SISTEMA PENALE

FASCICOLO

11/2026

DIRETTORE RESPONSABILE Gian Luigi Gatta
VICE DIRETTORI Guglielmo Leo, Luca Luparia, Mitja Gialuz

ISSN 2704-8098

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervè Belluta, Michele Caianiello, Massimo Ceresa-Gastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Risicato, Marco Scoletta, Carlo Sotis, Costantino Visconti.

COMITATO SCIENTIFICO (REVISORI) Andrea Abbagnano Trione, Dario Albanese, Alberto Alessandri, Silvia Allegrezza, Chiara Amalfitano, Enrico Mario Ambrosetti, Ennio Amodio, Gastone Andreazza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Enrico Basile, Fabio Basile, Alessandra Bassi, Teresa Bene, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Francesca Biondi, Rocco Blaiotta, Manfredi Bontempelli, Carlo Bonzano, Matilde Brancaccio, Carlo Bray, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Gaia Caneschi, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Carlotta Conti, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Jacopo Della Torre, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Stefano Finocchiaro, Carlo Fiorio, Roberto Flor, Luigi Foffani, Dèsirèe Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Alessandra Galluccio, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kostoris, Giorgio Lattanzi, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Adelmo Manna, Grazia Mannozzi, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Francesco Mazzacuva, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Lorenzo Picotti, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocolo, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Bartolomeo Romano, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Nicola Triggiani, Tommaso Trinchera, Andrea Francesco Tripodi, Giulio Ubertis, Maria Chiara Ubiali, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vigoni, Francesco Zacchè, Stefano Zirulia.

REDAZIONE Francesco Lazzeri, Giulia Mentasti (coordinatori), Enrico Andolfatto, Silvia Bernardi, Patrizia Brambilla, Pietro Chiaraviglio, Beatrice Fragasso, Ilaria Giugni, Elisa Grisonich, Francesco Lazzarini, Alessandro Malacarne, Cecilia Pagella, Emmanuele Penco, Gabriele Ponteprino, Sara Prandi, Valentina Vasta.

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.
I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili). La licenza è consultabile su *https://creativecommons.org/licenses/by-nc-nd/4.0/*.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2023, p. 5 ss.

SISTEMA PENALE

11/2026

PROFILI ATTUALI DELLE RESPONSABILITÀ PENALI IN MATERIA DI TRATTAMENTI SANITARI

di Lorenzo Picotti

Il saggio muove dalla constatazione della crescente digitalizzazione delle attività di diagnosi e cura, oltre che assistenziali e relative alla gestione nonché allocazione dei servizi e delle risorse in campo sanitario, che si correla a quello della ricerca e consente in questo ampio settore il progressivo impiego di sistemi di intelligenza artificiale. Considerando le fonti europee, che pur da diverse prospettive interessano questo importante ambito, quali l'AI Act (oggetto di recenti modifiche) ed il regolamento sullo spazio europeo dei dati sanitari (EHDS Act), che dovrà progressivamente applicarsi, nonché la legge nazionale sull'intelligenza artificiale n. 132 del 2025 ed i nuovi reati introdotti dal successivo decreto legislativo delegato n. 160 del 2026, che contengono norme rilevanti per questa materia, sono analizzati tre principali campi d'interesse: le eventuali ricadute penali della disciplina del consenso informato quando vi sia l'impiego di sistemi di intelligenza artificiale nei trattamenti sanitari; la tutela penale dei trattamenti dei dati personali sanitari a fronte della digitalizzazione e dell'impiego di sistemi di intelligenza artificiale nell'ambito in esame; le questioni che pone l'impiego di sistemi di intelligenza artificiale in relazione alla possibile responsabilità penale del sanitario per eventi avversi.

SOMMARIO: 1. Nuove esigenze di tutela di fronte alla digitalizzazione ed all'impiego di sistemi di intelligenza artificiale in ambito sanitario. – 2. Impiego di sistemi di intelligenza artificiale nei trattamenti sanitari e consenso informato: contenuto e limiti dell'informazione e relative ricadute penali. – 3. Tutela penale dei dati personali a fronte della digitalizzazione e dell'impiego di sistemi di intelligenza artificiale in ambito sanitario. – 3.1. Sulle fonti e sui limiti del trattamento dei dati sanitari quali dati appartenenti a "categorie particolari". – 3.2. Rilevanza penale delle violazioni in materia di trattamento di dati sanitari. – 3.2.1. Trattamento illecito di dati sanitari. – 3.2.2. Trasferimento illecito di dati sanitari all'estero. – 3.2.3. Comunicazione e diffusione illecite di dati sanitari. – 4. Impiego di sistemi di intelligenza artificiale e responsabilità penale del sanitario per eventi avversi. – 4.1. Premesse generali sulla tutela penale in materia. – 4.2. Sul nesso causale. – 4.3. Sulla colpa "personale". – 4.4. Sulla "colpa di organizzazione" e sul nuovo delitto colposo di omessa adozione di misure di sicurezza tecniche. – 5. Spunti conclusivi.

1. Nuove esigenze di tutela di fronte alla digitalizzazione ed all'impiego di sistemi di intelligenza artificiale in ambito sanitario.

Se la digitalizzazione e l'impiego sempre più estesi di sistemi di intelligenza artificiale (d'ora in poi: sistemi IA) stanno portando enormi vantaggi anche in campo medico e sanitario, ed in particolare anche in quello della ricerca in questi ambiti, nel

contempo tale sviluppo tecnologico suscita timori di nuovi rischi, tanto più insidiosi, in quanto difficili da riconoscere con immediatezza per la loro novità e, quindi, ardui da prevenire o contrastare tempestivamente, rispetto a quando possono emergerne gli effetti.

Come si è già rilevato con riferimento ad altri settori, in cui si stanno diffondendo tali nuove tecnologie, che vanno da quello delle auto a guida autonoma e dei trasporti, a quello dei mercati finanziari, da quello dell'amministrazione pubblica e dell'accesso a molteplici servizi e prestazioni, fino a quello delle c.d. armi intelligenti, occorre non solo adattare le regole che li disciplinano od introdurne di nuove, ma precisare o prevedere nuovi adeguati criteri di attribuzione della responsabilità penale, per violazioni della disciplina vigente – o da introdurre nel prossimo futuro – nonché per eventi avversi, in cui siano coinvolti sistemi IA. Infatti, la pervasività delle nuove tecnologie anche in ambito sanitario comporta che possano essere offesi interessi meritevoli di tutela penale, di natura individuale e collettiva, e violati diritti fondamentali delle persone[1]. Pertanto, laddove emergano nel diritto vigente lacune non colmabili dall'interprete, saranno necessari interventi del legislatore, nel rispetto degli essenziali principi garantistici di legalità (che comprende il divieto di applicazione analogica della legge penale) e di personalità della responsabilità penale, oltre che di *ultima ratio* e proporzione.

Un importante peso hanno in questa prospettiva i regolamenti dell'Unione europea sull'intelligenza artificiale (d'ora in poi: *AI Act*, già oggetto di successive modifiche[2]), e sullo spazio europeo dei dati sanitari (d'ora in poi: *EHDS Act*)[3], mentre a livello nazionale è intervenuta la legge 23 settembre 2025, n.132 sull'intelligenza

---

[1] Nell'ormai estesa bibliografia in argomento, basti qui citare, in quella italiana, le recenti monografie di L. D'AMICO, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, Napoli, 2025 e B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, Torino, 2025; volendo *ex multis* sinteticamente v. anche L. PICOTTI, *Responsabilità penale e sistemi di IA*, in S. PREZIOSI (a cura di), *Intelligenza artificiale e responsabilità umana. Uno spazio non libero dal diritto*, Roma, 2026, 89 ss.

[2] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (*AI Act*), che "*stabilisce regole armonizzate sull'intelligenza artificiale*" e modifica norme di precedenti regolamenti, tra cui il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017, relativo ai dispositivi medici, pubblicato in GUUE del 12 luglio 2024, serie L, It. Anche se entrato formalmente in vigore il 2 agosto 2024, molte norme si applicheranno in tempi successivi, come stabilisce l'art. 113, per dare tempo ad autorità, aziende, cittadini di adeguarvisi, con l'eccezione di alcune importanti disposizioni applicate già dal 2 febbraio 2025 (par. 3, lett. a) e dal 2 agosto 2025 (par. 3, lett. b). I termini sono stati da ultimo posticipati, in particolare al 2 dicembre 2027 per le disposizioni dell'art. 6 e correlate regole concernenti i sistemi "*ad alto rischio*", in forza del successivo regolamento (UE) 2026/1744 dell'8 luglio 2026 che modifica i regolamenti (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230, per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (c.d. *Omnibus* digitale sull'IA), pubblicato in GUUE del 24 luglio 2026, serie L, It. Nondimeno, ai fini delle valutazioni penalistiche sui vari punti qui trattati, con particolare riferimento proprio alla disciplina dei sistemi "*ad alto rischio*", l'*AI Act* ha già un importante valore ermeneutico e concettuale al quale fare riferimento.

[3] Il regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025, "*sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847*" (*EHDS Act*), è stato pubblicato in GUUE del 5 marzo 2025, serie L, it. Pur essendo entrato formalmente in vigore il 26 marzo 2025, ai sensi del suo art. 105 si applicherà soltanto a decorrere da molteplici termini successivi, su cui si veda la nota 28.

artificiale, che contiene disposizioni rilevanti anche per il settore in esame, in forza della quale sono di recente stati emanati i decreti legislativi da essa delegati[4] dei quali occorre parimenti tener conto per delineare il perimento della responsabilità penale anche nel settore in esame.

A tal fine si deve muovere dalla constatazione che quello sanitario (o, più precisamente, dei "*servizi sanitari*" pubblici e privati) rientra, alla stregua dell'*AI Act*, in quelli "*ad alto rischio*"[5], oggetto di un'articolata disciplina di valutazione preventiva e, poi, contenimento e monitoraggio dei "*rischi*" specifici, che l'utilizzo di questi sistemi IA comporta[6].

---

[4] Si tratta del d.lgs. 9 settembre 2026, n. 160, attuativo della delega prevista dall'art. 24, comma 5, lett. b) l. n. 132 del 2025, e del successivo d.lgs. 7 ottobre 2026, n. 179, attuativo della delega prevista dall'art. 24, comma 2, l. n. 132 del 2025. Per un primo commento delle disposizioni penali contenute nel d.lgs. n. 160 del 2026, ed in particolare all'art. 437-*bis*, da esso introdotto nel codice penale, sia consentito rinviare a L. PICOTTI, *Le disposizioni penali introdotte dal decreto legislativo dal decreto legislativo delegato in materia di intelligenza artificiale*, in portale *JL – UE e internazionale*, Lefebvre Giuffré (5.10.2026); per un'illustrazione dei contenuti dello schema di decreto legislativo che era stato approvato dal Consiglio dei Ministri nella seduta del 10 giugno 2026 e presentato dalla Presidenza al Senato della Repubblica per il prescritto parere parlamentare in data 24 giugno 2026, Atto del Governo n. 418,cfr. altresì B. FRAGASSO, *Disposizioni attuative in materia di intelligenza artificiale*, in *questa Rivista*, 12 giugno 2026.
Quanto al più complesso d.lgs. n. 179 del 2026, esso individua ed attribuisce varie competenze alle Autorità di notifica, vigilanza del mercato e controllo, per vero di natura governativa, anziché anche strutturalmente indipendenti, come richiederebbe l'art. 70, par. 1, secondo periodo, *AI Act* (vale a dire ACN *in primis*, nonché per il mercato AgiD, mentre per i rispettivi settori di competenza si confermano Banca d'Italia, Consob, IVASS, e Garante privacy), in attuazione del sistema di *Governance* delineato dal Capo VII, artt. 64 s. , *AI Act*. Vengono altresì introdotte specifiche disposizioni sostanziali e procedimentali in materia di sanzioni amministrative, non solo pecuniarie, di loro competenza (sezione V del capitolo II, art. 19-25), oltre a numerose disposizioni concernenti obblighi di formazione in materia di intelligenza artificiale (Capitolo III, artt. 36-51), anche nell'ambito delle professioni sanitarie (art. 47). Ai fini del presente studio è di particolare interesse la sezione VI del capitolo II (artt. 26-31), che introduce e regola le c.d. *regulatory sandboxes,* a partire dallo "*Spazio di sperimentazione italiano per l'IA*" (su cui si tornerà *infra*, par. 4.3 e nota 64), nel cui ambito si prevede fra l'altro la partecipazione del Garante per la protezione dei dati personali ai "*progetti di sistemi di IA innovativi che comportano il trattamento di dati personali*" (art. 28), fermo restando che ai sensi dell'art. 34, rubricato: "*Protezione dei dati e riservatezza*", viene ribadito in termini generali che «*Le forme di coordinamento operativo e informativo, nonché gli scambi di informazione disciplinati con appositi accordi e protocolli d'intesa* (…) *avvengono, anche in deroga all'obbligo del segreto d'ufficio, nel rispetto della vigente normativa in materia di protezione dei dati personali e dei principi di necessità, proporzionalità e minimizzazione*». Una prima illustrazione sistematica del secondo decreto è offerta da F. BAGNI, A. BENVENUTI, *Il D.Lgs. 179/2026 attuativo dell'AI Act: poteri delle autorità, sanzioni e spazi di sperimentazione*, in *Altalex – il QG* (13.10.2026).

[5] Si veda il Considerando (58) dell'*AI Act*, dedicato ai «*servizi e prestazioni essenziali, pubblici e privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi*». Fra questi, *in primis*, vi è espressa menzione delle «*prestazioni e servizi essenziali di assistenza pubblica* [resi] *dalle autorità pubbliche, vale a dire* servizi sanitari (evidenz. agg.), *prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia e la perdita di occupazione e l'assistenza sociale e abitativa*». E poiché «*le persone fisiche*» interessate «*sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile di fronte alle autorità responsabili*», i sistemi IA, se utilizzati, «*possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali*». Pertanto, sono da classificare "*ad alto rischio*", ai sensi dell'art. 6, par. 1 e dell'elenco di cui all'Allegato III, con le conseguenze di cui si dirà per la relativa disciplina.

[6] Per una sintetica esposizione dei possibili riflessi penali delle regole stabilite per i sistemi "*ad alto rischio*", cui dedica l'intero capo III, a partire dalla doverosa valutazione preliminare dei rischi e delle misure di

Pur potendo assicurare, infatti, un miglioramento delle previsioni, un'ottimizzazione delle operazioni e dell'assegnazione delle risorse, una personalizzazione dei servizi ed in particolare, sul piano terapeutico, una maggior sicurezza e tempestività di diagnosi, da un lato, ed efficacia e precisione delle cure e degli interventi, dall'altro (si pensi alla telemedicina ed alla chirurgia robotica di precisione, poco invasiva, ad esempio per interventi sulla prostata, per calcoli renali o biliari, per interventi oftalmici, ecc.), non si possono ignorare i rischi empirici ed i limiti tecnici, che l'impetuoso sviluppo tecnologico e la diffusione nelle attività anche quotidiane fanno emergere, manifestatisi altresì in eventi avversi[7].

Di qui le preoccupazioni etiche e giuridiche, riguardanti lo svolgersi dei rapporti con i pazienti e tutti gli interessati, nonché le responsabilità anche penali che possono configurarsi di fronte a possibili danni ed offese di beni giuridici e diritti fondamentali, che vanno dalla vita ed integrità fisica e psichica, alla libertà di autodeterminazione rispetto ai trattamenti sanitari, dalla *privacy* e tutela dei dati personali, alla sicurezza cibernetica, fino alla fede pubblica ed al buon andamento della pubblica amministrazione.

Il principio euristico, che in prima battuta dovrebbe orientare l'interprete ed in secondo luogo il legislatore, nelle scelte di riforma o criminalizzazione in questi nuovi ambiti, dovrebbe essere quello secondo cui quanto sarebbe penalmente rilevante, se un fatto illecito fosse commesso da una persona umana, non dovrebbe divenire penalmente irrilevante sol perché vi è stato l'intervento di un sistema IA. Tanto più che, di fronte ai nuovi sviluppi tecnologici ed all'estensione tumultuosa delle relative applicazioni, si estenderebbero corrispondentemente aree inaccettabili di impunità[8].

Circoscrivendo in questa sede l'analisi ai punti critici più significativi per l'eventuale configurabilità di responsabilità penali nel settore medico e sanitario, di fronte alla digitalizzazione ed all'impiego di sistemi IA, mi limiterò a considerare il possibile rilievo penale delle violazioni in materia di consenso informato al trattamento medico sanitario che faccia ricorso alle nuove tecnologie (par. 2), quello relativo alla

---

necessario contenimento, ai sensi dell'art. 9 *AI Act* ss., sia consentito rinviare a L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi? Le raccomandazioni dell'*Association Internationale de Droit Pénal *e la rilevanza del recente regolamento europeo sull'intelligenza artificiale*, in *questa Rivista*, 31 luglio 2024, in specie 9 s. e 12 s.; e da ultimo, a proposito dei nuovi delitti di "*Omissione di misure tecniche di sicurezza e di violazione dell'obbligo di sorveglianza umana"* nei sistemi *"ad alto rischio*", previsti dal citato art. 437-*bis* c.p., e richiamati *infra*, par. 4.2, 4.3 e 4.4, si veda più dettagliatamente, volendo, L. PICOTTI, *Le disposizioni penali introdotte dal decreto legislativo delegato*, cit., in specie par. 2.

[7] Per un quadro in materia sanitaria sia sufficiente in questa sede rinviare alle importanti ricerche di N. AMORE, E. ROSSERO, *Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità. Una ricerca sociologica e giuridico-penale*, Torino – Bologna, 2023.

