RESPONSABILITÀ SANITARIA
RISCHIO CLINICO E VALORE DELLA PERSONA

Fascicolo unico – Annuale (30.4.2025)
ISSN 29748844

Direttore scientifico
Giuseppe Cassano

Vicedirettori
Francesco Lauri
Caterina Brambilla
Sergio Di Nola

Comitato Scientifico
Fabio Addis
Maria A. Astone
Fabio Basile
Rocco Blaiotta
Mirzia Bianca
Alberto Cadoppi
Ilaria A. Caggiano
Michele Calaniello
Giovanni Canzio
Giovanna Capilli
Andrea Carinci
Paolo Cendon
Alberto Cisterna
Renato Clarizia
Giovanni Comandè
Claudio Consolo
Cristiano Cupelli
Enrico Del Prato
Astolfo Di Amato
Sergio Di Nola
Filippo Dinacci
Francesco Di Ciommo
Fabio Elefante
Guerino Fares
Francesco Fimmanò
Massimo Franzoni
Tommaso E. Frosini
Alberto M. Gambino
Lucilla Gatt
Arturo Iadecola
Francesco Introna
Bruno Inzitari
Luigi Kalb
Luca Lupària
Adelmo Manna
Antonella Marandola
Pier Giuseppe Monateri
Antonio Musio
Anna Carla Nazzaro
Mauro Orlandi
Angelo G. Orofino
Lorenzo Picotti
Nicola Pisani
Francesco Pizzetti
Carmine Punzi
Lucia Risicato
Marco Rossetti
Ugo Ruffolo
Piero Sandulli
Maurizio Santise
Livia Saporito
Giorgio Spangher
Pasquale Stanzione
Claudio Scognamiglio
Bruno Tassone
Raffaele Torino
Giacomo Travaglino
Livio Tronconi
Mario Trimarchi
Antonio F. Uricchio
Virginia Zambrano

Nel recente regolamento europeo sull'intelligenza artificiale (d'ora in poi: *AI-Act*)[2], il settore sanitario (o, più precisamente, dei "*servizi sanitari*" pubblici e privati) rientra in quelli "*ad alto rischio*", soggetti ad un'articolata disciplina di valutazione preventiva e, poi, contenimento e monitoraggio dei "*rischi*" che l'utilizzo dei sistemi IA comporta[3].

Pur potendo garantire, infatti, un miglioramento delle previsioni, un'ottimizzazione delle operazioni e dell'assegnazione delle risorse, la personalizzazione dei servizi, ed in particolare, sul piano terapeutico, maggior sicurezza e tempestività di diagnosi, da un lato, ed efficacia e precisione delle cure, dall'altro (si pensi 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 fa emergere, manifestatisi anche in eventi avversi[4]. Di qui le preoccupazioni etiche e giuridiche, riguardanti lo svolgersi dei rapporti con i pazienti e le responsabilità che possono insorgere, 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 diritto penale è però l'*ultima ratio* degli strumenti di tutela, che può intervenire solo quando altre tecniche alternative siano per loro natura inadeguate o, comunque, insufficienti a garantire il livello di protezione necessaria. Ed in ogni caso, la configurazione di una responsabilità penale richiede il rispetto di superiori principi garantistici, imposti dalla Costituzione e dalle Carte internazionali, quali quelli di legalità e di tassatività (artt. 25, comma 2, Cost., 7 CEDU, 49 CDFUE), nonché di personalità e di colpevolezza (art. 27, commi 1 e 3 Cost., e giurisprudenza della Corte di Strasburgo sull'art. 7 CEDU, relativa all'esigenza di "*prevedibilità*" della sanzione penale per l'autore del comportamento punibile).

Il principio euristico, che deve orientare le scelte di criminalizzazione in questi nuovi ambiti da parte del legislatore, si dovrebbe basare su un criterio di analogia (non invocabile nell'esercizio del magistero punitivo, vincolato invece al principio di stretta legalità), in forza del quale quanto sarebbe penalmente rilevante, se il fatto fosse commesso da una persona umana, non può essere penalmente irrilevante sol perché vi è l'intervento di un sistema IA. Tanto più che, di fronte ai nuovi sviluppi tecnologici ed all'estensione tumultuosa delle relative applicazioni, si estenderebbero inaccettabili aree di impunità[5].

Si tratta, quindi, di verificare se, ed in che misura, possa o debba configurarsi una responsabilità penale nel settore sanitario di fronte all'impiego di sistemi IA ed alla digitalizzazione che essa presuppone, guardando ad alcuni essenziali nuclei problematici in cui può rilevare: da quello del consenso informato al trattamento medico sanitario (par. 2), a quello della protezione dei dati personali (par. 3), dalla *cybersecurity* (par. 4) alla fede pubblica (par. 5), fino alla colpa medica (par. 6). Analisi da condurre non solo *de jure condito*, considerando possibili soluzioni ermeneutiche, ma anche guardando ad auspicabili interventi normativi (par. 7), che solo in parte trovano spazio nel controverso disegno di legge contenente "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*" recentemente approvato dal Senato della Repubblica ed ora all'esame della Camera dei Deputati[6].

---

généraux e loro collaboratori: PICOTTI, PANATTONI, *Traditional Criminal Law Categories and AI: Crisis or Palingenesis?* n. 1/2023; MIRÒ-LINARES, DUVAC, TOADER, GALARZA, *Criminalisation of AI-related Offences*, n. 1/2024; LELIEUR, BLOUNT, CHERQAOUI, BAMPASIKA, *Artificial Intelligence and Administration of Criminal Justice*, n. 2/2023; mentre è in corso di pubblicazione il quarto fascicolo a cura di STERIO, *International Perspectives on AI: Challenges for Judicial Cooperation and International Humanitarian/Criminal Law*.

[2] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (cd. *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 12.07.2024, serie L, It. Anche se entrato formalmente in vigore il 2.8.2024, molte norme si applicheranno in tempi successivi, come stabilisce l'art. 113, ed in particolare a partire dal 2.8.2026, per dare tempo ad autorità, aziende, cittadini di adeguarvisi, con l'eccezione di alcune importanti norme che si applicano già dal 2.2.2025 (par. 3, lett. a) e dal 2.8.2025 (par. 3, lett. b), mentre l'art. 6 par. 1 si applicherà solo dal 2.8.2027 (par. 3, lett. c). Nondimeno, ai fini delle valutazioni penalistiche sui vari punti qui trattati, con particolare riferimento ala disciplina dei sistemi "*ad alto rischio*", l'*AI Act* ha fin d'ora un importante valore giuridico e concettuale, cui fare riferimento.

[3] Si veda il Considerando (58) dedicato a quei "*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 dell'Allegato III. Per una più analitica esposizione delle regole stabilite per tali sistemi, a partire dalla necessaria valutazione preliminare dei rischi, e delle misure di necessario contenimento, ai sensi dell'art. 9, sia consentito rinviare a 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 www.sistemapenale.it (31.7.2024), in specie p. 9 s. e 12 s.

[4] Per un quadro in materia cfr. AMORE, ROSSERO, *Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità. Una ricerca sociologica e giuridico-penale*, collana Ldf - Torino, Il Mulino, Bologna, 2023.

[5] In tal senso si veda la risoluzione approvata all'esito dei lavori della Sezione I del XXI Congresso internazionale dell'*Association Internationale de Droit Pénal* (AIDP) di cui si è detto alla nota 1.

