Present Developments, And Future Outlook, Final Report, In Mit Lincoln Laboratory, 2019;

Ajani G., Pasa B, Diritto Comparato, Lezioni E Materiali, Giappichelli Editore, Torino, 2018

Alpa G., Code Is Law: Il Bilanciamento Dei Valori E Il Ruolo Del Diritto, In Rivista Contratto E Impresa 2/2021, Wolters Kluwer S.P.A.

Amidei A., Intelligenza Artificiale E Product Liability: Sviluppi Del Diritto Dell'unione Europea, In Giurisprudenza Italiana - Luglio 2019

Amidei A., Robotica Intelligente E Responsabilità: Profili E Prospettive Evolutive Del Quadro Normativo Europeo, In U. Ruffolo (A Cura Di) Intelligenza Artificiale E Responsabilità, Giuffrè, Milano, 2017

Arendt H., Vita Activa. La Condizione Umana, Trad. It. Di Finzi S, Bompiani, Milano, 2017,

Aries P., Duby G , La Vita Privata Dall'impero Romano All'anno Mille, Editori Laterza, Bari, 2001,

Balkin, J., "The Three Laws Of Robotics In The Age Of Big Data", In Ohio State Law Journal, 78(5), 2017

Benanti P., Le Macchine Sapienti, Marietti 1820, Bologna 2018

Bertolini A., Aiello G., Robot Companions: A Legal And Ethical Analysis, In J. Inf. Soc., 2018,

Bock T., Linner T., Robot-Oriented Design, Design And Management Tools For The Deployment Of Automation And Robotics In Construction, In Cambridge University Press, Maggio 2015,

Buyers, J., Artificial Intelligence – The Practical Legal Issues, Law Brief Publishing, 2018

Cabitza F.; Alderighi C.; Rasoini R.; Gensini G., Potenziali Conseguenze Inattese Dell'uso Di Sistemi Di Intelligenza Artificiale, In Rivista Oracolari In Medicina, 2017

Camardi C., Tabarrini C., Contact Tracing Ed Emergenza Sanitaria. "Ordinario" E "Straordinario" Nella Disciplina Del Diritto Al Controllo Dei Dati Personali, In "Nuova Giurisprudenza Civile Commentata", 3, 2020,

Carloni E., Digitalizzazione E Riforma Dell'amministrazione: La Nuova Agenda, In Mastragostino F., Piperata G., Tubertini C. (A Cura Di), L'amministrazione Che Cambia. Fonti, Regole E Percorsi Di Una Nuova Stagione Di Riforme, In Quaderni Della Spisa, Bologna, 2016,

Carrozza, M. C., Oddo, C., Orvieto, S., Di Minin, A., E Montemagni, G., Ai: Profili Tecnologici - Automazione E Autonomia: Dalla Definizione Alle Possibili Applicazioni Dell'intelligenza Artificiale", In Biolaw Journal – Rivista Di Biodiritto, N.3/2019

Casciaro G., Santise P., Il Consenso Informato, Giuffrè Editore, Milano 2012

Cerea F., Intelligenza Artificiale A Servizio Dei Pazienti Per Il Contrasto A Covid-19, In Rivista Diritti E Persona, Supplemento Ngcc 3/2020, Wolters Kluwer S.P.A

Chabris C E Simons D, Il Gorilla Invisibile. E Altri Modi In Cui Le Nostre Intenzioni Ci Ingannano, Il Sole 24 Ore, 2012

Ciccia Romito C., Green Pass E Gdpr: Gli Adempimenti Da Rispettare, - Avvocato, Research Fellow Islc, Università Degli Studi Di Milano, In Quotidiano Giuridico Wolters Kluwer 2021 S.P.A.

Cinque A., Privacy, Big-Data E Contact Tracing: Il Delicato Equilibrio Fra Diritto Alla Riservatezza Ed Esigenze Di Tutela Della Salute, In La Nuova Giurisprudenza Civile Commentata, N. 4, 1° luglio 2021, Wolters Kluwer S.P.A.