[8] In tal senso si vedano le Raccomandazioni contenute nella risoluzione approvata all'esito dei lavori della Sezione I del XXI Congresso internazionale di diritto penale dell'*Association Internationale de Droit Pénal* (AIDP), svoltosi a Parigi il 26-28 giugno 2024 (c.d. Congresso del Centenario dalla sua fondazione), cui si rinvia, nella quale sono stato il *Rapporteur général*, in L. PICOTTI, B. PANATTONI (eds.), *Traditional Criminal Law Categories and AI: Crisi or Paligenesis?* in *Revue Internationale de Droit Pénal*, Nr. 1/2023, 53 s. Per un'articolata esposizione in lingua italiana sia consentito rinviare a L. PICOTTI, *Categorie tradizionali del diritto penale*, cit. a nota 6.

protezione dei dati personali (par. 3) ed, infine, quello più generale della colpa medica (par. 4). Analisi da condurre guardando alle menzionate fonti europee e nazionali, salvo accenni agli ulteriori interventi normativi auspicabili o che si stanno prefigurando.

2. Impiego di sistemi di intelligenza artificiale nei trattamenti sanitari e consenso informato: contenuto e limiti dell'informazione e relative ricadute penali.

Notoriamente il consenso libero ed informato è un presupposto generale di liceità dei trattamenti sanitari[9], espresso quale "Regola generale" dall'art. 5 della Convenzione di Oviedo del 4 aprile 1997 sui "*Diritti dell'uomo e la biomedicina*" e già prima dalla consolidata interpretazione estensiva della Corte di Strasburgo del "*Diritto al rispetto della vita privata e familiare*" di cui all'art. 8 della Convenzione europea per la salvaguardia dei Diritti dell'uomo e delle Libertà fondamentali, che – per il richiamo contenuto nel par. 3 dell'art. 52 della Carta dei diritti fondamentali dell'Unione europea, il cui art. 7 parimenti riconosce tale diritto – è direttamente vincolante nell'ambito dell'Unione europea[10].

Nel nostro ordinamento, la fonte primaria è rappresentata dall'art. 32 Cost., che ha trovato un'importante articolazione positiva negli artt. 1-3 l. 22 dicembre 2017, n. 219, in linea con le molteplici previsioni del Codice di deontologia medica (cfr. i relativi artt. 16 e 33-39)[11].

Ma sul problema specifico occorre oggi menzionare l'art. 7 l. n. 132 del 2025 sull'intelligenza artificiale, rubricato: «*Uso dell'intelligenza artificiale in ambito sanitario e di disabilità*», che al comma 3 riconosce espressamente il *diritto* dell'interessato «*di essere informato sull'impiego di tecnologie di intelligenza artificiale*», dopo che nel comma 1 il legislatore ha proclamato che «*L'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla diagnosi e alla cura delle malattie,* nel rispetto dei diritti, delle libertà e degli interessi della persona*, anche in materia di protezione dei dati personali*» (evidenz. aggiunte; sull'ultimo aspetto, regolato dai successivi artt. 8 e 9, cfr. *infra*, par. 3).

---

[9] Nell'amplissima letteratura in materia, rinvio, per quella penalistica, a S. CANESTRARI, *Principi di biodiritto penale*, 2ª ed., Bologna, 2023, con esaustivi riferimenti bibliografici, oltre a quelli di cui alla successiva nota 18.

[10] Cfr. in argomento R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione Europea*, Milano, 2017, e su quest'ultimo punto F. FERRARO, *sub Art. 52*; nonché C. AMALFITANO, M. D'AMICO, S. LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione Europa nel sistema integrato di tutela. Atti del convegno svoltosi nell'Università degli Studi di Milano a venti anni dalla sua proclamazione*, Torino, 2022.

[11] Per un ampio *forum* interdisciplinare sulla legge citata cfr. S. CANESTRARI, A. FRANCESCONI, C. BERGONZINI, V. MOLASCHI, P. VERONESI, P. BENCIOLINI, F. GIARDINA, G. PIZZETTI, G. FERRANDO, P. MORINO, C. VIAFORA, A. GIANNINI, N. ZAMPERETTI, D. PARIS, G.R. GRISTINA, L. ORSI, L. BUSATTA, *La legge n. 219 del 2017. Norme in materia di consenso informato e di disposizioni anticipate di trattamento*, in *BioLaw Journal – Rivista di BioDiritto*, 2018, n. 1, 19 s.

La questione aperta riguarda non solo se la violazione di tale diritto abbia rilevanza penale, ma, a monte, quale debba essere il contenuto e quali i limiti dell'informazione sull'impiego di tali tecnologie: in specie se, oltre al fatto del loro impiego, essa debba estendersi anche ai rischi ed ai possibili errori dei sistemi IA, pur circoscrivendoli a quelli che sarebbero "*ragionevolmente prevedibili*" anche se statisticamente non molto elevati (su tale nozione si tornerà *infra* al par. 4.3. in materia di colpa e rischio consentito).

Il testo oggi scarno della norma è il risultato dei lavori parlamentari, per cui essa non enuncia più il contenuto minimo che dovrebbe avere tale informativa, come era nell'originaria formulazione[12], che ne estendeva l'oggetto alla "*logica decisionale*" utilizzata dal sistema, allineandosi alla posizione per così dire moderata sull'inopportunità di un'informativa eccessivamente dettagliata dal punto di vista tecnico, ma che però alludesse – in base al principio di trasparenza, su cui si tornerà – anche ai parametri di funzionamento dei sistemi IA impiegati, per garantire un'informazione effettiva sul loro ruolo e sui rischi correlati, non solo sul loro generico impiego.

In effetti, per il successivo comma 5 dell'art. 7 l. n. 132 del 2025, tali sistemi possono costituire soltanto «*un* supporto *nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica*» (evidenz. aggiunta).

L'informazione dovrebbe, dunque, delineare l'estensione ed i limiti di un tale "*supporto*" alle scelte terapeutiche ed al trattamento medico sanitario, che pur restano di competenza e, quindi, nella responsabilità del sanitario persona umana. Per cui il paziente dovrebbe essere informato, oltre che sui vantaggi, anche sui rischi che un tale "*supporto*" può determinare, affinché sia posto a conoscenza di tutte le "*conseguenze delle scelte operate*"[13].

Di certo non deve e neppure può pretendersi un affidamento cieco del paziente e, per altri aspetti, neppure del medico e dell'operatore sanitario nell'*output* dei sistemi IA[14], vale a dire nelle "*decisioni*" o raccomandazioni da essi suggerite, che possono anche

---

[12] L'originaria formulazione prevedeva il diritto dell'interessato «*di essere informato circa l'utilizzo di tecnologie di intelligenza artificiale e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata*». Nel commento alla formulazione della norma che era stata proposta, avevo segnalato la necessità che, oltre ai "*vantaggi*", nell'informativa si facesse espressa menzione anche dei "*rischi*" inerenti all'impiego di sistemi IA (cfr. L. PICOTTI, *Impiego di sistemi di intelligenza artificiale in medicina e digitalizzazione dei dati sanitari: possibili profili di rilevanza penale*, in *Responsabilità sanitaria, rischio clinico e valore della persona*, 2025, 120 ss.), necessità che ritengo di dover ribadire.

[13] Così il citato art. 33 del Codice di deontologia medica.

[14] Si parla, non solo in letteratura, del rischio di automatico od eccessivo affidamento negli *output* dei sistemi IA: tanto che l'*AI Act* prevede, fra i requisiti della persona fisica che deve garantire la "*sorveglianza umana*" su un sistema IA "*ad alto rischio*", come sono quelli in esame, che essa debba «*restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche*» (art. 14, par. 4, lett. b).

essere direttamente attuate, se si tratta di un sistema *embedded*, munito cioè di *hardware*, in specie robotico[15], in quanto esse possono presentare profili di criticità, oltre ad un *deficit* etico[16]. Il medico persona umana, infatti, deve o può tenere conto di circostanze e caratteristiche personali o variabili di contesto, che possono condizionare le decisioni sul trattamento in termini diversi rispetto a quelli cui può pervenire un sistema IA, che elabora i propri *out put* sulla base dei dati raccolti secondo criteri statistici e cognitivi generali, relativi alle astratte patologie da trattare. Mentre nel caso paradigmatico di un tumore maligno genitale di una giovane donna, l'opzione fra un intervento demolitivo ed uno conservativo può discendere anche da valutazioni empatiche e di sensibilità umana di fronte al singolo caso, non potendosi d'altronde dar rilievo solo alla *voluntas* della 'parte debole', in qualsivoglia modo espressa o fondata, che dovrà certamente essere considerata sapendo, però, che il paziente non si trova in posizione di parità con il sanitario. Per questo è necessario stabilire a livello pubblicistico limiti e garanzie per tutelarlo, a partire dal contenuto dell'informazione, su cui si deve basare il suo necessario consenso (come avviene a tutela di lavoratori, consumatori, investitori, ecc.)[17].

In dottrina[18] e giurisprudenza[19] si è sottolineato che il consenso informato del paziente al trattamento medico sanitario non dovrebbe ridursi ad un mero scambio burocratico di moduli e di firme, ma dovrebbe consistere in un "*percorso informativo e dialogico*" con il medico, finalizzato alla c.d. alleanza terapeutica. Obiettivo che non è questa la sede per discutere se sia raggiunto o meno nella prassi quotidiana della medicina. Ma rispetto all'obbligo di fornire un'informazione completa e chiara sull'impiego di sistemi IA, non si può non rilevare che si possono frapporre ostacoli

---

[15] La nozione di "*sistema IA*" contenuta nell'art. 3, n. 1) *AI Act*, pone l'accento su tale *autonomia* decisionale e sulla capacità di influenzare l'ambiente esterno anche *fisico*, definendolo «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*».

[16] In argomento si rinvia a L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano 2022 e, da ultimo, ID., *Il nodo etico. Informazione e valori nella società digitale*, Milano 2026. Sull'esteso dibattito relativo alla "capacità morale" ed alla "capacità di autodeterminazione" dei sistemi IA quali requisiti di una loro ipotizzata responsabilità penale diretta, si vedano *ex multis*, in senso critico, A. GIANNINI, *Criminal Behavior and Accountability of Artificial Intelligence Systems*, The Hague, 2023, in specie 128 s. con attenta analisi della letteratura straniera; nonché B. FRAGASSO, *Intelligenza artificiale*, cit., 613 s.

[17] Così sottolinea C. MENECH, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in M. FACCIOLI (a cura di), *Profili giuridici della robotica e dell'intelligenza artificiale in medicina*, Napoli, 2022, 9 s., in specie 23.

[18] Cfr. nella vasta bibliografia in argomento, S. CANESTRARI, *Il consenso informato e il rifiuto informato delle cure come "baluardi" di intangibilità corporea. Riflessioni a margine della l. 219/2017*, in *Per una ragione artificiale. In dialogo con Lorenzo d'Avack su Costituzione, ordine giuridico e biodiritto*, Roma, 2023, 137 s.; L. EUSEBI, *Il consenso informato e le disposizioni anticipate di trattamento*, in A. OLIVA, M. CAPUTO (a cura di), *Itinerari di medicina legale e delle responsabilità in campo sanitario*, Milano, 2021, 418 s.; già A. VALLINI, *Trattamento medico e consenso informato del paziente*, Roma 2012 con ampi richiami bibliografici e giurisprudenziali.

[19] Nel tormentato succedersi di orientamenti sul ruolo del consenso del paziente, quale fondamento di legittimazione dell'attività medico chirurgica, basti qui il richiamo alla sentenza della Cass. sez. un. pen., ud. 28 dicembre 2008, dep. 21 gennaio 2009, n. 2437, con nota di F. VIGANÒ, *Omessa acquisizione del consenso informato del paziente e responsabilità penale del chirurgo: l'approdo (provvisorio?) delle Sezioni Unite*, in *Cass. pen.*, 2009, 1811 s.

specifici (anche a prescindere dai limiti posti dal segreto industriale), come la c.d. opacità con cui i sistemi operano, la cripticità del linguaggio, i contenuti dei data base e dei possibili *bias* cognitivi, in generale gli effetti di imprevedibilità del *machine learning* o addirittura l''imperscrutabilità' delle *black box*[20].

Anche per queste ragioni l'informazione non può essere eccessiva, potendo essere anzi opportuno tacere nei dettagli l'intero novero dei possibili anche più improbabili rischi, dipendenti dalle caratteristiche tecniche del sistema, per non instillare spropositate paure. Il consenso potrebbe essere addirittura viziato, se l'informazione andasse oltre la "*capacità di comprensione*" del destinatario[21], richiamata espressamente dall'art. 33 Codice di deontologia medica e da valutare, quindi, anche dal punto di vista informatico, oltre che medico-terapeutico.

Tale approdo ermeneutico moderato sembra allinearsi alle regole generali stabilite dall'*AI Act*, per cui – ai fini della disciplina relativa alla "*sorveglianza umana*", che ai sensi dell'art. 9 è obbligatoria per un sistema "*ad alto rischio*", come è quello che coinvolge la salute ed i diritti fondamentali della persona (su cui si tornerà *infra*, par. 4), si devono considerare sia i rischi quando il sistema è «*utilizzato* conformemente *alla sua finalità prevista*», sia quelli quando possa essere «*in condizioni di uso improprio* ragionevolmente *prevedibile*» (così l'art. 14, par. 2, *AI Act*; evidenz. aggiunta), in ogni caso rispettando l'obbligo generale di *trasparenza* stabilito dall'art. 50, par. 1, *AI Act*. Esso impone infatti ai fornitori di garantire che i sistemi destinati ad interagire direttamente con le persone fisiche siano progettati e sviluppati in modo che gli interessati siano informati che un sistema IA sta interagendo con loro: obbligo che deve operare, quindi, non solo a tutela del paziente, ma anche del medico e del personale sanitario che ne facciano uso, e che quindi grava in gran parte anche sull'ente sanitario che rende disponibili all'uso tali sistemi, in quanto *deployer* (o gestore), secondo la terminologia dell'*AI Act* e le *Guidelines* pubblicate dalla Commissione europea[22].

---

[20] In argomento basti qui il rinvio all'attenta analisi di A. GIANNINI, *Criminal Behavior and Accountability*, cit., in specie 149 s. Per le ricadute in tema di configurazione ed accertamento del nesso di causalità con l'evento finale si veda *infra* 4.2. e nota 55.

[21] Al riguardo il Comitato nazionale di bioetica nella risoluzione su "*Intelligenza artificiale e medicina: aspetti etici*" del 29 maggio 2020 <https://bioetica.governo.it/it/documenti/pareri-gruppo-misto-cnbcnbbsv/intelligenza-artificiale-e-medicina-aspetti-etici/> ha condivisibilmente evidenziato che «*Il medico deve fornire al paziente la più idonea informazione sulla diagnosi, sulla prognosi, sulle prospettive e le eventuali alternative diagnostico terapeutiche e sulle prevedibili conseguenze delle scelte operate. Il medico dovrà comunicare con il soggetto tenendo conto delle sue capacità di comprensione, alfine di promuoverne la massima partecipazione alle scelte decisionali e l'adesione alle proposte diagnostico terapeutiche.* [*omissis*]». In argomento cfr. condivisibilmente C. DE MENECH, *Intelligenza artificiale e autodeterminazione*, cit., 22, con essenziali richiami.

[22] Le *Guidelines on transparency obligations for providers and deployers of AI systems*, pubblicate dalla Commissione europea il 20 luglio 2026, sono entrate in vigore il 2 agosto 2026. In sintesi, i *providers* devono progettare i sistemi IA in modo tale da garantire che le persone siano esplicitamente informate ogni volta che interagiscono direttamente con un tale sistema, e devono aggiungere "*contrassegni*" leggibili automaticamente, che consentano di individuare i contenuti generati o manipolati dall'IA. A loro volta i *deployers* (o gestori) dei sistemi IA devono informare le persone quando sono esposte a strumenti di riconoscimento delle emozioni e di classificazione biometrica, a *deepfake*, a pubblicazioni di testi in materie di interesse pubblico prive di revisione umana o controllo editoriale.

Sul piano della responsabilità penale la questione è, però, sdrammatizzata dalla evoluzione della giurisprudenza interna, circa il rilievo che potrebbe avere un consenso invalido al trattamento.

Se l'informazione non è "adeguata" certamente il consenso non è valido. Ma come è stato affermato dalla giurisprudenza, dopo numerose oscillazioni, tale vizio può non avere valenza *causale* rispetto all'evento costitutivo di un possibile reato colposo in danno del paziente[23].

In tale ipotesi potrebbe configurarsi una responsabilità civile, non una responsabilità penale, dovendosi escludere che possa dirsi integrato il delitto di violenza privata (*ex* art. 610 c.p.) ed, in caso di evento avverso, di lesioni personali dolose (*ex* art. 582 e 583 c.p.) o di omicidio preterintenzionale (*ex* art. 584 c.p.), come pur era stato ritenuto in precedenza, in casi in cui il trattamento medico chirurgico risultava posto in essere in assenza di consenso o sulla base di un consenso invalido[24].

Il consenso che viene in rilievo in questi casi, infatti, non ha una funzione scriminante, *ex* art. 50 c.p., vale a dire di causa di giustificazione che escluda l'antigiuridicità di un fatto tipico di reato, che sarebbe altrimenti illecito, perché l'attività medica persegue *ab origine* una finalità o, meglio, una funzione diagnostica e terapeutica rispetto ad una patologia in atto: per cui non integra una condotta che possa considerarsi *di per sé* "lesiva" sul piano penale, solo perché può incidere, materialmente e consapevolmente, sull'integrità fisica e sul corpo del paziente. Non si stabilisce, infatti, con essa un rapporto di aggressione e, di conseguenza, non si configura un reato di lesioni dolose, e tanto meno di omicidio preterintenzionale se ne consegua la morte, pur se manchi o sia invalido o venga oltrepassato il limite del consenso all'intervento medico. La responsabilità penale per detti eventi può sorgere, infatti solo per una violazione della *lex artis*, che configuri quindi un rapporto non corretto sul piano diagnostico o terapeutico con il paziente, e sia causale per la determinazione dell'evento. Responsabilità penale che si configurerebbe dunque solo nel caso in cui siano state *dolosamente* omesse informazioni o date informazioni inveritiere per acquisirlo[25], od ancora, sul piano della colpa, se la carenza di informazioni al paziente abbia impedito di acquisire dallo stesso dati ed informazioni rilevanti ai fini del trattamento[26].