[6] A.S. n. 1146-A approvato il 20.3.2025, dopo significative modifiche, in sede referente, dell'originario d.d.l. presentato dal Consiglio dei Ministri il 23.4.2024. Per un primo commento di questo articolato cfr. CASSANO, *Note minime sul d.d.l. in materia di intelligenza artificiale*, in *Dir. Internet*, 2024, n. 3, p. 383 s.

2. Consenso informato: presupposto di liceità penale del trattamento medico chirurgico realizzato con l'impiego di sistemi di intelligenza artificiale?

2.1. Consenso al trattamento sanitario ed impiego di sistemi di intelligenza artificiale

Notoriamente il consenso libero ed informato è un presupposto generale di liceità dei trattamenti sanitari, 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 vincolante nell'ambito dell'Unione europea.

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

In dottrina[7] e giurisprudenza[8] 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.

Piuttosto è qui da chiedersi come si debba atteggiare la disciplina e la prassi del consenso informato, se intervengono sistemi IA in fase di diagnosi o di cura, o nell'uso di dispositivi a domicilio, che ricorrano a tali tecnologie, anche con connessioni a distanza. Infatti, rispetto all'obbligo di fornire un'informazione completa e chiara da parte del medico o della struttura, si frappongono (anche a prescindere dai limiti posti dal segreto industriale) gli ostacoli più specifici della c.d. opacità con cui i sistemi operano, per la cripticità del linguaggio, per i contenuti dei data base e dei possibili *bias* cognitivi, per gli effetti di imprevedibilità del *machine learning* o addirittura l'"imperscrutabilità' delle *black box*.

La soluzione non può essere l'affidamento cieco del paziente e, per certi aspetti, anche del medico e dell'operatore sanitario nell'operato dei sistemi IA, vale a dire alle "decisioni" o raccomandazioni da esso suggerite o direttamente attuate[9], che possono presentare profili di criticità, ed anche un *deficit* etico.

Nelle scelte del medico persona umana, infatti, si deve o si 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 il sistema AI sulla base di dati statistici e cognitivi generali, relativi alla patologia da trattare (si può fare l'esempio di un tumore maligno genitale di una giovane donna, in cui si debba optare fra un intervento demolitivo ed uno conservativo).

Certamente il paziente deve essere reso 'edotto' del ricorso ad un sistema IA nel trattamento cui viene sottoposto, come ha affermato condivisibilmente il Comitato nazionale di bioetica in una risoluzione su "*Intelligenza artificiale e medicina: aspetti etici*" [10], e come si desume anche dall'obbligo generale di trasparenza stabilito dall'*AI Act*, che all'art. 50, par. 1, fissa l'obbligo per i 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 indirettamente grava anche sull'ente sanitario che rende disponibili all'uso tali sistemi (*disployer*, secondo la terminologia dell'*AI Act*).

Ma il problema sorge nello stabilire fino a che punto l'informazione debba e possa essere dettagliata anche dal punto vista tecnico (sul contenuto e sull'operatività degli algoritmi, sulle tecniche di *machine learning*, sul novero dei rischi tecnici che possano prevedersi, ecc.), affinché il consenso stesso possa dirsi *cosciente* o consapevolmente prestato.

Già si è rilevato che l'informazione non può e non deve essere *eccessiva*, sia perché può essere opportuno tacere nei dettagli l'intero novero dei possibili, anche più improbabili rischi, per non instillare spropositate paure, sia perché potrebbe addirittura viziare il consenso, se andasse oltre la "*capacità di comprensione*" del destinatario, richiamata espressamente dall'art. 33 Codice di deontologia medica[11]:

---

[7] Cfr. nell'ampia bibliografia in argomento, 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, p. 137 s.; EUSEBI, *Il consenso informato e le disposizioni anticipate di trattamento*, in OLIVA, CAPUTO (a cura di), *Itinerari di medicina legale e delle responsabilità in campo sanitario*, Milano, 2021, p. 418 s.; già VALLINI, *Trattamento medico e consenso informato del paziente*, Roma 2012, cui si rinvia anche per gli ampi richiami bibliografici e giurisprudenziali.

[8] 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. 28.12.2008, dep. 21.1.2009, n. 2437, con nota di VIGANÒ, *Omessa acquisizione del consenso informato del paziente e responsabilità penale del chirurgo: l'approdo (provvisorio?) delle Sezioni Unite*, in *Cass. pen.*, 2009, p. 1811 s.

[9] 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 AI 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).

[10] https://bioetica.governo.it/it/documenti/pareri-gruppo-misto-cnbcnbbsv/intelligenza-artificiale-e-medicina-aspetti-etici/ del 29.5.2020.

[11] Secondo cui "*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*

capacità, si può aggiungere, da valutare anche dal punto di vista tecnico informatico, oltre che medico-terapeutico.
Ma un'informazione non solo sull'uso, ma anche sui rischi e sul possibile malfunzionamento del sistema IA dovrebbe essere data, pur se questi non fossero statisticamente elevati, però non imprevedibili.
Nelle regole cautelari stabilite dal regolamento europeo relative alla "*sorveglianza umana*" - obbligatoria per un sistema IA ad alto rischio, come è quello che coinvolge la salute e i diritti fondamentali della persona - è espressamente previsto che si debbano considerare i rischi sia quando il sistema è "*utilizzato conformemente alla sua finalità prevista*", sia quando possa essere "*in condizioni di uso improprio ragionevolmente prevedibile*" (così l'art. 14, par. 2, dell'*AI Act*).
E dunque di questi rischi deve essere informato anche il paziente, che deve poter aver conoscenza delle "*conseguenze delle scelte operate*"[12].
Di certo, nel rapporto medico-paziente non basta dar rilievo alla *voluntas* della 'parte debole', in qualsivoglia modo espressa o fondata, poiché il paziente non si trova in posizione di parità: per cui è necessario stabilire a livello pubblicistico limiti e garanzie per tutelarla (come avviene a tutela di lavoratori, consumatori, investitori, ecc.)[13].
Al riguardo è interessante menzionare anche l'art. 7 del citato d.d.l. 1146 – A (cfr. *supra* nota 6), dedicato all'"*Uso dell'intelligenza artificiale in ambito sanitario e di disabilità*".
Infatti, dopo aver dato atto, al primo comma, dell'utilità dei sistemi di intelligenza artificiale "*per il miglioramento del sistema sanitario e la prevenzione e cura delle malattie*", ribadendo che il loro utilizzo "*deve avvenire nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali*" (aspetto quest'ultimo regolato dal successivo art. 8, su cui si tornerà *infra*, par. 3.1), si stabilisce al terzo comma il "*diritto*" dell'interessato "*di essere informato sull'impiego di tecnologie di intelligenza artificiale*".
Appare senz'altro opportuno il riconoscimento di un tale diritto, anche se la norma non enuncia più il contenuto che deve avere tale informativa, come era nell'originaria formulazione[14], che ne delimitava l'oggetto alla "*logica decisionale*" utilizzata dal sistema, allineandosi alla posizione intermedia sull'inopportunità di un'informativa eccessivamente dettagliata dal punto di vista tecnico, ma garantendone l'essenziale contenuto sul ruolo concreto che il sistema di intelligenza artificiale può assumere. In effetti è essenziale, per la finalità stessa dell'informazione in materia, che è alla base dell'espressione del consenso consapevole al trattamento sanitario con l'impiego di sistemi IA, che l'interessato sia avvertito dei profili "decisionali" ad essi affidati, con i connessi vantaggi e rischi.
Infatti, l'espressa finalità perseguita dal legislatore con questo nuovo intervento normativo, di "*promuovere*" lo sviluppo, la ricerca e la diffusione di tali sistemi (comma 4), non può spingersi fino a violare o limitare eccessivamente il rispetto dei diritti e delle libertà della persona, quando vi sia un impiego dei sistemi in questione. Per cui si deve auspicare una più completa formulazione della disposizione in esame.