Colletti E., Intelligenza Artificiale E Attività Sanitaria. Profili Giuridici Dell'utilizzo Della Robotica In Medicina, In Rivista Di Diritto Dell'economia, Dei Trasporti E Dell'ambiente Vol. Xix 2021

Comandé, G., Intelligenza Artificiale E Responsabilità Tra «Liability» E «Accountability». Il Carattere Trasformativo Dell'ia E Il Problema Della Responsabilità, In Analisi Giuridica Dell'economia, 2019

Comandè G., Responsabilità E Accountability Nell'era Dell'intelligenza Artificiale, In Di Ciommo F., Troiano O., Giurisprudenza E Autorità Indipendenti Nell'epoca Del Diritto Liquido, Studi In Onore Di Roberto Pardolesi, Piacenza, La Tribuna, 2018,

Coppini L., Robotica E Intelligenza Artificiale: Questioni Di Responsabilità Civile ,In Rivista Politica Del Diritto, Il Mulino 2018

Corso S., Il Fascicolo Sanitario Elettronico Fra E-Health, Privacy Ed Emergenza Sanitaria, In "Responsabilità Medica", 4, 2020

Cuffaro V., D'orazio R, La Protezione Dei Dati Personali Ai Tempi Dell'epidemia, In "Corriere Giuridico", 6, 2020,

D'acquisto G., Intelligenza Artificiale: Elementi , Giappichelli 2021

Del Prato, Il Principio Di Precauzione Del Diritto Privato: Spunti, In Liber Amicorum Per Francesco D. Busnelli. Il Diritto Civiletra Principi E Regole, Giuffrè, 2008

Di Ciommo Francesco, Covid-19 E Crisi Dei Diritti Fondamentali Della Persona: Le Responsabilità Della Responsabilità Civile, In Danno E Responsabilità, N. 3, 1 Maggio 2020, Wolters Kluwer S.P.A.

Yang G.Z Et Al., Medical Robotics—Regulatory, Ethical, And Legal Considerations For Increasing Levels Of Autonomy, In Science Robotics, 2017

Fabris F., Il Diritto Alla Privacy Tra Passato, Presente E Futuro, In Tigor: Rivista Di Scienze Della Comunicazione – A.I (2009) N.2 (Luglio-Dicembre)

Finocchiaro G., Intelligenza Artificiale E Protezione Dei Dati Personali, In Giurisprudenza Italiana, Luglio 2019

Finocchiaro G., Responsabilità E Intelligenza Artificiale, In Contr. E Imp., 2020,

Finocchiaro G., Il Punto Sull'app Immuni: Bilanciamento Tra Diritti, In Medialaws.Eu, 09 Giugno 2020

Fioriglio G., La Protezione Dei Dati Sanitari Nella Società Algoritmica. Profili Informatico-Giuridici, In Journal Of Ethics And Legal Technologies, Volume 3, November 2021

Fontana M. La Minaccia Di Erosione Del Diritto Alla Riservatezza Ai Tempi Del Covid-19: La Reazione All'emergenza, In Teaching European Law And Life Sciences (Biotell) A.A. 2019-2020

Fusaro A., Quale Modello Di Responsabilità Per La Robotica Avanzata? Riflessioni A Margine Del Percorso Europeo, In Ngcc, 2020

Gabrielli E. E Ruffolo U., Intelligenza Artificiale E Diritto, Dottrina E Attualità Giuridiche Intelligenza Artificiale, Giurisprudenza Italiana - Luglio 2019, Wolters Kluwer S.P.A.

Gambino A.M., E Manzi M., Intelligenza Artificiale E Tutela Della Concorrenza, In Giurisprudenza Italiana - Luglio 2019

Harari Y.N. , 21 Lezioni Per Il Xxi Secolo, Milano 2019, Bompiani Editore

Hart P.E., Duda R. O., Einaudi M.T., Prospector- A Computer-Based Consultation System For Mineral Exploration, In Journal Of The International Association For Mathematical Geology 10, 1978, P. 589-610

Malva A. E Zurlo V., La Medicina Nell' Era Dell' Intelligenza Artificiale : Applicazioni In Medicina Generale, In Rivista Società Italiana Di Medicina Generale N.4 , Vol.6 , 2019

Mantelero A., Il Costo Della Privacy Tra Valore Della Persona E Ragione D'impresa, Giuffrè Editore, Milano, 2007,

Martines, M., La Protezione Degli Individui Rispetto Al Trattamento Automatizzato Dei Dati Nel Diritto Dell'unione Europea, In Rivista Italiana Di Diritto Pubblico Comunitario, 2000

Mayer-Schonberger,Cukier, Big Data. A Revolution That Will Transform How We Live , Work , And Think, In Boston 2013.