In conclusione, una seppur carente informazione (ma non del tutto assente o vuota di contenuto) sul ricorso a sistemi IA nel trattamento medico chirurgico non può di per sé sola fondare una responsabilità penale per eventuali esiti avversi, restando però ferma la necessità – anche per rispetto dell'obbligo di trasparenza imposto dalle menzionate fonti europee – che sia fornito l'essenziale contenuto informativo di cui si è

---

[23] Cass. Sez. un. pen., ud. 28 dicembre 2008, dep. 21 gennaio 2009, n. 2437, sopra cit. a nota 19.

[24] Cfr. la ricostruzione dell'evoluzione giurisprudenziale che leggesi in Cass. pen., Sez. V, ud. 24 novembre 2015, dep. 21 aprile 2016, n. 16678, allineata con quanto espresso dalla citata sentenza delle Sezioni unite.

[25] Per un caso clamoroso di interventi chirurgici realizzati addirittura senza oggettive indicazioni terapeutiche, per scopi di lucro, causando lesioni e morte di pazienti, si veda Cass., Sez. I, 3 aprile 2018 (ud. 22 giugno 2017), n. 14776, a seguito della quale l'imputato Paolo Brega Massone è stato condannato a 21 anni e 4 mesi di reclusione per omicidio preterintenzionale di quattro pazienti, in luogo dell'iniziale condanna all'ergastolo per omicidio doloso.

[26] Così Cass. Sez. IV, 22 maggio 2015, n. 21537.

detto, e sempre che tale carenza non impedisca di acquisire informazioni sullo stato del paziente stesso, rilevanti anche nell'impiego di sistemi IA.

3. Tutela penale dei dati personali a fronte della digitalizzazione e dell'impiego di sistemi di intelligenza artificiale in ambito sanitario.

La progressiva digitalizzazione, che rende possibile e si correla strettamente all'impiego sempre più diffuso di sistemi IA in ambito sanitario, compresa la telemedicina e la robotica, oltre che nei servizi assistenziali, comporta e richiede il trattamento sempre più massiccio di dati personali, in specie "*relativi alla salute*" che appartengono ad una delle "*categorie particolari*" individuate dall'art. 9, par. 1, *GDPR*[27].

Il trattamento di tali dati – destinati a confluire nel "*Fascicolo sanitario elettronico*" (FSE) e nella "*Cartella clinica elettronica*" (CCE), convergendo poi tutti nell'"*Ecosistema dei dati sanitari*" (EDS), su cui si tornerà (in specie *infra,* note 33 e 35) – si dovrà collocare anche nel quadro delineato a livello europeo dal citato regolamento dell'Unione sullo "*spazio europeo dei dati sanitari*" (*EHDS Act*)[28].

Si tratta di uno sviluppo necessario per la modernizzazione della sanità, del resto rientrante negli obiettivi dell'area 6 del PNRR, per vero solo parzialmente raggiunti, che coinvolgono, oltre alla *privacy*, anche la *cybersecurity* (richiamata in più parti dell'*AI Act* e della l. n. 132 del 2025, in specie art. 3, commi 1 e 2, nonché 6, comma 2).

---

[27] Abbreviazione d'ora in poi usata nel testo per citare il regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[28] Emanato anche sulla base dell'esperienza pandemica da Covid 19, espressamente richiamata nei Considerando (2) e (3) del regolamento stesso (ad es. per il c.d. *contact tracing*), è entrato in vigore poco dopo l'*AI Act*, ma i termini della sua applicazione sono programmati per varie scadenze successive (*ex* art. 105), a partire dal 27 marzo 2027, ed in specie fino al 27 marzo 2029 per le parti principali, compreso l'uso primario e lo scambio del primo gruppo di categorie prioritarie in tutti gli Stati membri, ed al 27 marzo 2031 per la piena operatività, al fine di consentire agli operatori ed agli enti pubblici e privati interessati di conformarvisi, dopo che la Commissione europea avrà adottato, entro il 27 marzo 2027, diversi atti di esecuzione fondamentali, con regole dettagliate. Senza poter qui entrare nei particolari della complessa disciplina, basti evidenziare che secondo il comunicato ufficiale diffuso dopo l'avvenuta approvazione del Parlamento europeo del 24 aprile 2024, e ripreso nella successiva comunicazione della Commissione europea, l'atto interviene sull'assistenza sanitaria, sulla ricerca e sulla definizione delle politiche in materia, al fine di consentire agli operatori un accesso più rapido alle cartelle cliniche dei pazienti, anche per quelli provenienti da altri paesi dell'UE, grazie all'introduzione di un "*formato europeo*" comune. Il migliore accesso e scambio di dati sanitari non solo comporterà procedure amministrative più rapide ed economiche, ma nel contempo consentirà anche ai ricercatori un accesso ai dati sanitari più efficace e di qualità superiore, per migliorare non solo i trattamenti, ma anche la ricerca. Di qui i vantaggi per i cittadini, cui le norme in materia di *privacy* e sicurezza dovranno garantire che nessuna informazione personale sia condivisa con terzi senza il loro consenso e che i pazienti abbiano sempre la possibilità di aggiungere informazioni, correggere dati errati, limitare l'accesso e ottenere informazioni sul trattamento dei propri dati. Garanzie, per vero, che come si vedrà non sembrano pienamente assicurate dalla normativa vigente. Per una valorizzazione dal punto di vista delle finalità di ricerca cfr. però A. M. S. CALDORO, A. MENDOLA, AI Health *e dati sanitari tra ricerca scientifica uso secondario*, in *Dir. Internet*, n. 3/2026, 409 ss.

In questa sede mi limiterò a considerare quei profili della disciplina in materia di trattamento dei dati personali relativi alla sanità (par. 3.1.), che hanno rilievo per l'applicazione delle fattispecie incriminatrici (par. 3.2) contenute negli artt. 167 e 167-*bis* del d.lgs. 30 giugno 2003, n. 196 e successive modifiche (d'ora in poi Codice *privacy*).

3.1. Sulle fonti e sui limiti del trattamento dei dati sanitari quali dati appartenenti a "categorie particolari".

I dati concernenti la salute appartengono alle "*categorie particolari*" di dati personali (precedentemente qualificati nel nostro Codice *privacy* come "*dati sensibili*" sulla base delle distinzioni portate dall'abrogata direttiva CE 95/46), per cui l'art. 9 par. 1 *GDPR* stabilisce un generale, ma astratto *divieto* di trattamento. In forza del par. 2 è, invece, prevista una lunga serie di eccezioni, che in concreto delineano regole opposte, a partire dal "*consenso esplicito*" dell'interessato, menzionato alla lett. a), che precede le numerose altre ipotesi in cui prevalgono diverse esigenze. Restano in ogni caso da applicare – se non derogate – le previsioni generali degli artt. 5 (comuni principi applicabili) e 6, in specie par. 1, lett. a) *GDPR*, secondo cui il necessario consenso dell'interessato deve essere dato per *specifiche finalità* e va raccolto previa adeguata *informazione*, alla quale l'interessato ha diritto, *ex* artt. 12 e 13 *GDPR*. L'art. 5, lettera c) *GDPR* afferma poi il fondamentale "*principio di minimizzazione*", secondo cui i dati devono essere "*adeguati, pertinenti e* limitati a quanto necessario *rispetto alle finalità del trattamento*" (evidenz. aggiunte), principio espressamente ribadito anche dall'art. 66 *EHDS Act*.

La prima questione che si pone è se il ricorso a sistemi IA nel trattamento di questi dati appartenenti a "*categorie particolari*" debba essere preciso oggetto dell'informativa sulla cui base viene richiesto il predetto consenso ed eseguito il successivo trattamento. La risposta deve essere senz'altro affermativa, pur nei limiti di ragionevolezza e proporzionalità dei contenuti dell'informazione, che non deve essere 'eccessivamente' tecnica, proprio per essere comprensibile dall'interessato, come si è già visto nel precedente par. 2 a proposito del consenso al trattamento sanitario che implichi l'impiego di sistemi IA, il quale presuppone l'adempimento degli obblighi di *trasparenza* discendenti dal diritto dell'Unione europea.

La seconda questione, più complessa e di carattere generale, è in che modo ed in che limiti la digitalizzazione su larga scala ed il ricorso a sistemi IA in questo settore consentano di garantire *effettivamente* il rispetto dei diritti che ha l'interessato in relazione al trattamento dei dati personali "*particolari*" che lo riguardano, ed in specie alla "*minimizzazione*" di quelli raccolti e trattati, nonché al controllo del loro flusso.

Le nuove tecnologie rappresentano, in effetti, un fattore potenzialmente, se non strutturalmente 'antagonista' rispetto a tali diritti e principi garantisti, poiché la raccolta massiva e sistematica, nonché la circolazione di dati anche appartenenti a "*categorie particolari*", che la digitalizzazione consente, è fortemente sollecitata, quando nel trattamento intervengano sistemi di IA, aumentando in termini esponenziali le situazioni in cui la *privacy* viene compressa o addirittura sacrificata.

L'esigenza strutturale di detti sistemi è, infatti, di poter disporre, scambiare e comunicare liberamente la più gran quantità possibile di informazioni, per garantire – a tacere di possibili finalità illecite – la massima precisione e accuratezza nelle diagnosi e nei trattamenti sanitari, oltre che nella ricerca, e nel contempo la miglior organizzazione e gestione dei servizi, nonché allocazione ottimale delle relative risorse umane e finanziarie.

Non si tratta di impedire la soddisfazione di tali esigenze, dato che la raccolta, elaborazione, comunicazione ed utilizzazione massiva dei dati in questione porta a risultati che sono (anche) a favore degli interessati e della loro salute, oltre che della collettività. Piuttosto si tratta di stabilire e far rispettare – il più possibile – i limiti e le condizioni da osservare, perché il relativo trattamento, in tutte le diverse fasi, sia "*lecito*", come ribadisce, quale principio generale, l'art. 4, comma 2, l. 132 del 2025, naturalmente anche per quanto riguarda la condivisione ed il trasferimento transfrontaliero, promosso in particolare dall'*EHDS Act*[29].

Per delineare soluzioni soddisfacenti, che bilancino le diverse esigenze, occorre muovere dalla premessa già evidenziata, che l'«*Accesso […] alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi*» è compreso espressamente fra i sistemi IA classificati "*ad alto rischio*", ai sensi dell'art. 6, par. 2 *AI Act*, come si legge specificamente alla lettera a) del par. 5 dell'elenco contenuto nel suo Allegato III, in quanto essi possono avere un impatto negativo «*sulla salute, sulla sicurezza e sui diritti fondamentali*»[30].

Pertanto, il *training* di tali sistemi è consentito ricorrendo – di regola – soltanto ai c.d. dati sintetici od a "*dati derivati*", che tramite l'anonimizzazione o, se non è possibile, la pseudonimizzazione[31], consentano di non individuare (se non in ipotesi e con

---

[29] Il necessario raccordo sistematico fra la disciplina dell'allora emanando *EDHS Act* ed il regolamento generale sull'intelligenza artificiale del 2024 è evidenziato nel Considerando (68) dell'*AI Act*: dopo aver premesso che «*Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità* a fini di addestramento, convalida e prova dei sistemi di IA» (evidenz. aggiunte), si indica specificamente ad "*esempio*", quelli che riguardano la salute, per cui «*lo spazio europeo di dati sanitari […] agevolerà l'accesso non discriminatorio ai dati sanitari e* l'addestramento di algoritmi di IA *a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale*» (evidenz. aggiunte).

[30] Tale locuzione di sintesi che si legge nel Considerando (48), ricorre in molte altre parti dell'*AI Act*, sia nei suoi Considerando, sia nell'articolato.

[31] L'"*anonimizzazione*" indica il processo mediante il quale un'informazione, originariamente riconducibile a una persona fisica identificata o identificabile, viene trasformata in un dato non più riferibile, direttamente o indirettamente, ad un interessato. Per cui, venendo meno il legame con la persona, non ricade più nella disciplina del *GDPR*. Viceversa, la "*pseudonimizzazione*" è definita dall'art. 4 n. 5, *GDPR* come «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico* senza l'utilizzo di informazioni aggiuntive» (evidenz. aggiunte), fermo restando che tali "informazioni aggiuntive" devono essere conservate separatamente e soggette a misure tecniche ed organizzative idonee. Dunque, la "*pseudonimizzazione*" non elimina il collegamento tra dato ed interessato, ma esso diviene mediato ed indiretto, essendo subordinato alla disponibilità di dette informazioni ulteriori. Quindi rimane un "*dato personale*" soggetto alla disciplina del *GDPR*. In argomento vedi A. M. S. CALDORO, A. MENDOLA,

modalità tassative) l'identità personale dei singoli interessati, cui i dati si riferiscono, acquisendo però tutte le informazioni utili per l'elaborazione statistica, diagnostica, scientifica, ecc.

E viene in rilievo al riguardo la disciplina, più volte aggiornata, del trattamento per finalità di "*ricerca scientifica*" e per "*fini statistici*", di cui si occupa appositamente l'art. 8 l. n. 132 del 2025, dedicato alla "*Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario*", che stabilisce specifiche regole per il trattamento dei dati finalizzato a tali scopi.

In tali ipotesi, il trattamento dei dati sanitari, pur appartenenti alle "*categorie particolari*" di dati di cui si parla, trova una *base giuridica diversa dal consenso* dell'interessato, alla stregua delle previsioni contenute nell'art. 9, par. 2, lett. i) e j) *GDPR*.

Per cui è parzialmente superato il problema del diritto alla "*revoca*" del consenso, riconosciuto in generale quale diritto dell'interessato dall'art. 7, par. 3 *GDPR*, che potrebbe rappresentare un ostacolo a tali trattamenti e scambi di dati, ma di cui, nelle ipotesi indicate, diviene impossibile il suo esercizio, che è così di fatto negato. Significativo, in questa prospettiva, è il citato *EHDS Act*, che regola, fra l'altro, specificamente le condizioni di accesso, trasmissione, portabilità dei dati sanitari elettronici in tutto il territorio dell'Unione, riconoscendo l'interesse pubblico in tale settore, in particolare anche per il c.d. "*uso secondario*" di cui al capo IV (artt. 50 ss. *EHDS Act*), rispetto al quale è garantito all'interessato soltanto un – peraltro reversibile – "*diritto di esclusione*" (art. 71 *EHDS Act*).

Nelle numerose situazioni in cui si può, dunque, prescindere dal consenso esplicito dell'interessato, si devono stabilire specifiche garanzie, come quando – se è "*strettamente necessario*" per rilevare e correggere eventuali "*distorsioni*" – i fornitori di sistemi IA, ed ora anche i *deployers*, sono autorizzati a trattare i dati di cui si è detto rispettando i limiti e le condizioni stabilite dal nuovo art. 4-*bis AI Act*, specificamente rubricato: "*Trattamento di categorie particolari di dati personali ai fini del rilevamento e della correzione delle distorsioni*", oltre che dall'art. 10, par. 5, dello stesso regolamento, rubricato "*Dati e governance dei dati*", parimenti modificato dalla citata riforma dell'*AI Act* (cfr. *supra* nota 2), perché vi sia un allineamento almeno formale, pur con rilevanti esplicite deroghe, a quanto stabilito dal *GDPR*[32].

Quanto all'ordinamento interno, occorre menzionare, oltre al citato art. 8 l. 132 del 2025, l'art. 2-*sexies* del Codice *privacy*, su cui si tornerà anche per la sua rilevanza ai fini penali (*infra* 3.2.1) rubricato: *"Trattamento di categorie particolari di dati personali*

AI Health *e dati sanitari*, cit., par. 4, 415 ss. e, per l'ulteriore nozione di "*dati sintetici*", in specie 418-419 e nota 51.

[32] Al riguardo occorre richiamare la disciplina generale sulla c.d. *governance* dei dati, di cui al regolamento (UE) 2022/868 (*Data Governance Act*: *DGA*), applicato dal 24 settembre 2023, rispetto a cui bisogna considerare anche il capo VI del citato *EHDS Act,* dedicato alla *"Governance e coordinamento europei"*, che prevede l'istituzione di un apposito Comitato che agevoli la cooperazione e lo scambio di informazioni in materia di dati sanitari tra gli Stati membri e la Commissione (art. 92 ss.). Su tale disciplina dovrebbe incidere, nella prospettiva della semplificazione, l'altro regolamento *Digital Omnibus* proposto dalla Commissione europea il 19 novembre 2025 COM(2025) 837 final, in corso di esame davanti al Parlamento europeo.

necessario per motivi di interesse pubblico rilevanti". Tale norma richiama, ma in realtà va oltre il disposto dell'art. 9, par. 2, *GDPR*, in quanto elenca una serie di fonti europee ed interne, di rango non soltanto legislativo, dalle quali si possa desumere che i trattamenti siano «*necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g)*» del predetto art. 9 *GDPR*, così statuendo: «*qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge* o di regolamento o da atti amministrativi generali *che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*» (evidenz. aggiunte)[33].

Il comma 2 dello stesso art. 2-*sexies* del Codice *privacy* precisa che «*si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o* connessi *all'esercizio di pubblici poteri*» (evidenz. aggiunta) nelle numerosissime materie specificamente elencate, fra cui, alla lettera u), sono menzionati i «*compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica*».

Per le finalità di ricerca e statistica, rilevano poi specificamente, nel Capo III del Titolo VII del Codice *privacy*, ad esse dedicato, gli artt. 106, 110 e 110-*bis*, che riguardano rispettivamente le "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*", la "*Ricerca medica, biomedica ed epidemiologica*" ed il "*Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici*", con cui non sembra puntualmente coordinato il citato art. 8 l. n. 132 del 2025.