2.2. Sulla marginale rilevanza penale di un consenso non adeguatamente informato

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 evidenziato, tale vizio può di per sé non avere valenza *causale* rispetto all'evento costitutivo di un eventuale reato colposo in danno del paziente.
Rispetto ad un esito infausto o, comunque, avverso potrebbe delinearsi una responsabilità civile, ma non una responsabilità penale, come affermato ormai da numerose pronunce della Suprema Corte, a partire dalla citata sentenza delle Sezioni unite penali n. 2437/2009, con cui è stato escluso che si possa configurare il delitto di violenza privata (*ex* art. 610 c.p.) o, in caso di evento avverso, di lesioni personali dolose (*ex* art. 582 e 583 c.p.), o tantomeno di omicidio preterintenzionale (*ex* art. 584 c.p.), come in precedenza era stato ritenuto, se il trattamento medico chirurgico sia stato posto in essere in assenza di consenso o sulla base di un consenso invalido[15].
Il consenso che viene in rilievo in queste ipotesi, infatti, non ha funzione scriminante, *ex* art. 50 c.p., vale a dire di causa di giustificazione che escluda l'antigiuridicità di un fatto tipico di reato, altrimenti illecito, perché l'attività medica persegue una finalità o, meglio, una funzione terapeutica rispetto ad una patologia in atto, non integrando di per sé una condotta del sanitario penalmente tipica. La circostanza che essa incida, materialmente, sull'integrità fisica del paziente, non configura dunque il reato di lesioni dolose, anche se manchi o sia invalido il consenso ad essa. La responsabilità penale può, infatti, sorgere solo per una violazione della *lex artis*, che sia causale per la determinazione dell'evento. Oppure nel caso che dolosamente siano state omesse informazioni o date informazioni inveritiere per acquisirlo[16], od ancora, sul piano

---

conseguenze delle scelte operate. Il medico dovrà comunicare con il soggetto tenendo conto delle sue capacità di comprensione, allfine di promuoverne la massima partecipazione alle scelte decisionali e l'adesione alle proposte diagnostico terapeutiche. [omissis]". In argomento cfr. DE MENECH, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in FACCIOLI (a cura di), *Profili giuridici della robotica e dell'intelligenza artificiale in medicina*, Napoli, 2022, p. 9 s., in specie p. 23.

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

[13] Così sottolinea DE MENECH, *Intelligenza artificiale e autodeterminazione*, cit., p. 22, con essenziali richiami.

[14] L'originaria formulazione era più complessa, in quanto 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 espresso nel mio saggio del 2024 (citato nella nota in asterisco) alla formulazione originaria della norma, segnalavo la necessità che, oltre ai "*vantaggi*", si facesse espressa menzione anche dei "*rischi*" inerenti all'impiego di sistemi IA, necessità che ritengo di dover ribadire.

[15] Cfr. Cass. pen., Sez. V, ud. 24.11.2015, dep. 21.4.2016, n. 16678, conforme a quanto espresso nella sentenza Cass. sez. un. pen., ud. 28.12.2008, dep. 21.1.2009, n. 2437, sopra citata a nota 6.

[16] 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

della colpa, se la carenza di informazioni al paziente abbia impedito di acquisire dallo stesso dati ed informazioni rilevanti ai fini del trattamento[17].

In conclusione, una seppur carente informazione sul ricorso a sistemi IA nel trattamento medico chirurgico, fermi i limiti sopraddetti, non potrebbe di per sé dar luogo ad una responsabilità penale, salvo non consenta di acquisire informazioni rilevanti, anche per il sistema AI, sullo stato del paziente stesso.

3. Digitalizzazione dei dati sanitari ed impiego di sistemi IA a fronte del diritto alla protezione dei dati personali

Un vasto ambito di altre questioni di possibile rilievo penale suscita la digitalizzazione in atto dell'attività sanitaria, che rende possibile e si correla strettamente all'impiego, che si sta diffondendo, e certamente si diffonderà ulteriormente nei prossimi anni, di sistemi IA in tale settore.

Mi riferisco soprattutto all'introduzione ed all'utilizzo del "*Fascicolo sanitario elettronico*" (FSE) e della "*Cartella clinica elettronica*" (CCE), oltre che al ricorso alla telemedicina ed alla robotica, specie nella chirurgia di precisione e nei servizi assistenziali, da collocare nel quadro sovranazionale ormai delineato dal più recente regolamento dell'Unione europea per lo "spazio europeo dei dati sanitari" (*EHDS Act*)[18] emanato anche sulla base dell'esperienza pandemica da Covid 19[19], e recentemente entrato in vigore, oltre che da quello generale sull'intelligenza artificiale (*AI Act*).

Del resto, si tratta di obiettivi di necessaria modernizzazione della sanità, che rientrano già nell'area 6 del PNRR, per vero solo parzialmente raggiunti, e che coinvolgono i temi della *privacy*, da un lato, e della *cybersecurity*, dall'altro (cfr. *infra*, par. 4).

3.1. Sul trattamento dei dati sanitari quali "dati personali particolari"

Muovendo dalla tutela della *privacy*, basti dire che la digitalizzazione della sanità implica una nuova modalità di raccolta e trattamento dei "*dati particolari*" concernenti la salute, che ricadono nella previsione degli artt. 5 e 6, par. 1 del regolamento (UE) 2016/679 (c.d. GDPR), per cui è necessario il consenso al trattamento, che deve essere dato, previa adeguata informazione, per uno o più "*scopi specifici*", come si evince anche dall'art. 9, par. 2, lett. a) dello stesso regolamento, secondo cui quelli relativi alla salute rientrano nei "*dati appartenenti a categorie particolari*" (precedentemente qualificati nel nostro Codice *privacy* come "*dati sensibili*", sulla base delle distinzioni portate dalla oggi abrogata Direttiva CE 95/46).

La prima questione che si pone è se, oltre alla digitalizzazione, il ricorso a sistemi IA nel trattamento di questi "*dati particolari*" debba essere preciso oggetto dell'informativa sulla cui base viene richiesto il necessario consenso ed eseguito il successivo trattamento. La risposta ritengo debba 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 detto sopra (par. 2.1) a proposito del consenso al trattamento sanitario che implichi l'impiego di sistemi IA.

La seconda questione, più complessa e di carattere generale, è in che misura ed in che limiti la digitalizzazione su larga scala ed il ricorso a sistemi IA in questo settore si possano conformare al diritto al controllo del flusso dei propri dati ed al "principio di minimizzazione", quest'ultimo espressamente ribadito anche dall'art. 66 dell'*EHDS – Act*, rappresentando un fattore potenzialmente, se non strutturalmente 'antagonista' rispetto ad essi.

In effetti, le nuove tecnologie aumentano in termini esponenziali le occasioni di offesa o quantomeno compressione della *privacy*, data la raccolta massiva e sistematica di darti che la digitalizzazione consente e nel contempo richiede, specie quando nel trattamento intervengano sistemi di IA, in quanto è necessaria la più gran quantità possibile di dati per garantire precisione e accuratezza nella diagnosi e nel trattamento sanitario, oltre che per la miglior organizzazione e gestione dei servizi ed allocazione delle relative risorse umane e finanziarie.