Miotto, R., Li, L. Kidd, B. A., E Dudley, J. T., Deep Patient: Anunsupervised Representation To Predict The Future Of Patients From The Electronic Health Records, In Scientific Reports, 2016;

Mumford L., La Cultura Delle Città, Trad. It. Di E. E M. Labò, Giulio Enaudi Editore Milano 2007

Niger S., Le Nuove Dimensioni Della Privacy: Dal Diritto Alla Riservatezza Alla Protezione Dei Dati Personali, Cedam, Padova 2006,

O'neill C., Weapons Of Math Destruction: How Big Data Increases Inequality And Threatens Democracy, Penguin Books Ltd, Crown 2017 Pp. 1-272

Pagallo U., La Tutela Della Privacy Negli Stati Uniti D'america Ed In Europa, Giuffrè Francis Lefebvre S,P.A,Milano, 2008

Pagallo U., Robotrust And Legal Responsibility, In Know Techn. Pol., Vol. 23, 2010

Palmerini E., Robotica E Diritto: Suggestioni, Intersezioni, Sviluppi A Margine Di Una Ricerca Europea, In Resp. Civ. E Prev., 2016, Vol. 6

Pasquale F., Lo Storto G. ; Manca D., Bassotti P., Le Nuove Leggi Della Robotica. Difendere La Competenza Umana Nell'era Dell'intelligenza Artificiale – 3 Giugno 2021 Editore, In Luiss University Press (3 Giugno 2021)

Pasquino, Il Principio Di Precauzione Ai Tempi Del Covid-19 Tra "Rischio" Ed "Emergenza" , In Biolaw Journal, 2020

Passagnoli G., Ragionamento Giuridico E Tutele Nell'intelligenza Artificiale, In Persona E Mercato, 3/2019

Pioggia A., La Sanità Italiana Di Fronte Alla Pandemia. Un Banco Di Prova Che Offre Una Lezione Per Il Futuro, In Dir. Pubbl., 2020

Pellecchia E., Profilazione E Decisioni Automatizzate Al Tempo Della Black Box Society: Qualita` Dei Dati E Leggibilità Dell'algoritmo Nella Cornice Della Responsible Research And Innovation, In Le Nuove Leggi Civili Commentate 5/2018, Nlcc 5/2018 Wolters Kluwer S.P.A.

Peruselli C. , De Panfilis L. , Gobber G., Melo M., Tanzi S., Artificial Intelligence Palliative Care: Opportunities And Limits, In Recenti Prog Med 2020;111(11):639-645, Novembre 2020, Vol. 111, N. 11

Piraino, F. Il Regolamento Generale Sulla Protezione Dei Dati Personali E I Diritti Dell'interessato. Le Nuove Leggi Civili Commentate, 40(2), Wolters Kluwer S.P.A , 2017

Pizzetti Franco, Intelligenza Artificiale, Protezione Dei Dati Personali E Regolazione, Giappichelli, 2018

Prati E., Mente Artificiale, Egea S.P.A, Milano, 2017

Prosser W,. Privacy, A Legal Analysis, In California Law Review, N.48, 1960

Rodotà S., Intervista Su Privacy E Libertà, (A Cura Di)Conti P., Laterza Edizioni, Roma-Bari, 2005

Rodotà, S., Il Diritto Di Avere Diritti, Laterza, Roma-Bari, 2012

Ruffolo U., Intelligenza Artificiale E Responsabilità, Giuffrè 2017

Ruffolo U. Il Problema Della "Personalità Elettronica", In Journal Of Ethics And Legal Technologies ,Volume 2(1), Aprile 2020

Salanitro U., Intelligenza Artificiale E Responsabilità: La Strategia Della Commissione Europea, In Riv. Dir. Civ., 2020