In forza della prima norma è individuato un lungo elenco di garanzie che i soggetti pubblici e privati devono rispettare nel trattamento dei dati per le predette finalità, da prevedere nelle rispettive "*regole deontologiche*", a partire dal contenuto e dalle modalità anche semplificate dell'informativa (lettera b), fino a quelle dei casi in cui si può prescindere dal consenso (lettera d).

Al riguardo, l'art. 110 Codice *privacy* afferma che «*il consenso dell'interessato* non è necessario» non solo «*quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j)*» *GDPR*, ma anche «*quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno* sforzo sproporzionato, *oppure rischia di rendere impossibile o di* pregiudicare gravemente il conseguimento delle finalità *della ricerca*» (evidenz. aggiunte), con un rinvio dunque a valutazioni ampiamente discrezionali, in contrasto

---

[33] Il comma 1-*ter* di detto articolo, inserito dal d.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla l. 29 aprile 2024, n. 56, prevede – con un'ampiezza inusitata, certamente incompatibile con la riserva di legge che dovrebbe governare la materia – che il «*Ministero della salute disciplina, con uno o più decreti […], l'interconnessione a livello nazionale dei sistemi informativi su base individuale, pseudonimizzati, ivi incluso il fascicolo sanitario elettronico (FSE) compresi quelli gestiti dai soggetti*» elencati al comma 1-*bis* (inserito dal d.l. 8 ottobre 2012, n. 139, convertito dalla l. 3 dicembre 2021, n. 205, e modificato dalla menzionata normativa del 2024) "*o da altre pubbliche amministrazioni*" (sic!), definendo altresì le caratteristiche e disciplinando «*un ambiente di trattamento sicuro all'interno del quale vengono messi a disposizione dati anonimi o pseudonimizzati, per le finalità istituzionali di ciascuno*» di tutti i predetti soggetti. Sulla distinzione però fra "*anonimizzazione*" e "*pseudonimizzazione*" si veda la precedente nota 31.

con la menzionata esigenza di legalità. È vero che in tali ipotesi devono operare le garanzie che dovrebbe disporre il Garante in sede di autorizzazione, in forza della terza norma (art. 110-*bis* Codice *privacy*) introdotta nel 2017 e modificata nel 2024[34], secondo cui ad esso spetta «*autorizzare il trattamento* ulteriore *di dati personali, compresi quelli dei trattamenti* speciali [*rectius*: "*particolari*"] di cui all'articolo 9 del Regolamento, *a fini di ricerca scientifica o a fini statistici* da parte di soggetti terzi *che svolgano* principalmente *tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno* sforzo sproporzionato, *oppure rischia di rendere impossibile o di* pregiudicare gravemente il conseguimento delle finalità della ricerca […]» (evidenz. aggiunte): ma si ripropongono anche per tali trattamenti condizioni analoghe, assolutamente elastiche, su cui si fonda la deroga al principio del consenso. Per di più la disposizione, essendo riferita a trattamenti "*speciali*" e da parte di "*soggetti terzi*", vale a dire non "*titolari*" dei trattamenti stessi, sembra ancor meno chiara nel definire presupposti e limiti della deroga al principio del consenso, rispetto alla generalità dei "*dati sanitari*" possibile oggetto di trattamento.

Tuttavia, nel caso di trattamenti da parte degli "Istituti di Ricovero e Cura a Carattere Scientifico" (IRCCS, qual è ad es. il Centro San Raffaele di Milano), che hanno personalità giuridica di diritto pubblico, questi possono fondarsi sul comma 4 dell'art. 110-*bis* Codice privacy, secondo cui «non *costituisce trattamento* ulteriore *da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'art. 89 GDPR*» (evidenz. aggiunte). Sulle condizioni, anche relative alla valutazione d'impatto (VIP), che i titolari devono obbligatoriamente svolgere e pubblicare in tali ipotesi, si rinvia ai chiarimenti del Garante della *privacy* ed alle "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*", di cui all'allegato A.5 al Codice *privacy*.

Da ultimo, la l. n. 132 del 2025 sull'intelligenza artificiale è intervenuta anche sul trattamento dei dati personali acquisibili nel "*Fascicolo sanitario elettronico*", già oggetto del comma 1-*bis* dell'art. 2-*sexies* Codice *privacy*, introdotto dall'art. 9 d. l. 8 ottobre 2021, n. 139, convertito dalla l. 3 dicembre 2021, n. 205.

Alla stregua di questa più recente norma: «*I dati personali relativi alla salute, privi di elementi identificativi* diretti» (evidenz. aggiunta) «*sono trattati, nel rispetto delle finalità istituzionali di ciascuno, dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle Regioni anche mediante l'interconnessione a*

[34] L'articolo è stato aggiunto dall'art. 28, comma 1, lettera b) della l. 20 novembre 2017, n. 167, recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017*" ed è stato poi novellato nei termini riportati nel testo, mentre l'art. 44 d.l. 2 marzo 2024, n. 19, convertito dalla l. 29 aprile 2024, n. 56, ha modificato anche il primo comma dell'art. 110, attribuendo opportunamente al Garante il compito di individuare le garanzie da osservare, in sostituzione del semplice obbligo di consultarlo.

livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il 'Fasciolo Sanitario Elettronico' (FSE), aventi finalità compatibili *con quelle sottese al trattamento, con le modalità e per le* finalità fissate con decreto del Ministro *della salute, ai sensi del comma 1, previo parere del Garante, nel rispetto di quanto previsto dal Regolamento, dal presente codice, dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e dalle linee guida dell'Agenzia per l'Italia digitale in materia di interoperabilità*» (evidenz. aggiunte)[35].

A fronte di questa gran quantità di enti legittimati a trattare "*dati personali relativi alla salute*", rispetto ai quali è garantita solo l'assenza di dati identificativi "*diretti*", di cui non è chiaro il regime, le regole del trattamento sono stabilite dal Ministro della salute, con proprio "*decreto*" sottoposto al mero *parere* del Garante della *privacy*, da ritenere peraltro non vincolante, in mancanza di tale specificazione.

Per cui non persuade che venga meno il suo pieno controllo e che fonti di rango secondario, compresi decreti ministeriali e perfino regole deontologiche, possano concretamente disciplinare e restringere, in modo incisivo, la garanzia e l'esercizio di diritti fondamentali, quali sono quelli che vengono in rilievo, a partire dal principio del consenso esplicito ed informato, per finalità specificamente determinate, in violazione della riserva di legge che dovrebbe valere – oltre che ai fini penali di cui si dirà *infra* par. 3.2 – in materia di tutela dei diritti fondamentali della persona[36], tanto più esposti a rischio quando intervengano, nel trattamento, sistemi IA, che in quest'ambito, come detto, sono classificati "*ad alto rischio*" dall'*AI Act*.

Senza considerare che gli incroci fra i molteplici dati, compresi quelli "*personali derivati*" o "*sintetici*", può portare anche alla re-identificazione degli interessati, nonostante l'anonimizzazione o la pseudonimizzazione di cui si è detto (cfr. *supra* nota 31), che il comma 2-*bis* dell'art. 9 l. n. 132 del 2025 intende favorire consentendo *sempre* il trattamento ad esse finalizzato, benché si tratti dei dati appartenenti a "*categorie particolari*" da ricondurre all'art. 9 par. 1 *GDPR*.

Il necessario e ragionevole bilanciamento fra diritti fondamentali, interessi già meritevoli di tutela e nuove esigenze confliggenti, dovrebbe in conclusione essere definito con maggiore chiarezza e sistematicità dal legislatore nazionale, in sintonia con quello europeo, salvaguardando *effettivamente* l'esercizio del diritto all'autodeterminazione informativa, oltre che quello all'autodeterminazione nei trattamenti sanitari, con norme tassative di rango primario.

---

[35] Un'analoga situazione, con le debite distinzioni, si può ravvisare anche per la disciplina dei trattamenti oggetto delle "*Cartelle sanitarie elettroniche*", contenenti dati amministrativi su prestazioni, dispositivi sanitari e quant'altro, tenendo conto che in quest'ambito possono venire in rilievo anche le tematiche dell'*Internet of Things* (IoT), date le caratteristiche dei più moderni dispositivi sanitari.

[36] Come noto, l'art. 8 CDFUE, che sancisce il diritto fondamentale alla "*Protezione dei dati di carattere personale*", di cui vale la pena di riportare il testo, richiama espressamente la garanzia della legge, quale fonte di disciplina del trattamento dei dati personali: «1. *Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.* 2. *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo* previsto dalla legge. *Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.* 3. *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*» (evidenz. aggiunte).

Se, da un lato, va certamente superata l'ottocentesca ed individualistica nozione di *privacy* quale diritto "a restare soli", dovendo i sistemi IA essere posti in grado di accedere all'enorme quantità di dati anche personali reperibili in rete, per sfruttare le più avanzate capacità di veloce trattamento e rapidissima connessione, offerte dalle nuove tecnologie, al fine di potenziare nella misura massima possibile l'attendibilità delle valutazioni e previsioni probabilistiche su cui si fondano le diagnosi e le analisi dei fattori e delle situazioni di rischio, dall'altro devono essere salvaguardati non meno efficacemente gli interessi giuridici da proteggere ed in specie i diritti fondamentali che fanno capo alla persona.

In questa prospettiva può essere di importante supporto la garanzia di *trasparenza* dei trattamenti di dati personali, enunciato dall'art. 5 par. 1, lett. a) *GDPR*, che trova un importante riflesso nel citato art. 50 *AI Act*, e relative *Guidelines* (cfr. *supra* nota 22), al fine di contrastare la rilevata 'opacità' dell'IA, assicurandone l'esplicabilità alla stregua degli specifici obblighi che gravano sui fornitori dei sistemi IA "*ad alto rischio*" e che sono diretti a garantire che il loro funzionamento sia "*sufficientemente trasparente da consentire ai deployers di interpretare l'output*" del sistema ed "*utilizzarlo adeguatamente*" (art. 13 *AI Act*). Esigenza di trasparenza che dovrebbe logicamente rispecchiarsi, a valle, con lo stesso contenuto, anche nel rapporto con gli interessati e gli utenti tutti, vale a dire con i pazienti oltre che con il personale sanitario.

3.2. Rilevanza penale delle violazioni in materia di trattamento di dati sanitari.

Venendo all'esame dei profili penali connessi alla violazione della complessa disciplina dei dati personali di natura sanitaria, che si è sopra sinteticamente ricostruita, vengono in rilievo gli artt. 167 e 167-*bis* del nostro Codice *privacy*, nella formulazione portata dal d.lgs. 10 agosto 2018, n. 101 (di adeguamento alle disposizioni del *GDPR*), che puniscono rispettivamente il "*Trattamento illecito di dati*" e la "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*".

Si tratta di fattispecie delittuose strutturate quali norme sanzionatorie dei precetti extra-penali fissati dal *GDPR* e dal Codice *privacy*, cui espressamente rinviano per indicare le condotte illecite che li violano, richiedendo però requisiti ulteriori, che restringono la punibilità.

Il primo – che compare in entrambe le norme – è rappresentato dal «*fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato*», che l'agente deve perseguire con la propria condotta, ma che non è necessario che consegua, perché si abbia la consumazione del reato, come è proprio delle fattispecie denominate a dolo specifico[37].

---

[37] In argomento cfr. Cass, sez. III, ud. 11 dicembre 2013, dep. 28 gennaio 2014, n. 3683, secondo cui «*la struttura finalistica*» del reato a dolo specifico «*è incompatibile con la forma del dolo eventuale*» che postula l'accettazione solo in via ipotetica, seppur avverabile, del conseguimento di un risultato. Sulla struttura e sulle caratteristiche delle fattispecie c.d. a dolo specifico, che in realtà non caratterizzano una particolare forma di dolo, bensì stabiliscono un nesso teleologico con cui viene più precisamente tipizzato lo stesso "fatto" costitutivo del reato, sia consentito rinviare a L. PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi*

Il secondo requisito selettivo – previsto solo dall'art. 167 – è rappresentato dall'evento consumativo, costituito dall'oggettivo "*nocumento*", che è ravvisabile in qualsiasi pregiudizio giuridicamente rilevante, di natura anche non patrimoniale[38], e che deve essere dolosamente causato dal reo con la propria condotta, vale a dire con la volontà consapevole di produrlo[39].

Tali elementi distinguono gli illeciti penali in esame dagli illeciti di natura amministrativa, che sono previsti dai regolamenti europei in materia (art. 83 *GDPR*, artt. 99-101 *AI Act* ed art. 99 *EHSD Act,* che richiama anche i suoi artt. 63 e 64), i quali stabiliscono sanzioni pecuniarie molto severe, applicabili anche ad enti e persone giuridiche, e per cui non è richiesto il dolo. Per questo non può dirsi violato il principio del *ne bis in idem* (così anche il Considerando (168) dell'*AI Act*), di per sé applicabile al concorso fra sanzioni penali e sanzioni amministrative che abbiano carattere punitivo, avendo la fattispecie penale una diversa configurazione, fermo il necessario rispetto delle condizioni enucleate dalla giurisprudenza europea, fra cui, *in primis*, la proporzionalità del trattamento sanzionatorio complessivo[40].

3.2.1. Trattamento illecito di dati sanitari.

Senza soffermarsi sul delitto previsto dal primo comma dell'art. 167 Codice *privacy*, che non interessa in questa sede (riguardando violazioni relative ai servizi di comunicazione elettronica), vengono in rilievo i due più gravi delitti previsti nei

---

finalistici' delle fattispecie penali, Milano, 1993, in specie 501 s. sulla sua funzione tipizzante, da tener distinta da quella della colpevolezza cui appartiene invece il dolo, per cui incide sull'offesa (505 s.); nonché 595 ss. sulla compatibilità, nei limiti ivi precisati, delle fattispecie così strutturate con il dolo eventuale.

[38] Così costante giurisprudenza: cfr. Cass. Sez. III, 7 febbraio 2017, dep. 14 giugno 2017, n. 29549; Cass. Sez. III, 23 novembre 2016, dep. 28 marzo 2017, n. 15221.

[39] La giurisprudenza oggi prevalente considera il "*nocumento*" quale evento consumativo, che deve pertanto essere preveduto e voluto o comunque accettato dall'agente quale conseguenza della propria azione, indipendentemente dal fatto che costituisca o si identifichi con il fine dell'azione stessa (così Cass. Sez. III, 28 marzo 2017 cit.; Cass. Sez. III, 5 febbraio 2015, dep. 6 ottobre 2015, n. 40103), superando il precedente censurabile orientamento, non rispettoso del principio di colpevolezza, che ne affermava, invece, la natura di mera condizione obiettiva di punibilità, applicabile quindi oggettivamente (così Cass. Sez. III, 16 luglio 2013, dep. 18 febbraio 2014, n. 7504; Cass. Sez. III, 28 maggio 2004, dep. 9 luglio 2004, n. 30134).

[40] Sulla faticosa elaborazione delle Corti europee e delle nostre Corti costituzionale e di Cassazione, circa la portata di tale principio, che costituisce un diritto fondamentale valevole anche in ambito comunitario, sia consentito rinviare, per brevità, a L. PICOTTI, *Doppio binario sanzionatorio* e ne bis in idem*: verso un accettabile epilogo del lungo dialogo fra le Corti?*, in A. CADOPPI, P. VENEZIANI, ALDROVANDI (a cura di), *Legalità e diritto penale dell'economia. Studi in onore di Alessio Lanzi*, Roma, 2020, 510 s., ed ai richiami giurisprudenziali e bibliografici ivi contenuti. Si veda altresì M. SCOLETTA, *Il principio del* ne bis in idem *e i modelli punitivi "a doppio binario"*, in C. AMALFITANO, M. D'AMICO, S. LEONE (a cura di), *La Carta dei diritti fondamentali*, cit., 315 s.; e più di recente, prendendo spunto da C. Cost., 10 maggio 2022, n. 149, R. M. VADALÀ, *L'impianto sanzionatorio "punitivo" della legge sul diritto d'autore: il diritto al* ne bis in idem *nella permanenza del doppio binario*, in *Leg. Pen.*, 15 aprile 2023.

successivi commi 2 e 3, puniti – «*salvo che il fatto costituisca più grave reato*»[41] – con la reclusione da uno a tre anni.

In particolare, la fattispecie di cui al comma 2 punisce chiunque, al fine specifico sopraddetto, «*procedendo al trattamento dei dati personali di cui agli articoli 9 e 10*» *GDPR*, fra cui dunque anche quelli relativi alla salute sopra richiamati, «*in violazione […] delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies*» del Codice *privacy* «*arreca nocumento*» all'interessato.

Come si è sopra esposto, la prima norma extrapenale, cui rinvia la fattispecie incriminatrice, afferma semplicemente che «*sono ammessi*» i trattamenti dei dati delle categorie particolari in esame, quando siano «*necessari per motivi di interesse pubblico rilevante*»: interesse che dovrebbe essere definito dal comma 2, il quale però rinvia ad una molteplicità di ben 25 materie eterogenee, fra cui, alla lettera u), sono menzionati anche i «*compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario*» (cfr. *supra* par. 3.1), sempre che siano trattamenti «*effettuati da soggetti che svolgono compiti di interesse pubblico o* connessi *all'esercizio di pubblici poteri*» (evidenz. aggiunta) e «*siano previsti*» da fonti dell'Unione europea o nazionali, anche secondarie, quali i regolamenti interni, richiamate del tutto genericamente, senza che ne sia indicato specificamente il nucleo precettivo.

Poiché la condotta punibile è quella di "*violazione*" dei molteplici ed indefiniti precetti che potrebbero dunque venire in rilievo per il generico rinvio operato alle menzionate norme extrapenali, non si comprende come i destinatari, e neppure l'interprete più avveduto, possano stabilire con la necessaria sicurezza quando si abbia l'integrazione del reato.