La questione non è, dunque, come impedire od ostacolare la raccolta e l'utilizzo di tali dati, che è anche a favore degli interessati oltre che della collettività, ma piuttosto di stabilire e far rispettare rigorosamente i limiti e le condizioni che devono osservarsi, perché il loro trattamento, in tutte le sue diverse fasi, sia lecito, applicando la disciplina delineata dal GDPR ed, oggi, adattata dalle norme dell'*AI Act* in materia di raccolta e trattamento dei dati necessari all'addestramento ed al funzionamento corretto dei sistemi e modelli IA "*ad alto rischio*", oltre che dalle specifiche nuove disposizioni

---

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.

[17] Così Cass. Sez. IV, 22.5.2015, n. 21537.

[18] Il regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11.2.2025, "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 5.3.2025, serie L, it. Pur essendo entrato formalmente in vigore il 26.3.2025, ai sensi del suo art. 105 si applicherà soltanto a decorrere dal 26.3.2027, salvi ulteriori termini successivi previsti per determinate norme.

Senza poter qui entrare nel dettaglio di questa nuova complessa disciplina, basti richiamare il comunicato dell'ufficio stampa del Parlamento europeo, diffuso dopo l'avvenuta approvazione parlamentare del 24.4.2024, secondo cui l'atto europeo, che interviene sull'assistenza sanitaria, sulla ricerca e sulla definizione delle politiche in materia, consentirà agli operatori sanitari 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, per cui 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 i trattamenti e la ricerca. Di qui i vantaggi anche per i cittadini, cui le norme in materia di privacy e sicurezza dovranno garantire che nessuna informazione personale sia condivisa 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.

[19] La rilevanza delle *app* e dei sistemi di rilevazione dei contagi durante l'emergenza pandemica, per il c.d. *contact tracing*, viene espressamente richiamata nei Considerando (2) e (3) del citato *EHDS Act*.

dell'*EHDS Act*, che riguardano altresì la condivisone ed il trasferimento di tali dati anche transfrontaliero.

Come anticipato, la materia dell'"*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 oggetto dei sistemi IA classificati "*ad alto rischio*", ai sensi del suo art. 6, par. 2, in quanto inclusa nell'elenco di cui all'Allegato III dell'*AI Act*, lettera a) del paragrafo 5, dato che essi possono avere un impatto negativo sulla salute, sulla sicurezza e sui diritti fondamentali [20].

Alla stregua di questa disciplina, per il *training* di tali sistemi si deve ricorrere, di regola, ai c.d. dati sintetici od a "*dati derivati*", che tramite l'anonimizzazione e/o la pseudonimizzazione consentano di non individuare (se non in ipotesi tassative) l'identità personale dei singoli interessati, cui i dati in questione si riferiscono, pur acquisendo tutte le informazioni utili per l'elaborazione statistica, diagnostica, scientifica, ecc.

Ma vi possono essere situazioni in cui, se "*strettamente necessario*" per rilevare e correggere eventuali "*distorsioni*", i fornitori di sistemi IA sono autorizzati a trattare anche i "*dati particolari*" di cui si è detto, con i limiti e le condizioni stabilite in particolare dall'art. 10, par. 5, *AI Act*, rubricato "*Dati e governance dei dati*", che non collimano del tutto, nonostante le rassicuranti affermazioni normative, con quanto già stabilito dal GDPR[21].

Il primo problema è rappresentato dal diritto alla "*revoca*" del consenso, riconosciuto dall'art. 7, par. 3 GDPR, che può rappresentare un ostacolo a tali trattamenti e scambi di dati, salvo ritenere, al contrario, che divenga addirittura impossibile il suo esercizio, negandolo di fatto inaccettabilmente.

Il problema è superabile muovendo dal rilievo che il trattamento dei dati sanitari può trovare una base giuridica anche diversa dal consenso dell'interessato, già alla stregua delle previsioni contenute nell'art. 9, par. 2, lett. i) e j) GDPR, che menzionano le finalità di "*ricerca scientifica*" ed i "*fini statistici*".

Rileva in questa prospettiva il citato *EHDS - Act*, che regola, fra l'altro, specificamente le condizioni di accesso, trasmissione, portabilità dei dati sanitari elettronici nel territorio dell'Unione, riconoscendo l'interesse pubblico in tale settore, in particolare per il c.d. "*uso secondario*" di cui al capo IV (artt. 50 ss. *EHDS – Act*), rispetto al quale è garantito all'interessato un - reversibile - "*diritto di esclusione*" (art. 71 *EHDS – Act*).

Quanto all'ordinamento interno, occorre menzionare innanzitutto l'art. 2-*sexies* del Codice *privacy*, rubricato: "*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevanti*", che richiama, ma in realtà va potenzialmente oltre il disposto dell'art. 9, par. 1, GDPR, in quanto elenca una serie di fonti europee ed interne, di rango non soltanto legislativo, da cui 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: vale a dire "*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*".

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*" nelle materie specificamente indicate, 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*".

Più in specifico rilevano, per le finalità di ricerca, gli artt. 110 e 110-*bis* Codice *privacy*, che riguardano 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*".

In forza della prima norma "*il consenso dell'interessato non è necessario 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), del Regolamento*" oltre che "*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*".

Mentre in forza della seconda norma[22] spetta al Garante "*autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali 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*" (*omissis*).

Al di là dei rilievi critici, su cui si tornerà (*infra* par. 3.3), circa la possibilità che fonti di rango secondario possano restringere l'esercizio di un diritto fondamentale qual è quello in esame, ai fini dell'eventuale responsabilità penale per la violazione di

---

[20] Essi sono elencati nel Considerando (48). Ma tale locuzione di sintesi ricorre in molte altre parti dell'*AI Act*, sia nei suoi Considerando, sia nell'articolato.

[21] Al riguardo occorre muovere dalla disciplina generale sulla c.d. *governance* dei dati, di cui al regolamento (UE) 2022/868 (Data Governance Act: *DGA*), che si applica dal 24.9.2023, e 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.).

[22] Articolo già aggiunto dall'art. 28, comma 1, lettera b) della legge 20 novembre 2017, n. 167, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017" e poi novellato, mentre l'art. 44 del recentissimo d.l. 2.3.2024 n. 19, convertito dalla legge 29.4.2024, n. 56, ha modificato anche il primo comma dell'art. 110 citato, attribuendo al Garante il compito di individuare le garanzie da osservare, in sostituzione dell'obbligo di consultarlo.

una siffatta disciplina, che ha un carattere generale, restando da determinare i contenuti e precetti specifici, non sembra che possa assumere la funzione di integrare una fattispecie penale, quale quella di cui all'art. 167-*bis* dello stesso Codice *privacy*, di cui appresso si dirà (par. 3.3).

3.2. Considerazioni critiche sulle norme previste dal disegno di legge in materia di intelligenza artificiale riguardante i dati sanitari

Prima di esaminare tali aspetti, è però opportuno menzionare la regolamentazione dell'utilizzo di dati personali anche "*particolari*" da parte di sistemi IA nell'ambito sanitario, che viene prefigurata dal citato disegno di legge n. 1146-A in materia di intelligenza artificiale[23].

Infatti, al tema sono dedicate numerose disposizioni, contenute nei suoi artt. 7, 8, 8-*bis* e 9, oggetto di significative modifiche ed integrazioni durante i lavori parlamentari in sede referente, rispetto all'originario testo governativo.