Santise M., Principio Di Precauzione E Tecniche Di Gestione Del Rischio: Lockdown O Ripartenza?, In Aa.Vv., Diritto E Covid-19, A Cura Di Chiesi E Santise, Giappichelli Editore, Torino, 2020

Santoro A., La Responsabilità Da Contatto Sociale. Profili Pratici E Applicazioni Giurisprudenziali, Giuffrè, Milano 2012

Sartori, L., La Tutela Della Salute Pubblica Nell'unione Europea, Biblos, 2009

Sciarabba, V., Tra Fonti E Corti: Diritti E Principi Fondamentali In Europa: Profili Costituzionali E Comparati Degli Sviluppi Sovranazionali, Wolters Kluwer Italia, 2008, 131

Shapiro S. C., Encyclopedia Of Artificial Intelligence. Second Edition Vol. 1, John Wiley & Sons Inc; University Of Michigan, 31 Gennaio 1992, P. 1-1792

Shortliffe E. H, "Computer-Based Medical Consultations: Mycin", Elsevier Computer Science Library, Amsterdam 2012, Vol. 2

Schuilenburg M., Peeters, R., The Algorithmic Society. Technology, Power, And Knowledge. Routledge, Londra 2021

Simons K. W, A Restatement (Third) Of Intentional Torts? Article Is A Revised Version Of A Paper Presented At The Dan B. Dobbs Conference On Economic Tort Law Hosted By The University Of Arizona James E. Rogers College Of Law In Tucson, Arizona, On March 3–4, 2006. Articles From The Conference Are Collected In This Issue, Volume 48 Number 4, Of The Arizona Law Review.

Sirgiovanni B., Dal Consenso Dell'interessato Alla "Responsabilizzazione" Del Titolare Del Trattamento Dei Dati Genetici, Saggi E Approfondimenti, In Le Nuove Leggi Civili Commentate, N. 4, 1 Luglio 2020, P. 1010 Wolters Kluwer

Timiani M., Un Contributo Allo Studio Sul Diritto Alla Riservatezza, In Rivista Di Studi Parlamentari E Di Politica Costituzionale, 2012

Tripathi, M." Ehr Evolution: Policy And Legislation Forces Changing The Ehr", In Journal Of Ahima 83, N.10 (Ottobre 2012)

Uricchio A., Robot Tax: Modelli Di Prelievo E Prospettive Di Riforma, In Giurisprudenza Italiana N. 7/2019, Utet Giuridica, Torino Luglio 2019

Vannozzi D. , Intelligenza Artificiale E Big Data In Sanità: L'esperienza Di Cineca, Dicembre 2021, Vol. 112, N. 12 In Recenti Prog. Med.

Vecchione L., La Responsabilità Da Prodotto Difettoso E La Garanzia Di Conformità, Key Editore, 2022

Venosta F., "Contatto Sociale" E Affidamento, Giuffè, Milano 2021

Zeno-Zenovich, V., La Responsabilità Civile In Alpa, G., Et Al. “Diritto Privato Comparato”, Istituti E Problemi, Editori Laterza, Bari (1999).

Warren S., Brandeis L. D., The Right To Privacy, In Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890),

Westin A. , Privacy And Freedom, Athaeneum, New York, 1970,

SITI WEB E PUBBLICAZIONI ON LINE:

AA. VV., Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018, Agenzia dell’Unione europea per i diritti fondamentali e Consiglio d’Europa, 2018 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_it.pdf

Cappelletti P. · Golato M., Medicina Di Laboratorio 4.0, In La Rivista Italiana Della Medicina Di Laboratorio - https://link.springer.com/article/10.1007/s13631-018-00212-5 Riv Ital Med Lab (2018) 14:192–197 https://doi.org/10.1007/s13631-018-00212-5

Commissione Europea, White Paper on Artificial Intelligence: a European approach to excellence and trust COM(2020) 65,19.2.2020,https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach excellence-and-trust_en

De Luca A, Monaco S, In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia Italiana - V Appendice (1994), Robotica, https://www.treccani.it/enciclopedia/robotica_%28Enciclopedia-Italiana%29/#:~:text=La%20r.,nei%20territori%20slavi%20dell'Impero

Encyclopædia Britannica, Inc, Deep Blue, Computer Chess-Playing System, https://www.britannica.com/topic/Deep-Blue