Appare, quindi, violato il principio di stretta legalità in materia penale, sia sotto il profilo della riserva di legge, che, come si è detto, dovrebbe già valere in materia di disciplina del trattamento dei dati personali (cfr. *supra* nota 36), sia sotto quello della determinatezza o tassatività della fattispecie incriminatrice, di cui agli artt. 25, comma 2 Cost. nonché 1 c.p., da leggere nella prospettiva della "prevedibilità" delle conseguenze sanzionatorie della propria condotta, ricavabile dall'art. 7 CEDU, secondo l'insegnamento della Corte europea dei diritti dell'uomo circa la "qualità" che deve avere la legge penale[42].

Non viene invece in rilievo, in questa sede, il rinvio anche all'art. 2-*octies*, che contiene "*Principi relativi al trattamento di dati relativi a condanne penali e reati*", mentre interessa il richiamo alternativo alle "*misure di garanzia di cui all'articolo 2-septies*", che riguardano specificamente "*il trattamento di dati genetici, biometrici e relativi alla salute*".

---

[41] Come ha precisato la giurisprudenza, tale clausola di riserva presuppone, perché operi in concreto il meccanismo dell'assorbimento, che il reato più grave sia posto a tutela del medesimo bene-interesse tutelato dal reato meno grave che deve essere assorbito (così Cass. Sez. II, 7 maggio 2013, dep. 5 settembre 2013, n. 36365, che ha escluso che il delitto in esame potesse ritenersi assorbito nel delitto di ricettazione).

[42] Cfr. paradigmaticamente Corte eur. dir. uomo, Sez. II, sent. 31 dicembre 2019, Parmak e Bakir c. Turchia, ricc. 22429/07 e 25195/07, in *questa Rivista*, 19.2.2020, con una "scheda" ricca di riferimenti giurisprudenziali e bibliografici di Fr. MAZZACUVA, *La Corte europea ritorna sul principio di "prevedibilità" del diritto penale tra irretroattività, retroattività della* lex mitior *e* prééminence du droit.

Neppure tale norma contiene in realtà precetti specifici, da cui possa evincersi quale sia la condotta punibile in caso di loro «*violazione*», dato che rimanda *in toto* alle «*misure di garanzia disposte dal Garante*» con un proprio «*provvedimento*», che deve rispettare le condizioni e le modalità di adozione previste nel secondo e nel terzo comma, fermo restando che – con superfluo richiamo contenuto nel comma quarto, visto il principio di primazia del diritto dell'Unione – esse devono altresì rispettare «*quanto previsto dall'articolo 9, paragrafo 2*» *GDPR*, di cui sopra si è detto (par. 3.1).

Neppure in tale ipotesi il principio di stretta legalità in materia penale può dirsi compiutamente rispettato: né sotto il profilo della riserva di legge, per il rinvio a fonti secondarie senza che con "*sufficiente determinatezza*" ne siano vincolati i contenuti da fonti primarie, né sotto quello della tassatività della fattispecie incriminatrice, nonché della "prevedibilità" delle conseguenze sanzionatorie, di cui si è appena detto, poiché anche in questo caso appare arduo per i destinatari e per lo stesso più attento interprete individuare quali siano le condotte concretamente punibili per la "*violazione*" dei molteplici precetti che potrebbero venire in rilievo.

3.2.2. Trasferimento illecito di dati sanitari all'estero.

Il comma 3 dell'art. 167 Codice *privacy* stabilisce che la stessa pena della reclusione da uno a tre anni si applica altresì a chi, al medesimo fine specifico già esaminato ed arrecando nocumento, procede «*al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49*» *GDPR*.

La prima norma europea richiamata stabilisce che «*il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione* garantiscono un livello di protezione adeguato. *In tal caso il trasferimento non necessita di autorizzazioni specifiche*» (evidenz. aggiunte).

In questa prima ipotesi l'oggetto del divieto può dirsi sufficientemente determinato, essendo integrato da una decisione della Commissione, che trova fondamento e limiti nella norma regolamentare primaria.

La seconda norma del *GDPR* cui rinvia la fattispecie penale in esame prevede, invece, che, in mancanza di una siffatta decisione della Commissione europea sul «*livello di protezione adeguato*» che può offrire il paese terzo o l'organizzazione internazionale, il titolare o il responsabile del trattamento può trasferire dati personali verso di essi «*solo se* ha fornito garanzie adeguate *e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*» (evidenz. aggiunte).

In tal caso l'oggetto della possibile violazione è molto più elastico, dipendendo da una valutazione *ex post* di adeguatezza del livello di protezione che viene fornito dallo stesso titolare o responsabile del trattamento, comprese le norme vincolanti d'impresa, senza la cui determinazione appare svuotato lo stesso diritto a mezzi di ricorso effettivi.

Infine, l'art. 49 *GDPR* ammette «*il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale*» qualora si verifichi

almeno una delle sette condizioni elencate dalle lettere da a) a g), fra cui spicca – in questa sede – la prima: vale a dire che «*l'interessato abbia esplicitamente* acconsentito *al trasferimento proposto, dopo essere stato* informato dei possibili rischi *di siffatti trasferimenti per l'interessato, dovuti alla* mancanza di *una decisione di adeguatezza e di* garanzie adeguate» (lettera a), nonché, in alternativa, la quinta (lettera d), vale a dire che «*il trasferimento sia necessario per* importanti *motivi di interesse pubblico*» (evidenz. aggiunte), aperta dunque ad una valutazione ampiamente discrezionale.

Senza approfondire ulteriormente l'analisi ermeneutica di questa complessa disciplina extrapenale, che presenta molti profili di criticità, in relazione all'interesse pubblico sotteso alla ricerca e sperimentazione in ambito sanitario, tanto più rilevanti se riportati all'integrazione della fattispecie penale in esame, per ragioni analoghe a quelle appena esposte (par. 3.2.1.), è interessante segnalare che il menzionato *EHDS Act* costituisce un'ulteriore e nuova fonte che legittima, ed anzi persegue l'uso transfrontaliero, sia primario (art. 23 ss.), sia secondario (art. 75 ss.), proprio di dati inerenti alla salute in altri paesi dell'Unione, nonché il loro trasferimento anche verso paesi terzi (art. 88), alle condizioni stabilite dalle medesime norme europee, cui si deve per brevità rinviare. Trattandosi di disposizioni di carattere speciale, perché riferite espressamente ai dati sanitari, dovranno prevalere – in caso di conflitto – su quelle generali del *GDPR* sopra richiamate.

Di conseguenza, mentre il loro rispetto dovrebbe escludere l'applicabilità dell'art. 167 comma 3 Codice *privacy* in esame, la loro violazione non potrebbe, allo stato, integrare il delitto da esso previsto, sia perché l'*EHDS Act* non è ancora formalmente applicabile per questa parte (cfr. *supra* note 3 e 28), sia soprattutto per il divieto di analogia in materia penale, dato che il trasferimento "*fuori dei casi consentiti*" è esclusivamente riferito alle norme del *GDPR* espressamente elencate.

3.2.3. Comunicazione e diffusione illecite di dati sanitari.

Gli altri due delitti che vengono in rilievo sono quelli previsti rispettivamente dal primo e dal secondo comma dell'art. 167-*bis* Codice *privacy*, inserito dal d.lgs. n. 101 del 2018, che considera specificamente la nuova dimensione globale del *web* e la tematica dei *big data*, per cui assumono maggior disvalore le condotte di illecita "*comunicazione*" o "*diffusione*" che vengono incriminate[43].

---

[43] Tali due termini, che tipizzano le condotte punibili, vanno interpretati in base alle loro definizioni normative, contenute nell'originaria formulazione dell'art. 4, comma primo, rispettivamente lett. l) ed m) del Codice *privacy* (così *ex multis* Cass. Sez. III, 9 giugno 2006, dep. 23 giugno 2006, n. 22059), peraltro poi abrogato dal d.lgs. 101 del 2018, in quanto le definizioni andrebbero ricavate solo dall'art. 4 *GDPR*. Ma poiché questo non fornisce espressamente il contenuto di queste due nozioni, ritengo si debba far riferimento, a fini ermeneutici, a quelle nazionali pur abrogate, secondo cui la prima consiste nel «*dare conoscenza dei dati personali* a uno o più soggetti determinati *diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma,* anche mediante la loro messa a disposizione o consultazione» (evidenz. aggiunte), mentre la seconda è da ravvisare nel «*dare conoscenza dei dati personali* a soggetti indeterminati, *in qualunque forma,* anche mediante la loro messa a disposizione o

Non solo la pena è pertanto più grave (reclusione da uno a sei anni, sempre «*salvo che il fatto costituisca più grave reato*»), ma non è previsto, per questi due reati, che sia altresì arrecato un «*nocumento*». Di conseguenza, essendo esclusa la necessità dell'evento dannoso, la consumazione è anticipata al momento della commissione delle condotte tipizzate, bastando che l'agente persegua il fine specifico di cui si è detto, senza necessità che lo consegua.

In entrambe le fattispecie è dunque punito «*chiunque comunica o diffonde*» con il fine menzionato «*un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*». Ma mentre nell'ipotesi del primo comma è richiesto che la condotta sia «*in violazione degli articoli 2-ter, 2-sexies e 2-octies*» del Codice *privacy*, in quella del secondo comma occorre che sia posta in essere «*senza consenso*» […] «*quando il consenso dell'interessato* è richiesto *per le operazioni di comunicazione e di diffusione*» (evidenz. aggiunte).

Per la prima fattispecie, dunque, vi è un rinvio – per quanto interessa in questa sede[44] – alla medesima disciplina extrapenale dell'art. 2-*sexies* Codice *privacy* (cfr. *supra* par. 3.1), richiamata anche dalla già esaminata fattispecie di cui all'art. 167 comma 2, valendo, dunque, anche per questa le medesime osservazioni critiche sopra espresse (par. 3.2.1), mentre l'evidente concorso apparente di norme andrà risolto sulla base del principio di specialità (*infra* in questo paragrafo).

Nell'ipotesi del secondo comma, invece, il requisito della mancanza di consenso «*quando […] è richiesto per le operazioni di comunicazione e diffusione*» implica una preliminare ricerca, da parte dell'interprete, delle relative condizioni e regole, non sempre coincidenti con quelle sopra esaminate sulla necessità di consenso e sulla possibilità di derogarvi, che sono riferite genericamente a tutte le operazioni di «*trattamento*» (cfr. *supra* par. 3.1), ma non specificamente a quelle sole di «*comunicazione e diffusione*» che integrano la fattispecie penale.

Certamente un'ipotesi che può ricorrere è quella del già esaminato art. 49 *GDPR*, cui rinvia anche l'art. 167, comma 3, Codice *privacy*, che punisce fra le varie condotte, anche il «*trasferimento*» illecito di dati personali all'estero, irrogando tuttavia una pena minore per la sua violazione (par. 3.2.2).

Il concorso apparente di norme che potrebbe anche in questo caso configurarsi, va parimenti risolto nel senso della prevalenza della fattispecie in esame, in quanto "*speciale*" sotto il profilo degli elementi costituivi, sia per la mancanza dell'evento consumativo del «*nocumento*», sia per la più specifica condotta tipizzata («*comunicazione o diffusione*»: c.d. specialità per sottrazione), ritenuta dal legislatore più grave e meritevole di una pena più elevata, per cui opera – in ogni caso – il c.d. assorbimento.

---

consultazione» (evidenz. aggiunte).

[44] Viceversa non rilevano in questa sede il rinvio all'art. 2-*ter*, che disciplina la «*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*», essendo dal suo secondo comma espressamente esclusi i trattamenti «*ricompresi nelle particolari categorie di dati di cui* all'articolo 9» *GDPR* soggetti a specifica regolamentazione; e neppure quello di cui all'art. 2-*octies* Codice *privacy*, che contiene i «*Principi relativi al trattamento di dati relativi a condanne penali e reati*» parimenti non rilevante in questa sede.

In entrambe le fattispecie di cui all'art. 167 *bis* in esame, anche l'oggetto delle condotte incriminate presenta ampi margini di indeterminatezza, potendo riguardare non solo «*un archivio automatizzato*», ma anche una sua mera «*parte sostanziale*», mentre il relativo contenuto deve essere costituito da dati personali oggetto di trattamento «*su larga scala*»: nozioni tutte di cui non sono affatto chiari i parametri definitori, da ricavare per quanto possibile da pertinenti acquisizioni informatiche.

Emerge, in definitiva, ancora una frizione sotto molteplici aspetti con il principio di stretta legalità, in particolare per carente tassatività o determinatezza della fattispecie incriminatrice, oltre che per carente "*prevedibilità*" delle conseguenze sanzionatorie, profilandosi anche in tal caso plausibili censure di incostituzionalità, *ex* artt. 25 comma 2 e 117 comma 1 Cost. in relazione all'art. 7 CEDU.

Il confine della possibile rilevanza penale delle violazioni dell'articolata e complessa disciplina che consente il trattamento, anche con l'utilizzo di sistemi IA, di dati sanitari digitalizzati senza consenso dell'interessato, coinvolge altresì quelli che confluiscono nel "*Fascicolo sanitario elettronico*" e nelle "*Cartelle elettroniche sanitarie*", destinati a essere poi convogliati nel c.d. "*Ecosistema dei dati sanitari*" (EDS).

È un confine che non è affatto agevole determinare, anche perché è in forte ed attuale evoluzione, se si considerano le innovative fonti in materia, a partire dai recenti regolamenti sopra citati (*AI Act*, aggiornato dal *Digital Omnibus AI,* nonché *EDHS Act*), destinati ad essere applicati in tempi via via successivi, fino alle disposizioni della legge n. 132 del 2025 sull'intelligenza artificiale ed alle ulteriori norme delegate, da ultimo approvate[45].

Il lavoro dell'interprete ed, in specie, dei cultori del diritto penale, appare dunque impegnativo, ma da sviluppare ulteriormente in futuro, per l'importanza del settore in esame.

4. Impiego di sistemi di intelligenza artificiale e responsabilità penale del sanitario per eventi avversi.

4.1. Premesse generali sulla tutela penale in materia.

Un tema assai rilevante che si pone di fronte all'impiego di sistemi IA in medicina, sia in ambito diagnostico, sia in ambito terapeutico ed assistenziale, specie se possono operare direttamente nell'ambiente esterno anche con un *hardware* (come nella chirurgia robotica), è quello della c.d. colpa medica per eventi avversi, in cui entrino in gioco detti sistemi.

Possono infatti venire in rilievo, sotto il profilo penale, gli artt. 589 e 590 c.p., che puniscono rispettivamente l'omicidio colposo e le lesioni personali colpose, di cui l'art. 590-*sexies*, comma 2, c.p. (introdotto dall'art. 6 l. 6 marzo 2017, n. 24, c.d. legge Gelli-Bianco) limita l'ambito applicativo ai soli casi di «*imperizia*», «*quando sono rispettate le*

[45] Cfr. *supra,* nota 4.

raccomandazioni previste dalle linee guida […] ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali»[46].

Si tratta di reati di evento c.d. a forma libera, per cui qualsiasi azione od omissione, che sia causa o concausa della morte o delle lesioni personali del paziente, *ex* artt. 40, comma primo c.p. e, per la responsabilità omissiva, comma secondo (secondo cui «*non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo*»), nonché 41 c.p. (secondo cui il «*concorso di cause […] non esclude il rapporto di causalità*», salvo che – ai sensi del capoverso – quelle «*sopravvenute*» siano «*state da sole sufficienti a determinare l'evento*»), può far sorgere la responsabilità dell'esercente la professione sanitaria, a condizione che – oltre a detto nesso oggettivo di causalità, o meglio, come si dirà, d'imputazione oggettiva (*infra* par. 4.2) – si accerti anche la sua colpa personale (*infra* par. 4.3).

Come ricordato in esordio della presente analisi (*supra* par. 1), non può accettarsi che, sol perché vi è stato l'utilizzo di sistemi IA (ad es. nella diagnosi o nel trattamento), sia da escludersi la colpa penalmente rilevante per le caratteristiche di (relativa) "imprevedibilità" degli *output* forniti e dei 'comportamenti' posti in essere in misura più o meno autonoma da tali sistemi[47].

---

[46] Sul controverso impatto dell'art. 590-*sexies* c.p. sulla limitazione della responsabilità penale del sanitario, fra i numerosissimi contributi si vedano M. MATTHEUDAKIS, *La punibilità del sanitario per colpa grave. Argomentazioni intorno ad una tesi*, Roma 2021, in specie cap. III, 71 ss.; L. RISICATO, *Il nuovo statuto della colpa medica: un discutibile progresso nella valutazione della responsabilità del personale sanitaria* in *Leg. Pen.*, 5 giugno 2017; per un attento bilancio G. CANZIO, *Linee evolutive del sistema della responsabilità in ambito sanitario*, in *Responsabilità sanitaria, rischio clinico e valore della persona*, 2022, 3 s., con essenziali indicazioni bibliografiche e giurisprudenziali. Fra queste si veda in specie Cass. sez. un., 21 dicembre 2017, n. 87701, Mariotti, Rv. 272174-75-76, annotata da C. CUPELLI, *La legge Gelli-Bianco nell'interpretazione delle Sezioni Unite: torna la gradazione della colpa e si riaffaccia l'art. 2236 c.c.*, in *Dir. pen. cont. – Riv. trim.*, 2017, 12, 135, con ulteriori rinvii.