Pur non essendo questa la sede per un'approfondita analisi, sarà sufficiente evidenziare alcuni spunti di interesse per le ricadute che possono avere sotto il profilo penale.

Premesso che l'utilizzo di sistemi di intelligenza artificiale è positivamente apprezzato, perché "*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" (art. 7 comma 1; evidenziazione aggiunta), il successivo art. 8, sotto la rubrica "*Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario*" prevede, al primo comma, che "*sono dichiarati di* rilevante interesse pubblico *in attuazione dell'articolo 32 e 33 della Costituzione e nel rispetto di quanto previsto nell'articolo 9 lettera g) del Regolamento UE 679/16*" [...] "*in quanto* necessari *ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base*" (...) tutti i "*trattamenti di dati,* anche personali, *eseguiti da soggetti pubblici e privati senza scopo di lucro*", ed altresì da altri istituti di ricovero e cura *"per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale"* che perseguano un ampio novero di *"finalità"* a partire da quelle di *"prevenzione, diagnosi e cura di malattie"* nonché *"sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali* (....), *di salute pubblica, incolumità della persona, salute e sicurezza sanitaria"*.

Sulla base di tale ampia premessa, nel secondo comma sono indicati i requisiti di legittimazione del trattamento di queste categorie di dati, superandosi con una certa disinvoltura il requisito del "*consenso dell'interessato*", anche "*ove inizialmente previsto dalla legge*", stabilendosi – peraltro senza indicare stringenti condizioni - che, da un lato, "*l'obbligo di informativa dell'interessato*" che è pur sempre da garantire "*può essere assolto anche mediante messa a disposizione di un'*informativa generale sul sito web *del titolare*"; e che, dall'altro, per i trattamenti che perseguano le finalità sopraddette è "sempre autorizzato l'uso secondario *di dati personali privi degli elementi identificativi* diretti, *anche appartenenti alle categorie indicate all'articolo 9 del regolamento UE n. 679/2016*", con l'eccezione però dei casi in cui la relativa "*conoscenza sia inevitabile o necessaria ai fini della tutela della* (...) *salute*" degli interessati [evidenziazioni aggiunte].

Siffatta disciplina, prefigurata dal d.d.l. n. 1146-A, non sembra collimare con quella contenuta nella nuova vincolante fonte sovranazionale, che dedica l'intero capo IV (artt. 50 ss. *EHDS Act*), dopo l'ampia definizione dell'"*uso secondario*" dei dati sanitari, alla sua dettagliata disciplina, stabilendone, fra l'altro, finalità (art. 53) e divieti (art. 54), prevedendo appositi organismi di *governance* (art. 55) e condizioni dei servizi di accesso (art. 56), il menzionato diritto "*di esclusione*" esercitabile dagli interessati (art. 71), le condizioni di sicurezza (art. 73), la loro "*qualità*" e catalogazione (art. 77).

La norma del d.d.l. n. 1146-A si limita invece a stabilire, a presidio di un uso corretto di tali dati, soltanto una formale "*approvazione*" dei trattamenti "*da parte dei comitati etici interessati*" e la loro "*comunicazione*" all'Autorità garante per la protezione dei dati personali, che potrebbe disporne il blocco entro trenta giorni, valendo altrimenti il silenzio-assenso.

Una tale sincopata disciplina appare assolutamente censurabile, per la genericità dei presupposti di legge che consentono il superamento del diritto fondamentale al consenso informato in questo settore particolare di dati personali, che toccano l'essenza psico-fisica della persona e la sua stessa storia, cui non può certo sopperire l'*iter* burocratico 'diffuso', ma inadeguato, che verrebbe introdotto, vista la possibilità di esiti difformi da comitato etico a comitato etico e la mancanza di specifiche competenze in materia.

Nel contempo, appare insufficiente, oltre che difficile da realizzare in concreto, l'intervento del Garante della *privacy*, certamente ben più competente, che – scalzato dal ruolo assegnatogli dal Codice *privacy* in forza delle norme richiamate sopra (par. 3.1.) - potrebbe solo residualmente 'bloccare', nel termine molto stretto di trenta giorni, i trattamenti già approvati dai comitati etici, senza alcuna previsione della possibilità di dare prescrizioni od anche previe indicazioni per il superamento *ab origine* delle criticità riscontrabili.

In sede referente è stato invero inserito un nuovo art. 8-*bis*, contenente "*disposizioni in materia di trattamento dei dati personali*" ed in specie di quelli "*particolari*" di cui all'art. 9 GDPR, che vengono qui in rilievo per finalità di ricerca e sperimentazione, cui si aggiunge espressamente anche quella "*tramite sistemi di intelligenza artificiale e* machine learning": ma si tratta di una previsione generica, essendo interamente demandata ad un "*decreto del Ministro della salute*" (da emanare entro 120 giorni dall'entrata in vigore della legge, sentito il Garante della *privacy* ed altri enti e soggetti interessati) la disciplina concreta, senza che ne siano indicate a livello legislativo le linee direttive e le condizioni da rispettare.

Trattandosi di materia soggetta a riserva di legge, perché sono in gioco diritti fondamentali della persona, è auspicabile che, nell'ulteriore corso dei lavori parlamentari, la disciplina delineata da queste norme venga ulteriormente riveduta, e

---

[23] Cfr. *supra*, par. 2.1.

divenga oggetto anch'essa di delega legislativa, non solo per l'esigenza che intervenga in materia una fonte primaria, ma altresì perché siano stabiliti principi direttivi conformi alle previsioni del menzionato *EHDS Act*, cui l'ordinamento interno deve adeguarsi, essendo già in vigore.

In particolare occorre una ben più chiara definizione dei presupposti che legittimano le modalità e condizioni dei trattamenti di dati in esame, soprattutto laddove prescindono dal consenso dell'interessato, mentre deve riconoscersi un ruolo più incisivo alla funzione ed all'azione del Garante, in quanto autorità politicamente indipendente, deputata proprio a salvaguardare i diritti e le libertà fondamentali che vengono in rilievo in tutti gli ambiti di trattamento dei dati personali, ed in specie in quello sanitario, in cui sono trattati dati "*particolari*".

Il menzionato disegno di legge n. 1446-A interviene, infine, anche sul trattamento dei dati acquisibili nel "*Fascicolo sanitario elettronico*", già oggetto del comma 1-*bis* dell'art. 2-*sexies* del Codice *privacy*, introdotto dall'art. 9 del d.l. 8.10.2021, n. 139, convertito dalla legge 3.12.2021, n. 205.

Alla stregua di tale norma "*I dati personali relativi alla salute, privi di elementi identificativi* diretti, *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 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*" [evidenziazioni aggiunte].

Da siffatta norma emerge una gran quantità di enti legittimati a trattare "*dati personali relativi alla salute*", rispetto ai quali è garantita solo l'assenza di dati identificativi "*diretti*", mentre le regole del trattamento sono stabilite ancora una volta 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 appare violata sia la garanzia del suo "controllo", sia quella della riserva di legge, che dovrebbe valere non solo ai fini penali, dato che tali regole costituiscono tecnicamente un'integrazione normativa del precetto di cui all'art. 167-*bis* Codice privacy (cfr. *infra* par. 3.2.), ma anche in materia di tutela dei diritti fondamentali della persona[24], tanto più esposti a rischio quando intervengano, nel trattamento, sistemi di intelligenza artificiale, che in quest'ambito, come detto, sono classificati dall'*AI Act* "*ad alto rischio*".