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Neologismi 2018, “Blockchain” https://www.treccani.it/enciclopedia/blockchain_%28altro%29/#:~:text=s.%20f.%20inv.,nodo

%2C%20per%20assicurarne%20la%20tracciabilit%C3%A0.&text=%C2%ABDagli%20anni%20Settanta%20il%20legame,allentato%2C%20fino%20alla%20finanziarizzazione%20attuale

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedie On Line, Ingegneria Genetica, https://www.treccani.it/enciclopedia/ingegneriagenetica/#:~:text=Insieme%20di%20tecnologie%20che%20permettono,(%E2%9E%94%20biotecnologie%2C%20genetica)

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Neologismi (2019), machine learning, https://www.treccani.it/vocabolario/machinelearning_%28Neologismi%29/#:~:text=le%20m.,computazionale%20e%20l'ottimizzazione%20matematica

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia On Line, Intelligenza Artificiale, https://www.treccani.it/enciclopedia/intelligenza-artificiale

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Neologismi (2012), Big Data, https://www.treccani.it/vocabolario/big-data_res-007d6462-8995-11e8-a7cb-00271042e8d9_%28Neologismi%29/

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Vocabolario On Line, Algoritmo , https://www.treccani.it/vocabolario/algoritmo/

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia On Line, Cloud Computing , https://www.treccani.it/enciclopedia/cloudcomputing/#:~:text=Letteralmente%20%E2%80%9Cnuvola%20informatica%E2%80%9D%2C%20termine,e%20archiviare%20dati%20in%20rete

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Italiana - V Appendice (1994), Sistemi Esperti (7 maggio 2022), https://www.treccani.it/enciclopedia/sistemi-esperti_%28Enciclopedia-Italiana%29/#:~:text=I%20s.e.%20sono%20programmi%20per,ricerca%20in%20intelligenza%20artificiale%20

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia della Matematica, Lisp, (07 maggio 2022),https://www.treccani.it/enciclopedia/lisp_%28Enciclopedia-della Matematica%29/#:~:text=Il%20lisp%20si%20basa%20sul,tra%20parentesi%20(%E2%86%92%20notazione)

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Della Matematica Treccani (2013), Sistema Esperto, https://www.treccani.it/enciclopedia/sistema-esperto_%28Enciclopedia-della-Matematica%29/

Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A, Enciclopedia Treccani on line, definizione di sistema binario, https://www.treccani.it/enciclopedia/codice-binario,

Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Vocabolario On Line,Perizia, https://www.treccani.it/vocabolario/perizia/#:~:text=Stima%20e%20giudizio%20espressi%20da,%2C%20di%20na%20scrittura%2C%20ecc

CAPPELLI M., ENCICLOPEDIA TRECCANI, - Enciclopedia della Scienza e della Tecnica (2008): https://www.treccani.it/enciclopedia/percettrone_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/

Commissione Europea, COMUNICAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=DE

Dr. Moraga P., Unlocking Coronavirus' Secrets Through Cellphone Data And Social Media, In King Abdullah Umiversity Of Science And Technology, https://www.kaust.edu.sa/en/news/unlocking-the-secrets-of-coronavirus

Facial Recognition Technology: Fundamental Rights Considerations In The Context Of Law Enforcement (Tecnologia Di Riconoscimento Facciale: Considerazioni Sui Diritti Fondamentali Nell'ambito Delle Attività Di Polizia E Giudiziarie), https://fra.europa.eu/en/publication/2019/facial-recognition

Firmino M, Giovani A., Morais H, ed altri- Computer-aided detection (CADe) and diagnosis (CADx) system for lung cancer with likelihood of malignancy, in BioMedical Engineering OnLine, https://biomedical-engineering-online.biomedcentral.com/articles/10.1186/s12938-015-0120-7

HAENLEIN M. e KAPLAN. A. “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence.” California Management Review, Volume: 61 fascicolo: 4, p. 5-14 Articolo pubblicato per la prima volta online il 17 luglio 2019, https://doi.org/10.1177/0008125619864925

Hwang EJ, Park S, Park CM e altre, Development and validation of a deep learning-based automated detection algorithm for major thoracic diseases on chest radiographs, in JAMA NetworkOpen 2019, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2728630

Jelinek A., Dichiarazione sul trattamento dei dati nel contesto dell'epidemia di Covid-19 del 19 marzo 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_it_1.pdf.