[47] Si vedano le Raccomandazioni contenute nella citata risoluzione adottata a conclusione dei lavori della Sezione I del XXI Congresso internazionale dell'*Association Internationale de Droit Pénal* del 2024, di cui *supra* a nota 8. In materia, cfr. i successivi approfonditi contributi di L. D'AMICO, *La misura della (im)prevedibilità*, cit., in specie 220 s. e B. FRAGASSO, *Intelligenza artificiale e responsabilità penale,* cit., in specie 358 s.; volendo *ex multis*, in sintesi, anche L. PICOTTI, *Responsabilità penale e sistemi di IA*, cit., in specie 101 ss.
Più in generale, nel dibattito penalistico si rinvia ai contributi di R. BARTOLI, *La responsabilità medica tra individuale e collettivo: rischi, regole, centri di imputazione*, in D. BIANCHI (a cura di), *Distribuzione del rischio sanitario tra responsabilità dell'organizzazione e responsabilità individuali*, Torino 2021, 80 s.; A. CAPPELLINI, *L'"allocazione della colpa" nella responsabilità penale sanitaria,* ivi, 54 s.; B. PANATTONI, *Profili penali dell'interazione uomo-macchina nell'ambito della responsabilità medica,* in L. PICOTTI (a cura di), *Automazione, Diritto e Responsabilità. Atti del Convegno dii studi del 21-22 ottobre 2022 conclusivo della ricerca condotta dal team "Automazione, Diritto e Responsabilità" (AUDIRR) nell'ambito del Progetto d'eccellenza del Dipartimento di Scienze giuridiche dell'Università di Verona*, Napoli, 2023, 269 s. Cfr. anche N. AMORE, E. ROSSERO, *Robotica e intelligenza artificiale nell'attività medica*, cit., 185 s., TERRIZZI, *Medical devices e diritto penale,* cit., 177 s. e, volendo, L. PICOTTI, *Robotica ed intelligenza artificiale in medicina: possibili aspetti di rilievo penale*, in M. FACCIOLI (a cura di), *Profili giuridici dell'utilizzo della robotica*, cit., 89 s.; nel più esplorato campo della responsabilità civile si veda, oltre all'interessante contributo comparatista di G. GUERRA, *Profili di responsabilità del produttore del robot chirurgico nell'ordinamento americano*, ivi, 57 s., *ex multis* N. RIZZO, *Strutture della responsabilità civile e intelligenza artificiale: i problemi in medicina*, ivi, 1 s.; M. FACCIOLI, *Principi e categorie della responsabilità sanitaria alla prova della telemedicina*, in L. PICOTTI (a cura di), *Automazione, Diritto e Responsabilità*, cit., 245 s., con ampie indicazioni bibliografiche anche di carattere generale.

Si creerebbe, altrimenti, uno spazio d'impunità od irresponsabilità penale, che necessariamente si espanderebbe, per gli sviluppi impetuosi e gli impieghi sempre più estesi delle nuove tecnologie, rispetto ad offese a beni giuridici primari e diritti fondamentali della persona, quali la vita e l'incolumità personale, che richiedono e già ricevono una consolidata protezione penale di fronte a fatti commessi con i mezzi e le modalità tradizionali.

Se la tutela penale non può quindi venir meno, occorre allora rivedere criticamente i criteri d'imputazione, soprattutto della causalità e della colpa, alla luce delle peculiari caratteristiche dell'impiego di tali sistemi[48], rispettando naturalmente le garanzie della legalità e della personalità della responsabilità penale, stabilite a livello costituzionale.

Si tratta, infatti, di fondamentali *principi sovraordinati* dello Stato di diritto, che devono restare intangibili. Viceversa, come ho già evidenziato nella premessa metodologica di un mio precedente contributo[49], le *categorie dogmatiche* ed i dogmi concettuali, in quanto tali, non devono essere considerati immutabili, perché sono il risultato di un processo di formazione storicamente determinato, frutto dello sviluppo della dottrina e della giurisprudenza, oltre che della legislazione, affermatesi in concrete condizioni storiche, culturali, sociali, politiche e filosofiche – nonché, aggiungo, di determinati stadi di sviluppo tecnologico – che quindi con il loro mutare non possono che modificarsi, come del resto è già avvenuto in passato, come paradigmaticamente dimostra l'evoluzione dei concetti di "azione" e di "colpa", e la stessa possibilità di configurare una responsabilità "da reato" delle persone giuridiche e degli enti.

Si deve, dunque, muovere dalla constatazione che un sistema IA non è riducibile ad un mero strumento passivo od oggetto statico, nelle mani dell'uomo, come sembrerebbe far pensare il termine di 'utilizzo' di un robot (ad es. nella chirurgia o nell'assistenza) o di un sistema diagnostico basato sull'IA, perché esso non resta nel pieno e costante dominio dell'agente umano, in ogni fase di operatività fino all'*output*, come potrebbero essere un bisturi o dati clinici, nonché la letteratura medica disponibili all'operatore, al contrario interagendo, in una sorta di 'dialogo", con l'operatore stesso, per cui residua un margine più o meno ampio di autonomia. Per cui tale mutamento tecnologico permea di sé il nuovo tipo di rapporto uomo-macchina, che si distingue da quello rappresentato dal comune ricorso alle risorse informatiche, e dunque non può non impattare anche sulle categorie penalistiche su cui si fonda la responsabilità dell'uomo.

Per questo deve distinguersi concettualmente la semplice "automazione" di singole seppur avanzate funzioni, il cui *output* resta pur sempre sotto il pieno controllo finale dell'uomo (come ad es. per la ricerca automatizzata di testi in banche dati selezionate o dati anamnestici risalenti del paziente, ecc.), dalla vera e propria

---

[48] Ritiene invece che considerazioni riconducibili ad esigenze di tutela ed a valutazioni di politica criminale non possano «*incidere sull'interpretazione e sull'applicazione delle norme in materia di causalità*» B. FRAGASSO, *Intelligenza artificiale*, cit. 393, e nota 100. Obiezione cui rispondo nel testo richiamando anche un mio precedente lavoro.

[49] L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale*, par. 2, 3 s.

"autonomia" decisionale ed operativa, che – basandosi su tecniche di *machine learning* e su algoritmi adattivi, fin dalla ricerca, raccolta e selezione di dati ed informazioni fra le enormi quantità reperibili nel *web* (*big data*) o acquisibili dalla realtà esterna tramite adeguati sensori visivi, acustici, termici ecc., certamente non disponibili se non in minima parte al singolo operatore – porta ad *output* decisionali e comportamentali che possono essere caratterizzati da 'imprevedibilità' e possibile 'opacità' del processo che vi è alla base[50].

L'interazione fra uomo e macchina, alla quale il sanitario sempre più ricorre, è infatti complessa, ma non può essere definita in termini di effettiva "collaborazione", dato che – almeno allo stato attuale dello sviluppo tecnologico – va escluso il riconoscimento di una "soggettività" propria del sistema IA in quanto tale, od addirittura una sua capacità penale, per cui possa essere destinatario di precetti e sanzioni.

Esso, infatti, non possiede una libertà cosciente di autodeterminazione, qual è quella richiesta a fondamento dell'imputabilità ai fini penali, e neppure appaiono concepibili sanzioni (seppur *sui generis*) applicabili nei suoi confronti, perché non potrebbero perseguire le funzioni retributiva, di prevenzione generale e speciale proprie della pena[51].

Nondimeno occorre tener conto del 'diaframma', che può essere anche temporale, che si crea fra l'atto umano e l'offesa dei beni giuridici penalmente rilevanti, posta in essere o condizionata, specie nell'ultimo tratto, dall'impiego di detti sistemi IA, cui l'agente umano ed, in particolare, il personale sanitario 'trasferisce' importanti attività, interagendo anche dialogicamente e facendovi, in maggior o minor misura, affidamento per la superiore capacità cognitiva, decisionale ed operativa – sicura, precisa ed immediata – che tali sistemi possiedono. Tanto che può configurarsi un obbligo, anche giuridicamente rilevante (ad es. sul piano della colpa, in caso di omissione), di ricorrere ad essi per garantire il miglior trattamento che la scienza e la tecnologia rendono disponibile[52].

---

[50] Tale distinzione, ma con diversa significazione, è trattata anche da B. FRAGASSO, *Intelligenza artificiale e responsabilità penale,* cit., cap. II, 43 s., che parla di «*automazione*» quale «*capacità* [dell'algoritmo] *di raggiungere un determinato obiettivo in assenza di intervento umano*» (in specie 48) o più ampiamente quale «*capacità di un sistema di compiere una determinata attività (o parte di essa), agendo direttamente sul mondo reale o virtuale, in assenza di un intervento umano*» (in specie 53 S.), contrapponendola alla nozione di «*autonomia*» che sarebbe invece connotata dalla «*capacità dell'algoritmo di agire in situazioni di incertezza*» (in specie 48 s.): ma l'A. poi finisce per riconoscere anche l'effettiva «*autonomia*» decisionale di detti sistemi, quale possibile fattore interruttivo della causalità (cap. VII; par. 3.2, 392 s.): nozione quest'ultima che caratterizza la stessa definizione normativa generale di un sistema IA contenuta nell'art. 3, n. 1 *Ai Act* (riportata *supra* nota 15).

[51] Rinvio al riguardo ai punti 4 e 5 del par. 1 delle Raccomandazioni dell'AIDP, cit. a nota 8. Per un'attenta trattazione e riferimenti ulteriori cfr. successivamente A. GIANNINI, *Criminal Behavior and Accountability*, cit., 117 s.; nonché L. D'AMICO, *La misura della (im)prevedibilità*, cit., Parte seconda, cap. I, 123 s., e B. FRAGASSO, *Intelligenza artificiale e responsabilità penale,* cit., cap. XI, 613 s.; più brevemente, volendo, anche L. PICOTTI, *Intelligenza artificiale e diritto penale,* cit., 295 s.

[52] Su tali profili convincentemente U. PAGALLO, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Milano, 2022.

Ai fini della responsabilità penale per eventi avversi che possano derivarne, non si può dunque che risalire ai soggetti umani che 'stanno dietro' ai sistemi IA, i quali decidono di impiegarli, utilizzandoli nel proprio "interesse" o "vantaggio", seppur non egoistico, riferibile alla miglior terapia o al più efficace trattamento che devono, e così possono e scelgono di porre in essere.

4.2. Sul nesso causale.

Tale interazione 'dialogica' fra l'uomo ed i sistemi IA, che è instaurata per volontà cosciente del primo, rappresenta il primo anello all'origine della catena causale che può portare all'evento avverso.

Data la menzionata struttura a forma libera dei reati che possono venire in rilievo e sopra indicati, è sufficiente – dal punto di vista della tipicità della condotta, nel rispetto del principio di legalità – qualsiasi 'contributo' eziologico alla produzione dell'evento, anche di natura omissiva (*ex* art. 40, primo e secondo comma c.p.), ad es. per mancato controllo o mancata sorveglianza, essendo configurabile una posizione di garanzia del medico o del personale sanitario competente, rispetto alle fonti di pericolo per la vita, la salute, l'incolumità del paziente ad essi affidato, che costituiscano rischi specifici nascenti dalla patologia oggetto di cura o dal trattamento posto o da porre in essere, ricadendo nella sfera degli obblighi di vigilanza ed intervento che su di essi incombono, e che non vengono certo meno perché decidono di ricorrere a sistemi IA[53].

Pertanto, anche di fronte alle c.d. *black box*, non essendo esimente l'*error in causa*, la scelta dell'operatore di ricorrere ed affidarsi all'IA appare integrare quanto meno una 'condizione necessaria' da cui dipende la causazione dell'evento, che può inserirsi od aggiungersi alla catena che – a monte – va dall'ideatore al programmatore, dal produttore al fornitore, ed – a valle – fino al "gestore" (o *deployer*) nonché all'utilizzatore finale del sistema, in conformità al c.d. principio di equivalenza dei contributi causali – c.d. *conditio sine qua non* – ricavabile dal menzionato art. 41 c.p., dato che con l'eliminazione mentale dell'antecedente o degli antecedenti in esame, verrebbe meno l'evento stesso.

Al riguardo, l'autonomia dei sistemi IA – data l'ampia regolamentazione che a livello europeo e nazionale ha ormai e sempre più avrà la loro produzione, distribuzione, utilizzazione, anche attraverso l'operato dei vari organismi tecnici e "spazi normativi"

---

[53] Sull'ambito di rilevanza penale di tale sfera di obblighi cfr. in generale M. CAPUTO, *Colpa penale del medico e sicurezza delle cure*, Torino 2017, nonché i riferimenti di cui alle precedenti note 46 e 47. Sul tema della posizione di garanzia che può essere ascritta in generale ai vari soggetti che intervengono nella produzione e distribuzione di sistemi IA, si veda lo *Special Report* di C. GRANDI, *Positive Obligations (Garantestellung) Grounding Criminal Responsibility for not Having Avoided an Illegal Result Connected to the Ai Functioning*, in L. PICOTTI, B. PANATTONI (eds.), *Traditional Criminal Law Categories and AI*, cit., 67 s., ed in particolare le 'raccomandazioni' conclusivamente formulate, 73 s.; nonché I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, 2021, 83 s., 106; in posizione cauta L. D'AMICO, *La misura della (im)prevedibilità*, cit., 287 s., 305.

(c.d. *regulatory sandboxes*) previsti dal diritto europeo e nazionale[54] – non può considerarsi un fattore del tutto *eccezionale* od *assolutamente* imprevedibile, tale da interrompere (*ex* art. 41, capoverso, c.p.) la catena causale, salvo che soverchianti e straordinarie anomalie possano far risalire la responsabilità ad anelli anteriori della menzionata catena, al termine della quale si colloca l'utilizzatore finale.

Nonostante la possibilità tecnica ed anzi l'obbligo di tracciare l'*iter* che ha portato all'evento (cfr. art. 12 *AI Act* che regola anche la durata della conservazione delle registrazioni obbligatorie), può certamente residuare una difficoltà di prova per la precisa ricostruzione ed individuazione delle caratteristiche e cause delle anomalie che lo abbiano concretamente determinato[55], rispetto a cui sia da stabilire l'eventuale sfera di responsabilità umana.

Per superare tali difficoltà, ai fini della tutela risarcitoria di natura civile – che può essere di grande rilievo in ambito sanitario, in alternativa od in aggiunta alla tutela penale – sono stati introdotti (dal citato d.lgs. n. 160 del 2026, in attuazione della delega legislativa di cui all'art. 24, comma 5, lettera d) l. n. 132 del 2025) meccanismi di agevolazione probatoria, con la previsione, in particolare, che l'Autorità giudiziaria ordini «*l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema*» (art. 17) nonché una presunzione semplice (salvo prova contraria) del "*nesso di causalità*" fra la violazione di uno o più obblighi previsti dall'*AI Act* ed il danno prodotto (art. 18). Tali previsioni appaiono in linea anche con quanto stabilisce la direttiva europea sulla responsabilità da prodotto difettoso, estesa ai vizi del *software*, peraltro non ancora attuata nell'ordinamento nazionale[56].

Ma certamente nessuna presunzione è invece applicabile in campo penale, in cui si dovrebbero, piuttosto, valorizzare i criteri della c.d. imputazione oggettiva dell'evento, metodologicamente condivisi da tempo in dottrina[57], secondo cui – fermo il

---

[54] Secondo la definizione fornita dall'art. 3, n. 55 *AI Act* sono «*un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare*». La loro disciplina è poi prevista all'art. 57 *AI Act*, di cui alla successiva nota 65, anche per i riferimenti normativi al diritto nazionale.

[55] Il problema nasce soprattutto con riferimento al citato fenomeno definito *black box* (algoritmico), per cui non sia possibile ricostruire, neppure da parte dei tecnici che hanno progettato i sistemi stessi, *tutti* i singoli anelli della catena che hanno portato in concreto ad un certo *output*, che potrebbe non essere ripetibile: cfr. al riguardo A. GIANNINI, *Criminal Behavior*, cit., 149 s., nonché l'ampia trattazione di B. FRAGASSO, *Intelligenza artificiale e responsabilità penale*, cit., 382 s., che prospetta, quale possibile fattore interruttivo del nesso causale, l'autonomia ed opacità complessiva del sistema IA.

[56] Si veda la Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio, in GUUE 2024/2853 del 18.11.2024 serie L, It, per cui vi è termine per il suo recepimento fino al 9 dicembre 2026.

[57] Su questa complessa tematica, basti in questa sede il rinvio, nella dottrina italiana, alla monografia di M. DONINI, *Imputazione oggettiva dell'evento. 'Nesso di rischio' e responsabilità per fatto proprio*, Torino 2006, anche per ampie indicazioni bibliografiche specie alla dottrina tedesca. Da ultimo si veda anche M. F. CARRIERO, *Causalità e imputazione. Le leggi scientifiche tra metodo e dogmi*, Torino, 2025. Nella giurisprudenza di legittimità, si veda in sintesi, sulla scia della famosa sentenza della Cass., sez. un. 10 luglio 2002, dep. 11 settembre 2002, n. 30328 (c.d. Franzese), più di recente Cass., sez. IV, 2 ottobre 2024, dep. 11 dicembre 2024, n. 45399, con nota di TRIMBOLI, *Responsabilità medica e leggi statistiche: la Cassazione ribadisce che il rapporto di*

richiamato presupposto della *conditio sine qua non* – non occorre che si abbia poi la spiegazione scientifica o tecnica di ogni singolo passaggio della catena causale, da cui si è originato l'evento finale, purché questo rappresenti la specifica *concretizzazione del rischio* (o dei rischi) cui sono stati esposti i beni giuridici da salvaguardare – in questi casi, specificamente, la vita e l'incolumità personale – dall'utilizzo dei sistemi IA, soccorrendo criteri normativi, desunti da correlazioni statistiche od anche ipotetiche ragionevolmente plausibili, a fronte della mancanza di fondate spiegazioni scientifiche alternative.

Per evitare o ridurre tali difficoltà, possono essere introdotte fattispecie che anticipino la soglia della tutela penale sanzionando, ad esempio, quali reati preparatori, l'impiego di "dispositivi medici" – in cui possono rientrare i sistemi IA anche quali loro componenti – non autorizzati o pericolosi, od irregolarmente acquisiti tramite appalti non rispettosi della disciplina di sicurezza in materia, finalizzata a garantirne elevati *standard*[58].