Viceversa, il citato disegno di legge n. 1146-A dedica il suo art. 9 ad una riforma della normativa in materia di "*Fascicolo sanitario elettronico*", prevedendo l'introduzione dell'art. 12-*bis* (rubricato: "*Intelligenza artificiale nel settore sanitario*") nel decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre, 2012, n. 221, in forza del quale viene istituita una "*piattaforma di intelligenza artificiale*" per il supporto alle finalità di cura e per l'assistenza territoriale (comma 2), le cui "*soluzioni di intelligenza artificiale*" sono disciplinate da appositi *decreti* emanati ai sensi del comma 1, coinvolgendo sia l'Autorità "politica" per l'innovazione tecnologica e la transizione digitale, sia quella (altrettanto "politica") per la sicurezza della Repubblica e la cybersicurezza: non però l'Autorità Garante per la protezione dei dati personali, che viceversa sarebbe non solo quella più specificamente competente in materia di trattamento di dati personali, ma anche quella indipendente (e non politica) deputata alla tutela dei diritti fondamentali delle persone, come impone l'art. 8 CDFUE, di particolare rilievo trattandosi di "*dati particolari*", come quelli sanitari.

Anche sotto questo aspetto, appare dunque necessaria una revisione delle scelte di politica legislativa in materia, ed un'attenta riformulazione delle disposizioni in questione, che devono allinearsi alle vincolanti Carte sovranazionali dei diritti ed in ogni caso alla disciplina delineata dall'*EHDS Act*.

Il necessario e ragionevole bilanciamento fra interessi ed esigenze potenzialmente confliggenti, che coinvolge i diritti fondamentali, deve essere definito con chiarezza dal legislatore nazionale, in sintonia con quello europeo, preservando l'esercizio dei diritti all'autodeterminazione informativa oltre che all'autodeterminazione nei trattamenti sanitari. Se, da un lato, va certamente superata l'ottocentesca ed individualistica nozione del diritto "a restare soli", per cui i sistemi IA devono essere posti in grado di sfruttare l'enorme capacità di trattamento e velocità di connessioni offerte da tutta la rete, per potenziare nella misura massima possibile l'attendibilità delle valutazioni e previsioni probabilistiche, su cui si fondano le diagnosi e le analisi dei fattori o delle situazioni di rischio, dall'altro devono essere altresì salvaguardati i diritti fondamentali della persona di cui si è detto. Ed a tal fine può essere di concreto supporto il principio di *trasparenza* dei trattamenti di dati personali, enunciato dall'art. 5 par. 1, lett. a), GDPR, che dovrebbe contrastare la rilevata 'opacità' dell'IA, assicurandone l'esplicabilità, alla stregua degli specifici obblighi che gravano sui fornitori di sistemi IA "*ad alto rischio*" cui spetta garantire che il loro funzionamento sia "*sufficientemente trasparente da consentire ai deployer di interpretare l'output*" del sistema e "*utilizzarlo adeguatamente*" (art. 13 *AI Act*). Trasparenza che dovrebbe logicamente rispecchiarsi, a valle, anche nel

---

[24] 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*" [evidenziazioni aggiunte].

rapporto con gli interessati e gli utenti tutti, vale a dire con i pazienti e con lo stesso personale sanitario[25].

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

Venendo ora ad un rapido esame dei profili penali connessi alla violazione della disciplina dei dati personali di natura sanitaria, vengono in rilievo gli artt. 167 e 167-*bis* del nostro Codice *privacy*, nella formulazione portata dal d.lgs. 10.8.2018, n. 101 (di adeguamento del d.lgs. 30.6.2003, n. 196, 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 degli specifici precetti extra-penali fissati dal GDPR e dal Codice *privacy*, cui il legislatore rinvia, per definire le condotte illecite che li violano, richiedendo però due requisiti ulteriori, che restringono la punibilità.

Il primo 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[26].

Il secondo requisito selettivo è rappresentato dall'evento consumativo, costituito dall'invece oggettivo "*nocumento*" che deve essere dolosamente causato dal reo con la propria condotta, vale a dire con la volontà consapevole di produrlo.

Tali due elementi sembrano sufficienti a distinguere gli illeciti penali in esame dagli illeciti di natura amministrativa, che sono previsti dai regolamenti europei con sanzioni pecuniarie severe - ai sensi dell'art. 83 GDPR, degli artt. 99-101 *AI Act* e dell'art. 99 *EHSD Act*, che richiama anche quelle di cui agli artt. 63 e 64 del medesimo regolamento - senza che possa essere violato il divieto di *bis in idem* (così anche il Considerando (168) dell'*AI Act*), di per sé applicabile anche al concorso fra sanzioni penali e sanzioni amministrative che abbiano carattere punitivo[27].

In primo luogo viene dunque in rilievo il delitto di cui al comma 2 dell'art. 167, che ("*salvo che il fatto costituisca più grave reato*") punisce con la reclusione da uno a tre anni, chiunque, al fine specifico sopraddetto, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del GDPR, "*in violazione (...) delle misure di garanzia di cui all'articolo* 2-septies" del Codice *privacy* - che riguardano il trattamento dei dati genetici, biometrici, relativi alla salute – "*arreca nocumento*" all'interessato. Mentre il comma 3 stabilisce che la stessa pena si applica altresì a chi, al medesimo fine ed arrecando nocumento, procede "*al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti*".

Senza poter approfondire in questa sede l'analisi ermeneutica di queste due fattispecie, basti segnalare che il menzionato *EHDS Act* costituisce oggi una fonte che legittima, ed anzi persegue l'uso transfrontaliero, sia primario (art. 23 ss.), sia secondario (art. 75 ss.), di tali dati in altri paesi dell'Unione, nonché il loro trasferimento anche verso paesi terzi (art. 88), purché alle condizioni stabilite da dette norme europee. Di conseguenza, la violazione di queste ultime potrebbe integrare il delitto in esame, perché il trasferimento avverrebbe "*fuori dei casi consentiti*".

L'ulteriore delitto che viene in rilievo è quello previsto dall'art. 167-*bis* Codice *privacy*, inseritovi dal d.lgs. 101/2018, che considera specificamente la nuova dimensione globale del *web* e la tematica dei *big data*. Infatti la norma punisce più gravemente, con la reclusione da uno a sei anni (salvo sempre che il fatto costituisca più grave reato), chi, al fine specifico di cui si è già detto, "*comunica o diffonde un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento* su larga scala, *in violazione degli articoli* 2-ter, 2-sexies e 2-octies" [evidenz. aggiunta]; nonché chi, ai sensi del comma 2, "*comunica o diffonde, senza consenso*" un tale archivio automatizzato o una sua parte sostanziale, "*quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione*".

Bisogna, dunque, risalire alla disciplina dell'art. 2-*sexies* Codice *privacy* [28], di cui sopra si è detto (par. 3.1), per individuare le violazioni che – in presenza degli altri requisiti specifici - possono integrare la fattispecie penale.

Ma come si è già evidenziato, la norma extrapenale richiamata non individua dei contenuti specifici delle eventuali condotte

---

[25] Il necessario raccordo sistematico fra la disciplina dell'allora emanando *EDHS Act* ed il regolamento generale sull'intelligenza artificiale 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*", si indica specificamente ad "*esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari*" che "*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*".