Lederberg J., "How DENDRAL Was Conceived And Born." In Proceedings Of ACM Conference On History Of Medical Informatics, 1987, P. 5-19, https://dl.acm.org/doi/10.1145/41526.41529

Madani A., Arnaout R., Mofrad M., " Fast and accurate view classification of echocardiograms using deep learning", in NPJ Digit Med 2018, https://www.nature.com/articles/s41746-017-0013-1,

Magalini S., Istituto della Enciclopedia Italiana fondata da Giovanni Treccani S.p.A , Enciclopedia Italiana - V Appendice (1995) Telemedicina, https://www.treccani.it/enciclopedia/telemedicina_%28Enciclopedia-Italiana%29/#:~:text=La%20t.,ove%20essi%20sono%20rispettivamente%20situati.

Magni V., Interlenghi M, altri "Development and Validation of an AI-driven Mammographic Breast Density Classification Tool Based on Radiologist Consensus, Radiology, in Artificial Intelligence, https://pubs.rsna.org/doi/abs/10.1148/ryai.210199

Malizia A, Pattern Recognition Tecniche E Applicazion, in APPLICAZIONI- MONDO DIGITALE Vol n.2, giugno 2006, http://archivio-mondodigitale.aicanet.net/Rivista/06_numero_3/Malizia_p._40-50.pdf

Martinelli G., In Istituto Della Enciclopedia Italiana Fondata Da Giovanni Treccani S.P.A, Enciclopedia Italiana - V Appendice (1994), Definizione Reti Neurali, https://www.treccani.it/enciclopedia/reti-neurali_%28Enciclopedia-Italiana%29/#:~:text=La%20r.n.%20%C3%A8%20un%20insieme,reale%20come%20il%20sistema%20nervoso

Mayer, McKinney S. e altri "International evaluation of an AI system for breast cancer screening", in Nature 2020, gennaio 2020, https://www.nature.com/articles/s41586-019-1799-6

McCarthy J., Minsky M. L., Rochester N., Shannon C.E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf

MININNI A., Il test di Turing, https://www.andreaminini.com/ai/test-di-turing/

Ministero Dello Sviluppo Economico, Proposte Per Una Strategia Italiana Per L'intelligenza Artificiale, Https://Www.Mise.Gov.It/Images/Stories/Documenti/Proposte_Per_Una_Strategia_Italiana_Ai.Pdf

NHS Covid19, v. https://covid19.nhs.uk

Nielsson N. J., The Quest for Artificial Intelligence, Print version published by Cambridge University Press http://www.cambridge.org/us/0521122937

Pasceri G. E Altri, Intelligenza Artificiale In Radiologia, Documento Sirm 2020, https://sirm.org/wp content/uploads/2021/04/317-Documento-SIRM-2020-Intelligenza-artificale-in-radiologia.pdf

Parlamento Europeo, Risoluzione del 16 febbraio 2017, Gazzetta Ufficiale Unione Europea, https://eur-lex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT#:~:text=C%20252%2F241,Gioved%C3%AC%2016%20febbraio%202017,non%20contravvengano%20alla%20Prima%20Legge

Presidente del Garante per la protezione dei dati personali ,App "Immuni": via libera del Garante privacy, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356588

Presidente del Garante per la protezione dei dati personali, Sicurezza del dato sanitario e condivisione Intervento di Pasquale Stanzione, in Panorama, 18 febbraio 2022 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9747071

Presidente del Garante per la protezione dei dati personali, Garante privacy su proliferazione app di contact tracing. Violano la privacy i trattamenti non coperti dalla normativa nazionale, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9447462

Rajpurkar P. e altri, CheXNeXt: Deep learning for chest radiograph diagnosis, in Stanfor Dml Group, https://stanfordmlgroup.github.io/projects/chexnext/

Rocco P., Fondamenti di robotica – Programmazione del moto, Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria, https://rocco.faculty.polimi.it/FDR/Programmazione%20del%20moto.pdf