Ma un'altra via, che sembra quella prescelta dal nostro legislatore delegato, è di far ricorso a reati di pericolo concreto, anziché di evento. Ed infatti l'art. 12 d.lgs. 160 del 2026 ha aggiunto – nel capo I del Titolo VI della parte speciale del codice, fra i delitti contro l'incolumità pubblica «*mediante violenza*» (non, dunque, contro la persona, di cui al Titolo XII) – l'art. 437-*bis* c.p., rubricato "*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*"[59]. La norma contiene quattro nuove fattispecie penali, di cui una punibile anche a titolo di colpa (oltre a due circostanze aggravanti speciali), per cui la si analizzerà nel par. 4.4, dopo aver esaminato il tema della colpa nell'ambito in esame, in cui maggiormente può venire in rilievo.

4.3. Sulla colpa "personale".

Fondamentali principi di garanzia in materia di responsabilità penale pacificamente richiedono che – a differenza della responsabilità civile – la sua

---

causalità tra omissione ed evento deve essere verificato alla luce di un giudizio di alta probabilità logica, in *questa Rivista*, 8 gennaio 2025.

[58] Lo stesso *AI Act*, all'art. 62, par. 3, lett. d), prevede che l'Ufficio per l'IA, istituito presso la Commissione europea, in conformità al sistema di *Governance* sopra richiamato a nota 4, intraprenda fra l'altro azioni per «*valutare e promuovere la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA*».

[59] Questo il testo dei primi due commi: «*Chiunque, nella progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio,* omette misure tecniche *idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero* omette misure di sorveglianza umana *è punito, qualora dal fatto derivi un* pericolo concreto per la vita o l'incolumità individuale, *con la reclusione da uno a cinque anni. Qualora dal fatto derivi un* pericolo concreto *per l'incolumità pubblica o per la sicurezza dello Stato, la pena è della reclusione da due a otto anni.*

Salvo che il fatto costituisca più grave reato, chiunque, al di fuori dei casi indicati al comma 1, altera *sistemi di intelligenza artificiale ad alto rischio è punito, qualora dal fatto derivi un* pericolo concreto *per la vita o l'incolumità individuale, con la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo concreto per l'incolumità pubblica o per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni*» (evidenz. aggiunte).

attribuzione si basi, oltre che sull'elemento oggettivo, su di un rimprovero giuridico "*personale*", quantomeno di natura colposa, come si ricava dall'art. 27, commi 1 e 3, Cost.

Colpa penale che diverge da quella civile, non solo essendo esclusa ogni forma di responsabilità oggettiva o per fatto altrui, ad es. del dipendente, ma anche di responsabilità c.d. per posizione, nonché – come già detto a proposito del nesso di causalità – qualsivoglia ricorso a presunzioni legali[60].

Si è già sottolineato, trattando del consenso al trattamento sanitario (*supra* par. 2), che ci troviamo nel campo di attività lecite di base, dato che la volontaria invasione anche materiale della sfera corporea del paziente non costituisce alcuna "*lesione*" personale, ai sensi dell'art. 582 c.p., non essendo causa di una "*malattia*" ma, al contrario, è un intervento diretto a favore del paziente e della sua salute, in conformità alla funzione terapeutica della condotta, che è diretta a curare patologie preesistenti (con i debiti adattamenti rispetto alla chirurgia ed ai trattamenti estetici).

In tale contesto, l'impiego di sistemi IA può offrire la massima utilità, per l'entità e qualità di informazioni ampie ed aggiornate, di cui l'operatore può disporre in tempo reale, limitando l'eventualità di errori ed incrementando la precisione e la rapidità delle diagnosi, dei trattamenti e degli interventi anche chirurgici od a distanza[61].

Il nodo problematico, tuttavia, è quello delle c.d. regole cautelari sulla cui violazione si fonda la colpa, dovendo essere rispettate dall'operatore ed, a monte, dalla catena di soggetti coinvolti, che vanno dal produttore e fornitore, al gestore (*deployer*) di tali sistemi, trattandosi di attività *lecite*, ma *pericolose*.

Al riguardo, il modello di comportamento dell'*homo eiusdem condicionis et professionis* – dal quale si ricavano usualmente le regole di diligenza, prudenza e perizia la cui violazione configura la c.d. colpa generica ai fini penali[62] – non appare agevolmente applicabile quando intervengano sistemi IA, che in quanto tali non sono persone umane ed operano ciascuno con proprie caratteristiche e modalità tecniche, in

---

[60] Sui fondamenti generali della colpa, nella letteratura contemporanea cfr. G. FORTI, *Colpa ed evento nel diritto penale*, Milano, 1990, nonché F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, Padova, 1993, con i necessari richiami ai molteplici autorevoli contributi precedenti. In tempi più recenti si vedano le voci raccolte nel volume diretto da M. DONINI, *Reato colposo. Enc. Dir. – I Tematici*, 2021, ed ivi in specie D. CASTRONUOVO (voce) *Colpa penale*, 200 s. con ampi richiami bibliografici.

[61] A quest'ultimo proposito si parla di "telemedicina", sulle cui specifiche problematiche basti qui il rinvio a M. FACCIOLI, *La responsabilità civile di medici e strutture sanitarie nell'esercizio della telemedicina*, in *Responsabilità Medica*, 2, 2025, 156 ss.; sui profili penali M. MATTHEUDAKIS, *Peculiarità della telemedicina e responsabilità penale colposa*, in *Responsabilità Medica*, 1, 2026, 31 ss.

[62] Una particolare questione pone il tema della "*perizia*", dato che il vigente art. 590-*sexies* c.p., sopra ricordato, dichiara non punibile l'imperizia del sanitario (ma non la sua negligenza od imprudenza) quando lo stesso abbia seguito le «*raccomandazioni previste dalle linee guida […] ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali*», sempre che siano «adeguate alla specificità del caso concreto». Raccomandazioni e buone pratiche che allo stato non considerano i sistemi IA, per cui dovrebbero essere integrate ed aggiornate, con riferimento esplicito anche all'impiego delle tecnologie in questione, includendo i casi e modi in cui si possa o addirittura si debba fare ricorso ad essi, nella diagnosi, nella terapia ed eventualmente anche nell'assistenza. tal senso si veda già A. FIORELLA, *Responsabilità penale dei Tutor e dominabilità dell'Intelligenza Artificiale. Rischio permesso e limiti di autonomia dell'Intelligenza Artificiale*, in R. GIORDANO (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano 2022, 657; mentre sulle proposte di riforma anche di tale norma si veda *infra*, nota 71.

relazione ai diversi campi di operatività, di cui sopra si è fatto cenno (cfr. par.1): per cui non sembrano agevolmente ricavabili delle "regole cautelari" preesistenti e generalizzabili, da rispettare nella prospettiva di prevenzione dei rischi nel loro operato in parte autonomo, che si configura, come detto, quale dinamica interazione 'dialogica' con l'utilizzatore[63].

Piuttosto occorre muovere dal parametro, assai ampio e generale, della "miglior scienza ed esperienza", inclusa quella informatica e robotica, da riferire agli specifici settori in cui operano detti sistemi, e da concretizzare in relazione alle diverse azioni ed ai necessari interventi dell'agente umano che 'sta dietro' gli stessi, il quale che deve prioritariamente acquisire la necessaria formazione tecnica, rispettando poi la disciplina specifica relativa alle diverse fasi della progettazione, produzione, immissione in commercio, distribuzione e gestione, fino all'utilizzazione finale, non potendosi indirizzare il rimprovero penale (soltanto) a quest'ultima fase, per l'eventuale esito infausto o lesivo, od il pericolo concretamente cagionato ai beni protetti, dato il richiamato principio dell'equivalenza causale di tutti i contributi eziologicamente rilevanti per la causazione dell'evento (art. 41 c.p. e *supra* par. 4.2).

Il parametro d'imputazione più adeguato deve dunque essere quello della c.d. colpa specifica, che presuppone l'esistenza di *preesistenti* regole scritte di comportamento, di natura cautelare, destinate ai diversi ambiti di competenza, aventi funzione di prevenzione o, quantomeno, di riduzione dei rischi ad un livello accettabile (quello del c.d. rischio consentito)[64], nel bilanciamento con i vantaggi che porta l'impiego dei sistemi IA.

Regole caratterizzate, dunque, da specifiche connotazioni tecniche, che devono essere rispettate innanzitutto dai *produttori* e poi trasferite ai *fornitori* ed agli *utilizzatori* dei sistemi "*ad alto rischio*", vincolati dagli interventi delle Autorità competenti al rilascio di autorizzazioni all'uso e al controllo di tali sistemi nei diversi ambiti, secondo le

---

[63] E' stato prospettato ed enfatizzato in dottrina un cambio di paradigmi determinato dal ricorso massivo ai sistemi IA in medicina, che farebbe superare il modello dell'*Evidence-Based Medicine* (incentrata su una metodologia di ricerca scientifica condotta dall'uomo, al quale rimane poi la scelta e responsabilità del singolo caso clinico), su cui si fondano anche le Linee Guida, a favore di una *Data-Driven Medicine*, affidata invece agli algoritmi di apprendimento automatico, basata sui *Big Data* e capace addirittura di indicazioni terapeutiche sullo specifico caso clinico, alle quali il medico devolverebbe le decisioni e gli interventi, con conseguente spostamento anche della responsabilità dagli operatori – ridotti a meri esecutori delle indicazioni cogenti dei sistemi algoritmici – alle strutture che li implementano (così N. AMORE, E. ROSSERO, *Robotica e intelligenza artificiale nell'attività medica*, cit., 199 s., 215 s.). Pur suggestiva nella prospettiva avveniristica in cui si colloca, la tesi non è convincente, perché estremizza una contrapposizione che va invece ricondotta ad una sinergia fra uomo e macchina, da regolare e garantire anche tramite una chiara e vincolante disciplina giuridica, incontrovertibilmente orientata, a livello interno e sovranazionale, alla "*dimensione antropocentrica*" (art. 1, comma 1 l. n. 132 del 2025), in forza del quale «*i sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati* nel rispetto dell'autonomia e del potere decisionale dell'uomo» (art. 3, comma 3, evidenz. aggiunte), ribadito espressamente per l'ambito medico dall'art. 7, comma 5, secondo cui il loro "*supporto*" (come si dirà nel testo) deve lasciare «*impregiudicata la* decisione, *che è* sempre rimessa agli esercenti *la professione medica*» (evidenz. aggiunte).

[64] In argomento, cfr. le Raccomandazioni AIDP citate alla nota 8, in specie par. 2. *On the need for extra-criminal regulation, standards and obligations*, nn. 6-9 e, con rinvio ad esse, L. PICOTTI, *Categorie tradizionali del diritto penale*, cit., 14.

indicazioni espresse dai molteplici organismi tecnici e sulla base delle esperienze acquisite negli "*spazi normativi*" (c.d. *regulatory sandboxes*), previsti dal diritto europeo e nazionale [65]. Su tali basi soltanto possono poi definirsi regole specifiche, che devono essere basate – come detto – sulla 'miglior scienza ed esperienza' del settore.

Viene in rilievo al riguardo anche il già citato art. 9 *AI Act*, che prevede per i sistemi "*ad alto rischio*", l'obbligo di istituire un «*sistema di gestione dei rischi*», «*inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita* […], *che richiede un* riesame *e un aggiornamento costanti e sistematici*» (evidenz. aggiunte), da documentare e mantenere nel tempo. Rientrano nelle varie fasi, in cui si deve articolare tale gestione dei rischi, l'identificazione, l'analisi e la valutazione di quelli «*noti e* ragionevolmente prevedibili *che il sistema [...] può porre per la salute, la sicurezza e i diritti fondamentali*», sia quando è usato «*conformemente alla sua finalità prevista*» sia quando lo sia «*in condizioni di* uso improprio *ragionevolmente prevedibile*» (lettere a) e b); evidenz. aggiunte). Obblighi che dunque incombono anche sugli operatori sanitari, facenti capo ai rispettivi enti, in quanto *disployer* di sistemi "*ad alto rischio*" (sul punto si tornerà *infra* par. 4.4.).

La colpa dell'agente umano non potrebbe del resto escludersi per il sol fatto che un esito avverso, dovuto ai concreti comportamenti dei sistemi IA, non sia stato "previsto", essendo in generale sufficiente, per il rimprovero colposo, la *possibilità* di prevedere (c.d. prevedibilità), non tanto il singolo fatto concreto che si sia verificato, quanto la tipologia di fatti ed eventi cui esso appartenga e che le misure cautelari non rispettate, in quanto disponibili, di cui si è detto, avevano per l'appunto la finalità di evitare. La colpa non richiede, infatti, la previsione concreta dell'evento causato, come dimostra normativamente la circostanza aggravante comune dei reati colposi di cui all'art. 61, n. 3 c.p., che si applica quando siano commessi «*nonostante la previsione*

---

[65] L'*Ai Act* prevede all'art. 57 che gli Stati membri istituiscano «*spazi di sperimentazione normativa per l'IA*» che ai sensi del par. 5 hanno il compito di garantire «*un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente. Tali spazi di sperimentazione possono comprendere prove in condizioni reali soggette a controllo*». A livello interno, il menzionato d.lgs. n. 179 del 2026 dedica dunque l'intera sez. VI del capo II agli "*Spazi di sperimentazione normativa*" (cfr. *supra*, nota 45), prevedendo *in primis* l'istituzione di uno «*Spazio di sperimentazione italiano per l'IA […] finalizzato a sostenere la condivisione di migliori pratiche mediante la cooperazione con le autorità competenti, nonché a promuovere l'innovazione e la competitività e a favorire lo sviluppo di un ecosistema dell'intelligenza artificiale*» che deve contribuire altresì «*all'apprendimento normativo, inteso come sviluppo di un approccio regolatorio fondato sulle evidenze emerse dalla sperimentazione*». Lo stesso *AI Act* prevede del resto all'art. 60 la possibilità di «*Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA*», nonché, nell'ambito delle apposite strutture di *Governance* di cui al Capo VII, l'istituzione di un "*Gruppo di esperti scientifici indipendenti*" che fornisca consulenza all'Ufficio per l'IA, anche sui "*rischi sistemici*" in particolari dei modelli di IA per finalità generali. Infine, occorre segnalare che in materia operano anche le Commissioni Tecniche di Standardizzazione (UNI, ISO, CEN-CENELEC) che devono definire fra l'altro le regole pratiche per i sistemi "*ad alto rischio*", con riferimento ai sistemi di gestione dei rischi e qualità dei dati, tracciabilità, registrazione degli eventi (*logging*) e robustezza tecnica, interfacce per la trasparenza e la supervisione umana obbligatoria.

dell'evento» (c.d. colpa cosciente). Ma si deve trattare di eventi che, pur imprevisti – che sono peraltro quelli maggiormente temibili – siano "*ragionevolmente*" prevedibili.

Ai predetti criteri d'imputazione, che delineano la c.d. misura *oggettiva* della colpa, si deve poi aggiungere l'ulteriore elemento della *rimproverabilità* personale, sia pur di natura normativa e non etica, consistente nella disapprovazione dell'ordinamento giuridico per non aver agito diversamente da quanto in concreto sarebbe stato esigibile, vale a dire possibile e doveroso fare (c.d. misura *soggettiva* della colpa). Valutazione finale individualizzante, di cui resta controversa anche l'estensione[66], non potendosi giungere ad una giustificazione soggettiva di qualsiasi condotta, ma che – pur circoscritta alla presenza di dimostrate anomalie e situazioni del tutto eccezionali, che abbiano impedito di riconoscere la situazione di rischio o di adottare o adeguare le misure per fronteggiarla – appare imprescindibile per rispettare appieno il principio di colpevolezza, senza scivolare in forme occulte di responsabilità oggettiva.

4.4. Sulla "colpa di organizzazione" e sul nuovo delitto colposo di omessa adozione di misure di sicurezza tecniche.

Poiché in ambito sanitario i sistemi IA vengono per lo più impiegati o resi disponibili ai singoli operatori nel contesto di strutture organizzate complesse, come sono le aziende ospedaliere od i presidi sanitari del territorio, le eventuali carenze nella valutazione dei rischi e nell'adozione di adeguate misure di prevenzione, che possano aver reso possibili eventi avversi, potrebbero integrare la c.d. "colpa di organizzazione".

L'ancoraggio della responsabilità penale della persona umana alla colpa specifica, nei termini delineati, sembra integrarsi con tale modello più generale, applicabile nell'ambito di organizzazioni complesse, sulla cui base si imputa la responsabilità "da reato" alle persone giuridiche ed agli enti, ai sensi del d.lgs. 8 giugno 2001, n. 231[67], imponendo di muovere dal necessario *risk assessment*, al quale devono seguire adeguate misure organizzative e cautelari, in funzione dichiaratamente preventiva, con attribuzione di competenze specifiche ed istituzione di un apposito organismo di vigilanza, che deve essere previsto dai "*modelli organizzativi*" (c.d. MOG), al fine di garantire il monitoraggio e la massima attenzione ai segnali d'allarme per eventi avversi, che devono contenere i rischi nell'ambito di quelli accettabili o "consentiti".

---

[66] In argomento, nel risalente dibattito nella dottrina italiana e, prima, tedesca, basti in questa sede il rinvio (anche per le ulteriori indicazioni bibliografiche) al risalente contributo di V. DE FRANCESCO, *Sulla misura soggettiva della colpa*, in *Studi urbinati*, 1977, 273 s.; più recentemente R. BARTOLI, *Colpevolezza: tra personalismo e prevenzione*, Torino, 2005, 177 s.; M. DONINI, *L'elemento soggettivo della colpa. Garanzie e sistematica,* in *Riv. it. dir. proc. pen*., 2013, 137 s.

[67] Nella sterminata letteratura in argomento, con specifica attenzione al tema della responsabilità penale connessa all'uso di sistemi IA, si veda lo *Special Report* di V. MONGILLO, *Corporate Criminal Liability for AI-Related Crimes: Possible Legal Techniques and Obstacles*, in L. PICOTTI, B. PANATTONI (eds.), *Traditional Criminal Law Categories and AI*, cit., 77 s., cui si rinvia anche per l'ampia bibliografia, non solo nazionale.