[26] Sulla struttura e sulle caratteristiche delle fattispecie c.d. a dolo specifico, che in realtà non si caratterizzano per una particolare forma di dolo, bensì per il nesso teleologico con cui viene più precisamente tipizzato il fatto costitutivo del reato, sia consentito rinviare a PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993.

[27] Sulla faticosa elaborazione delle Corti europee relative alla portata di tale principio, che costituisce un diritto fondamentale valevole anche in ambito comunitario, sia consentito rinviare, per brevità, a PICOTTI, *Doppio binario sanzionatorio* e ne bis in idem*: verso un accettabile epilogo del lungo dialogo fra le Corti?*, in CADOPPI, 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 SCOLETTA, *Il principio del ne bis in idem e i modelli punitivi "a doppio binario"*, in AMALFITANO, D'AMICO, LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione Europa nel sistema integrato di tutela*, Torino, 2022, p. 315 s; e più di recente, prendendo spunto da C. Cost., 10 maggio 2022, n. 149, 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. penale* (15 aprile 2023).

[28] Non interessando in questa sede quello degli 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", e 2-*octies*, che contiene i "Principi relativi al trattamento di dati relativi a condanne penali e reati".

da sanzionare, perché rimanda ad una molteplicità di fonti, fra cui anche regolamenti ed atti amministrativi di rango inferiore alla legge, dei quali non sono esplicitati con precisione gli ambiti di intervento né i criteri direttivi cui debbano conformarsi. Si prospetta dunque una violazione del principio di legalità in materia penale, oltre che in materia di tutela dei dati personali[29], dandosi adito a possibili censure di incostituzionalità.

Concludendo: vi è certamente un'ampia e complessa base giuridica, per il trattamento, anche con l'utilizzo di sistemi IA, dei dati sanitari digitalizzati, compresi quelli del "*Fascicolo sanitario elettronico*", al di là del ristretto perimetro individuale dei singoli pazienti presso cui siano stati raccolti e per cui sia stato espresso il relativo consenso. Ma il confine con la possibile rilevanza penale delle violazioni di una tale articolata disciplina non è affatto agevole da determinare ed è, del resto, in forte evoluzione, se si considerano le innovative fonti in materia: dai regolamenti europei di recente entrata in vigore (*AI Act* ed *EDHS Act*) al disegno di legge A-1146 sull'intelligenza artificiale in corso di esame parlamentare.

Un'analoga situazione, pur 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 soprattutto in quest'ambito possono venire in rilievo le tematiche dell'*Internet of Things* (IoT), per le caratteristiche dei più moderni dispositivi sanitari. Gli incroci fra tali molteplicità di dati, compresi quelli "*personali derivati*" o "*sintetici*", potrebbe portare anche alla re-identificazione degli interessati stessi, nonostante l'anonimizzazione o pseudonimizzazione di cui si è detto, che il comma 2-*bis* dell'art. 8 d.d.l. n. 1146-A intende favorire, consentendo sempre il trattamento finalizzato ad esse, benché si tratti dei "*dati particolari*" di cui all'art. 9, par. 1 GDPR, ferma solo la previa informativa all'interessato.

4. Sulla *cybersecurity*

Nell'ambito dei trattamenti dei dati sanitari digitalizzati, emerge in modo forte il tema della *cybersecurity*, richiamata da molteplici norme anche dell'*AI Act*[30] ed oggi espressamente anche dell'*EHDS Act*, in specie agli artt. 44, dedicato alla "*gestione dei rischi posti dai sistemi di cartelle cliniche elettroniche e degli incidenti gravi*", e 73 dedicato alla necessità di "*un ambiente di trattamento sicuro che sia soggetto a misure tecniche e organizzative e rispetti prescrizioni in materia di sicurezza e interoperabilità*" che vengono poi elencate.

Pur non essendo questa la sede per l'approfondimento di questo complesso argomento, con le relative ricadute penali[31], va segnalata la ricorrente menzione dell'esigenza di sicurezza cibernetica, oggetto di molteplici obblighi incombenti sui fornitori, sui *disployer* e, più in generale, sui titolari e responsabili dei sistemi e dei trattamenti, per prevenire i rischi non solo di attacchi informatici, ma anche di incidenti e perdite accidentali.

Sul piano penale, contro fatti dolosi di terzi (intranei od estranei) si possono richiamare *de jure condito* le fattispecie che a livello nazionale puniscono, innanzitutto, l'accesso abusivo ad un sistema informatico o telematico, che deve essere "*protetto da misure di sicurezza*" per meritare tutela penale (cfr. art. 615 *ter* c.p.), a fronte di condotte criminose che possono realizzarsi anche a distanza (si pensi in particolare ai rischi che sotto questo aspetto potrebbe presentare la telemedicina, per connessioni non adeguatamente protette, anche da parte dell'utente stesso).

In secondo luogo, vengono in rilievo i danneggiamenti informatici, che siano in pregiudizio di sistemi IA, e che possono riguardare sia singoli dati o componenti *software* (art. 635-*bis* e art. 635-*ter* c.p.), sia anche componenti *hardware* (art. 635-*quater* ed art. 635-*quinquies* c.p.), secondo una differente struttura e con gravità crescente di pene, a seconda che si tratti di dati e sistemi privati ovvero pubblici, o comunque di interesse pubblico, come sono certamente quelli che vengono in rilievo nel caso delle attività sanitarie.

Nell'ampia categoria dei "*sistemi informatici*" oggetto di protezione penale vanno certamente compresi sia l'*hardware* che il *software* di sistemi IA, oltre che le infrastrutture di reti che sono alla base dei trattamenti e delle comunicazioni in esame.

Ma per la rilevanza penale di tutte le condotte incriminate, si richiede il dolo di chi agisce illecitamente, mentre comportamenti meramente colposi potrebbero avere rilievo solo sul piano delle sanzioni amministrative (come quelle previste dal GDPR, dall'*AI Act*, dall'*EHSD Act*) o della responsabilità civile.

Tuttavia, la dimensione della cybersicurezza è oggi ben più estesa di quella che viene in rilievo nei singoli delitti sopra menzionati, perché riguarda la *prevenzione* di rischi anche

---

[29] 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 die 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*" [evidenziazioni aggiunte].

[30] Senza pretesa di completezza, data la molteplicità di norme in cui compare la necessità di garantire un adeguato livello di cibersicurezza, si vedano ad es. l'art. 70, par. 4, sugli obblighi in materia che devono essere adempiuti dalle autorità nazionali; l'Allegato IV, par. 5, lettera h) relativo alla "*documentazione tecnica*" che – ai sensi dell'art. 11, par. 1 - il fornitore dei sistemi IA deve fornire.

[31] In argomento sia consentito rinviare, per un sintetico inquadramento nel diritto interno, Picotti, *Cybersecurity: quid novi?*, in *Dir. internet*, n. 1/2020, p. 11 s. Sugli ulteriori sviluppi a livello europeo e nazionale, dopo l'approvazione della c.d. NIS 2, cfr. Flor, *Cybersecurity for Artificial Intelligence e diritto penale: prime riflessioni nel prisma del diritto europeo*, in Luchtman et al. (eds.), *Of swords and shields: due process and crime control in times of globalization - Liber amicorum prof. dr. J.A.E. Vervaele*, Hague, 2023, p. 785 s.; con specifica attenzione agli aspetti tecnologici si veda Luca Viganò, *Nuove frontiere della cybersecurity*, in Picotti (a cura di), *Automazione, Diritto e Responsabilità*, Napoli, 2023, p. 213 s. A livello normativo si segnala il d. l. 10.8.2023, n. 105, conv. dalla legge 9.10.2023, n. 137, che all'art. 2-*bis* ha integrato i compiti dell'"Agenzia per la cybersicurezza nazionale", istituita con il d. l. 14.6.2021, n. 82, conv. dalla legge 4.8.2012, n. 109.

sistemici, compresi accadimenti accidentali, oltre che di attacchi informatici intenzionali che possono anche essere su larga scala, sia dall'interno, che dall'esterno: per cui la disciplina della cybersicurezza si compenetra con l'esigenza primaria di protezione e "*robustezza*" delle infrastrutture critiche, oltre che dei sistemi di AI "*ad alto rischio*", come quelli in esame.