Saidi H., Opfermann M.K., Wei S. E Altri, Chirurgia Laparoscopica Robotica Autonoma Per Anastomosi Intestinale, In Science Robotics" Del 26 Gennaio 2022 Vol 7 , Edizione 62, https://www.science.org/doi/abs/10.1126/scirobotics.abj2908

Saudi Covid, index, https://covid19.pemandu.org/Saudi%20Arabia

Teaching one-to-one, in Cambridge University Press and Cambridge Assessment English, https://www.cambridgeenglish.org/Images/525581-teaching-one-to-one-part-1.pdf

Trafton D. e Wolfe J.: "Because even radiologists can lose a gorilla hiding in plain sight", in Heard on Morning Edition February 11, 20133, https://www.npr.org/sections/health-shots/2013/02/11/171409656/why-even-radiologists-can-miss-a-gorilla-hiding-in-plain-sight,

YANG G.Z. et al., Medical robotics—Regulatory, ethical, and legal considerations for increasing levels of autonomy, in Science Robotics, 2, 2017 https://www.science.org/doi/10.1126/scirobotics.aam8638

GIURISPRUDENZA

CORTE DI GIUSTIZIA

Sentenza 12 Novembre 1969, Erich Stauder C. Città Di ULM – Sozialamt, Causa 29/69 https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A61969CJ0029

Sentenza 14 maggio 1974, J. Nold, Kohlen- und Baustoffgroβhandlung c. Commissione, C.4/73, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A61973CJ0004

Sentenza 13 Dicembre 1979, Liselotte Hauer C. Land Rheinland – Pfalz, C-44/79, https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A61979CJ0044

Sentenza 15 Maggio 1986, Marguerite Johnston C. Chief Constable Of The Royal Ulster Constabulary, C. 222/84 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A61984CJ0222

Sentenza 13 Luglio 1989, Hubert Wachauf C. Germania, Causa C-5/88, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A61988CJ0005

Sentenza 7 maggio 2009, College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer, C-553/07, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62007CA0553

Sentenza della Corte, Grande Sezione, dell'8 aprile 2014, Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a., Cause riunite C-293/12 e C-594/12, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0293

Sentenza 1° ottobre 2015, Smaranda Bara e a. c. Casa Naţională de Asigurări de Sănătate e a., Causa C-201/14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0201

Sentenza 4 maggio 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA «Rīgas satiksme», C-13/16, https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62016CJ0013

CORTE EUROPEA DEI DIRITTI DELL'UOMO

Sentenza 4 dicembre 2008, S. e Marper c. Regno Unito, cause riunite ricc. nn. 30562/04 e 30566/04, Corte Edu, in Biodiritto, Unverità di Trento, https://www.biodiritto.org/Biolaw-pedia/Giurisprudenza/Corte-Europea-dei-Diritti-dell-Uomo-S.-Marper-v.-UK-limite-alla-conservazione-dei-dati-genetici

CORTE DI CASSAZIONE

Sentenza 22 gennaio 1999, Cassazione Civile n. 589, Normattiva, https://www.normattiva.it

Sentenza 11 gennaio 2008, Cassazione Civile Sezioni Unite n. 577, Normattiva, https://www.normattiva.it

Sentenza 9 Giugno 2010, Cassazione Civile N. 13881, Normattiva, https://www.normattiva.it

Sentenza 19 febbraio 2013, Cassazione Civile n. n. 4030. Normattiva, https://www.normattiva.it

Sentenza 13 gennaio 2015 Corte di Cassazione civile n. 280, Normattiva, https://www.normattiva.it

Sentenza del 05 luglio 2017, Cassazione civile, Sezioni Unite, n. 16601, Normattiva, https://www.normattiva.it

Sentenza 12 febbraio 2019 Cassazione penale n.30626, Normattiva, https://www.normattiva.it

Sentenza 12 giugno 2019 Cassazione penale n. 3972 Normattiva, https://www.normattiva.it

Sentenza 30 ottobre 2019, Cassazione civile ordinanza n. 27970, Normattiva, https://www.normattiva.it

Sentenza 21 novembre 2019 Cassazione penale n.49774, Normattiva, https://www.normattiva.it