Su tali basi normative, il concreto rimprovero di colpa alle persone umane, ed all'ente da esse formato, che 'stanno dietro' alla produzione, distribuzione, impiego dei sistemi IA, non potrebbe più considerarsi quale inammissibile «*colpa per non aver previsto l'imprevedibile*», come è stato detto[68], ma per la violazione di quelle cautele, anche organizzative, che stanno 'a monte' e sono specificamente finalizzate ad evitare che si verifichino eventi della tipologia di quello che potrebbe essersi realizzato.

Al riguardo emergono però, *de jure condito*, due limiti applicativi.

Innanzitutto, alla disciplina del d.lgs. 231 del 2001 sono espressamente sottratti gli enti pubblici, salvo che svolgano attività economiche (art. 1, comma 3, d.lgs. n. 231 del 2001). E tali non sono considerate le attività sanitarie, che non perseguono fini di lucro, per cui potrebbero interessare solo le aziende ospedaliere private[69].

In secondo luogo, nell'elenco tassativo dei reati cui si applica la predetta disciplina, non sono inclusi gli omicidi colposi e le lesioni personali colpose, che non siano riferibili a violazione delle regole in materia di salute e sicurezza sui luoghi lavoro (art. 25-*septies* d.lgs. n. 231 del 2001).

Solo in parte sembra aver posto rimedio a tali lacune il recente intervento del legislatore delegato, che ha introdotto il citato art. 437-*bis* c.p., per sanzionare l'omessa adozione di misure di sicurezza tecnica e di sorveglianza umana nei sistemi di intelligenza artificiale "*ad alto rischio*", in cui rientrano, come detto, quelli in ambito sanitario (cfr. *supra*, par. 1).

Più precisamente, la norma prevede, ai commi 1, 2 e 4, tre nuovi delitti punibili a titolo di dolo, consistenti rispettivamente nell'*omissione* di misure tecniche di sicurezza e di sorveglianza umana prescritte per i sistemi IA "*ad alto rischio*", da cui sia derivato pericolo per la vita, l'incolumità pubblica o privata (comma 1, primo periodo), ovvero per la sicurezza della Stato (secondo periodo, che prevede una circostanza aggravante speciale, con aumento della pena di oltre un terzo[70]), nonché nell'"*alterazione*" di tali

---

[68] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. proc. pen.*, 2020, 1771 s.

[69] Per un caso di estensione a società non soltanto private, ma a partecipazione mista, si veda però – in sede cautelare – Cass., sez. II, 9 luglio 2010, dep. 21 luglio 2010, n. 28699, con nota di O. DI GIOVINE, *Sanità ed ambito applicativo della disciplina sulla responsabilità degli enti: alcune riflessioni sui confini tra pubblico e privato*, in *Cass. pen.*, 2011, 1888 s.

[70] La pena base, della reclusione da uno a cinque anni, viene aumentata a quella da due a otto anni. Ma che si tratti di circostanza aggravante speciale, con importanti conseguenza sulla "bilanciabilità" con eventuali circostanze attenuanti, ai sensi dell'art. 69, comma 4 c.p., e non di un titolo autonomo di reato, come invece sostenuto da primi commenti, risulta dall'applicazione dei criteri distintivi stabiliti dalla Corte di Cassazione a sezioni unite, con sentenza 26.6.2022, n. 26351, Fedi, per qualificare la "Truffa aggravata per il conseguimento di erogazioni pubbliche" di cui all'art. 640-*bis* c.p. quale circostanza aggravante speciale della truffa di cui all'art. 640 c.p. Come ho già sottolineato (cfr. L. PICOTTI, *Le disposizioni penali introdotte dal decreto legislativo*, cit., par. 2), il punto più critico della nuova fattispecie è nella mancanza di una disciplina normativa degli obblighi di adozione delle "*misure tecniche di sicurezza*" e delle "*misure di sorveglianza umana*" alle quali devono essere specificamente assoggettati i sistemi "*ad alto rischio*", la cui violazione integra l'omissione costituente la condotta punita dal reato in esame, solo in parte ricostruibile guardando alle prescrizioni dettate dall'*AI Act* per tale categoria di sistemi, peraltro non ancora formalmente applicabili, per la posticipazione del relativo termine al 2 dicembre 2027 a seguito dell'*Omnibus* digitale IA, di cui si è detto alla nota 2.

sistemi, che abbia cagionato analoghi pericoli concreti (comma 2)[71], od, infine, in quello *proprio* dell'«*utilizzatore professionale*» che «*intenzionalmente*» abbia omesso tali misure (comma 4)[72].

Più rilevante, per l'ambito medico-sanitario, è però il delitto punito dal comma 3, che con una formulazione estremamente sintetica, stabilisce semplicemente che «*Se taluno dei fatti previsti dal primo comma è commesso per colpa grave*», si ha una riduzione di pena, «*da un terzo a un sesto*» (dunque la reclusione da quattro mesi a quattro anni e due mesi per l'ipotesi base, da un anno e quattro mesi a sei anni e otto mesi per la circostanza aggravante speciale).

Si tratta anche in questa ipotesi di una fattispecie autonoma di reato, per la diversità dell'elemento soggettivo non doloso, che tocca la struttura stessa del fatto tipico, per cui sarebbe incongruo considerarla quale mera circostanza attenuante, seppur speciale, che sarebbe illogicamente bilanciabile con eventuali circostanze aggravanti.

Il principale problema interpretativo che pone la norma nasce dal fatto che, allo stato, non sono chiaramente individuabili né i precetti la cui violazione integra l'omissione costitutiva della condotta, né tantomeno le regole cautelari, cui devono attenersi le attività, di per sé lecite, ed anzi incentivate dallo stesso legislatore, di progettazione, addestramento, produzione, immissione sul mercato ed anche di "gestione" da parte del *deployer* di sistemi IA "*ad alto rischio*" per i quali occorre adottare le menzionate misure di "*sorveglianza umana*". Ed in mancanza di previe, riconoscibili regole cautelari, scritte o meno, è impossibile stabilire quando vi sia colpa per la loro violazione ('specifica' nel primo caso come appare più consono in questo ambito, come sopra si è argomentato, al par. 4.2., od anche solo 'generica' nel secondo caso).

A fortiori, in assenza di tali regole, non si veda come possa stabilirsi quando sia "*grave*", secondo la graduazione voluta dal legislatore, in conformità ad una tendenza di politica criminale diretta ad escluder la colpa lieve dal perimetro della responsabilità penale nel campo delle attività lecite di base.

---

[71] Questo autonomo ulteriore delitto doloso e di pericolo concreto per i menzionati beni giuridici ha natura commissiva, e forse per tale ragione è punito con una pena più grave (reclusione da due a sei anni nell'ipotesi base, da tre a dieci anni se ricorra la circostanza aggravante speciale del pericolo per la sicurezza dello Stato), rispetto all'ipotesi omissiva di cui al primo comma. Nella norma di delegazione non vi era però alcun espresso riferimento ad una qualsivoglia condotta commissiva, per cui si rafforzano i dubbi di legittimità costituzionale sull'incriminazione prevista soltanto dalla norma delegata, anche se la nozione di "*alterazione*" del sistema potrebbe abbracciare, nel suo più ampio significato, l'effetto di possibili strumentali omissioni, che tuttavia non devono ricadere, per espressa clausola di esclusione, nei «*casi indicati nel primo comma*» (in argomento rinvio ancora a L. PICOTTI, *Le disposizioni penali introdotte dal decreto legislativo*, cit., par. 3).

[72] Come ho già sottolineato, si tratta di un'ipotesi speciale rispetto a quella di omessa adozione di "*misure di sorveglianza umana*", peraltro punita con le stesse pene di cui al primo comma, compreso l'aggravamento per la circostanza ad effetto speciale di cui si è detto (cfr. L. PICOTTI, *Le disposizioni penali introdotte dal decreto legislativo*, cit., par. 4). Non viene però punita anche l'omessa adozione di "*misure tecniche di sicurezza*", evidentemente non ritenute di competenza dell'utilizzatore finale, di cui viene delimitata la punibilità anche attraverso il requisito del dolo intenzionale, che esclude l'applicazione del reato nei casi di mero dolo eventuale (che per il suo labile confine con la colpa cosciente, potrebbe eccezionalmente rilevare per la responsabilità penale del personale sanitario), oltre che, ad essere rigorosi, anche del dolo diretto.

Tutti questi delitti vengono nel contempo aggiunti, dall'art. 15 d.lgs. n. 160 del 2026, all'elenco dei reati presupposto della responsabilità degli enti, tramite l'inserimento di un nuovo art. 25-*vicies* nel d.lgs. n. 231 del 2001, rubricato "*Reati commessi con l'uso di sistemi di intelligenza artificiale*", in cui è incluso – accanto al menzionato nuovo art. 437-*bis* c.p.[73] – anche il delitto di "*Illecita diffusione di contenuti generati o manipolati artificialmente*" (art. 612-*quater* c.p.), già inserito nel codice penale dalla stessa l. n. 132 del 2025.

Tuttavia, la prospettiva della novella non è quella specifica del campo sanitario, in cui appaiono di marginale rilievo le fattispecie dolose.

Come deve escludersi uno specifico rilievo anche della circostanza aggravante comune di cui all'art. 61, n. 11-*undecies* c.p. (introdotta dell'art. 26, comma 1, lettera a) l. n. 132 del 2025), poco applicabile ai casi di colpa medica, essendo stata formulata anch'essa nella prospettiva di comportamenti dolosi, richiedendo che il fatto sia stato commesso «*mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o le modalità di utilizzo,* abbiano costituito mezzo insidioso*, ovvero quando il loro impiego abbia comunque* ostacolato la pubblica o privata difesa*, ovvero* aggravato le conseguenze *del reato*» (evidenz. aggiunte): "*aggravamento*" quest'ultimo difficile da dimostrare nel campo in esame e, comunque, di difficile riconduzione alla natura sostanzialmente colposa che deve avere la sua imputazione (*ex* art. 59, comma 2 c.p.), specie considerando la problematica interazione di detti sistemi con gli operatori sanitari.

Allo stato, fermi i dubbi di legittimità costituzionale per violazione del principio di stretta legalità e, comunque, per la carente tassatività delle fattispecie esaminate[74], restano immutate le questioni che sollevano in campo sanitario i delitti colposi di *evento* di cui agli artt. 589 e 590 c.p., allorché entri in gioco l'impiego sempre più frequente di sistemi IA, per cui si richiederebbe quantomeno una delimitazione o riconfigurazione della speciale causa non punibilità stabilita per l'imperizia dall'art. 589-*sexies* c.p.[75].

Si aggiunga che neppure con riferimento alla responsabilità degli enti il legislatore delegato ha "*precisato*" quanto prevedeva, come oggetto di delega, l'art. 24, lettera c), comma 5, l. n. 132 del 2025: vale a dire «*i criteri di imputazione della responsabilità penale delle persone fisiche* e amministrativa degli enti *per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente*» (evidenz. aggiunte).

Per cui spetta all'interprete ricostruire la trama dei predetti obblighi e delle predette regole cautelari, a partire dalla vincolante, ma insufficiente disciplina ai fini penali, che l'*AI Act* detta per i sistemi IA "*ad altro rischio*", per di più non ancora

---

[73] Per vero il legislatore delegato ha richiamato l'art. 437-*bis* c.p. come se si trattasse di un unico "*delitto*" – mentre la norma, come si è detto, ne prevede quattro – né ha distinto fra le fattispecie dolose e quella colposa, nel graduare le sanzioni applicabili all'ente.

[74] Oltre alle valutazioni critiche sopra espresse nel testo, per ulteriori relative anche alle deleghe legislative contenute nella l. n. 132 del 2025, sia consentito rinviare a L. PICOTTI, *I contenuti penali della legge sull'intelligenza artificiale*, in G. CASSANO, E.M. TRIPODI (a cura di), *Intelligenza artificiale. La disciplina italiana. Legge 23 settembre 2025 n. 132*, Pisa, 2026, 343 ss.; nonché già in *questa Rivista*, 2 dicembre 2025.

[75] Cfr. già A. FIORELLA, *Responsabilità penale dei Tutor*, cit., 657; e *supra* nota 62.

formalmente applicabile, in quanto il termine già previsto del 2 agosto 2026 è stato rinviato al 2 dicembre 2027 dall'*Omnibus* digitale IA (sopra citato a nota 2).

Un auspicabile intervento ulteriore, che più compiutamente delineasse i confini della colpa medica penalmente rilevante nel caso di impiego di sistemi IA potrebbe e dovrebbe auspicabilmente provenire allora, a livello nazionale, dalle nuove disposizioni da emanare in attuazione di un'altra importante e più ampia delega legislativa, contenuta nel disegno di legge oggetto da tempo di lunghi lavori parlamentari «*in materia di professioni sanitarie e disposizioni relative alla responsabilità professionale degli esercenti le professioni sanitarie*»[76]. Nel testo finora disponibile non figura però alcuna disposizione specifica al riguardo, che andrebbe invece introdotta e coordinata con i parametri della responsabilità penale nella gestione e nell'impiego dei sistemi IA "*ad alto rischio*", di cui si è trattato, come sono quelli che riguardano l'ambito sanitario, per garantire, da un lato, la piena tutela anche penale dei fondamentali beni giuridici e diritti in gioco in tale campo e, dall'altro, un chiaro perimetro di tale più grave forma di responsabilità, che può incombere sugli operatori sanitari, peraltro irrinunciabile a fronte del loro rango.

5. Spunti conclusivi.

L'importanza della sanzione penale, e di quella punitiva di natura formalmente amministrativa per la responsabilità 'da reato' dell'ente, la cui irrogazione può anche prescindere dalla concreta individuazione della singola persona fisica che nel suo ambito lo abbia realizzato (*ex* art. 8 d.lgs. n. 231 del 2001) e potrebbe per questo essere utilmente applicata con riferimento ai reati nella cui commissione sia coinvolto l'impiego di sistemi IA[77], ha un'essenziale funzione non solo di tutela dei beni giuridici e dei diritti

[76] Si veda il d.d.l. presentato dal Governo alla Camera dei Deputati il 13 novembre 2025 (AC 2700), recante "*Delega al Governo in materia di professioni sanitarie e disposizioni relative alla responsabilità professionale degli esercenti le professioni sanitarie*", all'esame della Commissione, il cui art. 7, collocato nel Capo II intitolato "*Disposizioni in materia di responsabilità professionale degli esercenti le professioni sanitarie*", prevede una riforma del menzionato art. 590-*sexies* c.p., qual era stato formulato dalla legge n. 24 del 2017 (c.d. Gelli-Bianco), che contiene l'esonero di responsabilità, per i reati di omicidio colposo e di lesioni personali colpose commessi nell'esercizio di attività sanitarie, per ogni forma di colpa, dunque anche per negligenza od imprudenza, non solo per imperizia, purché *non grave* e sempre che vi sia stato il rispetto delle linee guida o delle buone pratiche clinico-sanitarie. Viene inoltre circoscritta la discrezionalità giudiziale nella valutazione di inesigibilità del comportamento astrattamente doveroso, con l'inserimento di un nuovo art. 590-*septies*, rubricato: "*Colpa nell'attività sanitaria*", che precisa i parametri che il giudice deve applicare nell'accertamento anche del suo grado, recependo molti criteri di quelli che erano stati introdotti per l'applicazione della speciale clausola di non punibilità dei sanitari durante l'emergenza pandemica da Covid 19, quali la scarsità delle risorse umane e materiali disponibili, le eventuali carenze organizzative, la complessità della patologia del paziente, la mancanza, limitatezza o contraddittorietà delle conoscenze scientifiche sulla patologia o sulla terapia, la presenza di situazioni di urgenza o emergenza, ecc. Per un primo commento si veda C. CUPELLI, *La proposta di modifica dell'art. 590*-sexies *c.p. e il nuovo art. 590*-septies *c.p. nel disegno di legge di riforma della responsabilità penale degli operatori sanitari (AC 2700)*, in *Riv. it. med. leg.*, 4/2025, 1105 ss.

[77] Per alcuni spunti in argomento, rinvio a L. PICOTTI, *Responsabilità penale e sistemi di IA*, cit., in specie 107.

fondamentali che possono essere offesi, ma altresì di monito e di guida al comportamento corretto, conforme a diritto, degli esercenti le professioni sanitarie e degli operatori che intervengono in questo ampio settore, a partire dagli enti competenti per cui operano.

Anche per questo non pare rinunciabile la previsione della responsabilità penale nel campo medico-sanitario, così rilevante per la salvaguardia di tali essenziali interessi e diritti, non apparendo sufficiente, già *de jure condito*, quella che può essere offerta da altre tecniche di tutela, come quelle civile ed amministrativa, specie se si considerano anche i profili processuali dei mezzi di indagine ed acquisizione delle prove, di cui solo la giustizia penale dispone nel modo più incisivo ed efficace.

Appare, però, indispensabile un attento e calibrato adeguamento non solo ermeneutico, ma anche normativo, che coinvolga le categorie penalistiche d'imputazione della responsabilità, ed in specie della causalità e della colpa, sia personale che organizzativa, al fine di colmare le difficoltà e lacune riscontrate, seguendo le linee tracciate dalla disciplina europea sopra richiamata, senza lasciare alla sola giurisprudenza il pur indispensabile intervento applicativo ed interpretativo in materia.

Il ricorso allo strumento penale non deve essere un demagogico sostituto, facilmente introducibile con la moltiplicazione di norme incriminatrici e di circostanze aggravanti, ma piuttosto l'*ultima ratio* di un'efficace tutela, che deve trovare a monte solide basi in un'organica e razionale disciplina extrapenale del settore, alla cui concretizzazione partecipino necessariamente tecnici e giuristi.

E per questo obiettivo, la dottrina ed il confronto interdisciplinare possono e devono dare un importante contributo.

Editore

ASSOCIAZIONE
"PROGETTO GIUSTIZIA PENALE"