E coinvolge, pertanto, non solo enti e soggetti pubblici, ma anche enti ed operatori privati, in specie che prestino servizi pubblici essenziali, come quelli sanitari.

Specularmente, i sistemi IA possono e debbono rafforzare la cybersicurezza, come emerge anche dall'art. 18 (rubricato: "*Utilizzo dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale*") del citato d.d.l. n. 1146-A, in forza del quale all'art. 7, comma 1, del d. l. 14.6.2021, n. 82, convertito, con modificazioni, dalla legge 4.8.2021, n. 109 (che riguarda le funzioni dell'"Agenzia per la cybersicurezza nazionale"), dopo la lettera m-*ter*), va inserita la seguente: «m-*quater*) *promuove e sviluppa ogni iniziativa, anche di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale*».

Si tratta dunque di un'esigenza cogente, anche se nello stesso d.d.l. approvato dal Senato non sono più previsti gli specifici interventi di finanziamento per gli investimenti in questo ambito, che erano invece annunciati nell'originario art. 21 dello schema di disegno di legge.

5. Sulle falsità informatiche

Infine, un semplice cenno merita anche il tema delle falsità materiali ed ideologiche che riguardino dati e documenti informatici contenuti in specie nel "*Fascicolo sanitario elettronico*" o nelle "*Cartelle sanitarie elettroniche*" e che siano eventualmente imputabili anche all'impiego di sistemi IA.

Viene in questi casi in rilievo l'art. 491-*bis* c.p., che estende espressamente l'applicabilità di tutti i delitti di falsità in atti, offensivi della c.d. fede pubblica, anche alle falsità relative a "*documenti informatici pubblici*", quali sono certamente quelli in questione, essendo tali tutti quelli che, applicando la definizione del Codice dell'Amministrazione digitale, costituiscono "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*" (art. 1, lett. p del d.lgs. 82/2005 e succ. modifiche), redatti od anche ricevuti o conservati da un pubblico ufficiale nell'esercizio delle sue funzioni[32].

Qualche nuovo problema può però suscitare l'attribuzione di una falsità materiale od ideologica, rispettivamente *ex* art. 476 o *ex* art. 479 segg. c.p., al soggetto umano che 'sta dietro' l'impiego di un sistema IA, al quale debba farsi risalire la "*contraffazione*" od "*alterazione*" del documento informatico, oppure la "*difformità dal vero*" dell'attestazione in esso contenuta, avente valore probatorio, di atti e fatti giuridicamente rilevanti.

Tali condotte potrebbero essere frutto dell'autonoma acquisizione di dati ovvero dell'autonomo trattamento realizzati dal o tramite un sistema IA. Nonostante l'oggettiva sussistenza di tali falsità, potrebbe quindi non essere accertabile il dolo di un agente umano, richiesto quale condizione per la punizione di queste fattispecie delittuose. Lo spazio di autonomia decisionale, che connota l'operato dei sistemi IA, può infatti far sfuggire l'*output* dall'ambito di concreta previsione della persona competente, per cui esso non sarebbe imputabile ad una sua volontà consapevole. Al riguardo, non può che farsi rinvio, in questa sede, ai criteri di possibile attribuzione della responsabilità penale anche per fatti dolosi, elaborati dall'*Association Internationale de Droit Pénal*, nella risoluzione della Sezione I del XXI Congresso Internazionale di Diritto penale tenutosi a Parigi il 25-28 giugno 2024, di cui si è detto[33].

6. Responsabilità medica per eventi avversi colposi

6.1. Premesse generali sulla tutela penale in materia

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

Vengono 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 legge 6.3.2017, n. 24, c.d. legge Gelli-Bianco) limita l'ambito applicativo, nei casi di "*imperizia*", "*quando sono rispettate le raccomandazioni previste dalle linee guida* [...] *ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali*" [34].

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, anche capoverso (secondo cui "*non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo*"), e 41 c.p. (secondo cui il "*concorso di cause... non esclude il rapporto di causalità*", salvo che quelle "*sopravvenute*" siano "*state da sole sufficienti a determinare l'evento*"), può far sorgere la

---

[32] Per un inquadramento sui delitti di falsità informatiche ed il commento critico della prima formulazione della norma che li ha introdotti nel codice penale italiano, si veda, volendo, PICOTTI, *Commento Art. 3 legge 23 dicembre 1993, n. 547 (Art. 491-bis cod. pen.: Documenti informatici)*, in *Legisl. pen.*, 1996, n. 1-2, p. 62 s.; sulla sua modifica cfr. ID., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2018, p. 700 s., in specie p. 701 s.; per attente osservazioni anche critiche cfr. GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491 bis c.p.*, in *Dir.inf. inf.*, 2006, p. 589 s.

[33] Cfr. i riferimenti anche bibliografici di cui alla nota 1.

[34] Sull'impatto dell'art. 590-*sexies* c.p. (introdotto dalla c.d. Leggi Gelli Bianco) sui limiti della responsabilità penale del sanitario, fra i numerosissimi contributi si veda RISICATO, *Il nuovo statuto della colpa medica: un discutibile progresso nella valutazione della responsabilità del personale sanitaria*, in *www.lalegislazionepenale.eu*, 5 giugno 2017; per un attento bilancio sintetico 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 questi in specie si veda Cass. sez. un., 21 dicembre 2017, n. 8770/18, Mariotti, Rv. 272174-75-76, annotata da CUPELLI, *La legge Gelli-Bianco nell'interpretazione delle Sezioni Unite: torna la gradazione della colpa e si riaffaccia l'art. 2236 c.c.*, in *www.penalecontemporaneo.it*, 2017, 12, 135, con ulteriori ampi rinvii.

responsabilità dell'esercente la professione sanitaria, a condizione che – oltre al menzionato nesso oggettivo di causalità - si accerti anche la relativa colpa "personale".
È stato già autorevolmente affermato che 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, stanti le caratteristiche di (relativa) imprevedibilità degli *output* forniti e dei comportamenti posti in essere "autonomamente" da tali sistemi[35].
Si creerebbe, altrimenti, uno spazio di impunità od irresponsabilità, rispetto ad offese a beni giuridici primari e diritti fondamentali della persona, quali la vita e l'incolumità personale, che richiedono e già ricevono, altrimenti, protezione penale.
Questa non può quindi venir meno, salvo adeguare i criteri di imputazione della causalità e della colpa alle peculiari caratteristiche di tali sistemi e della loro utilizzazione.
A tal fine si deve muovere dal rilievo che un sistema IA non è riducibile ad un mero strumento passivo 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 non resta nel pieno e costante dominio dell'agente umano, come potrebbe essere un bisturi o la lettura di dati clinici e della letteratura medica da parte dell'operatore stesso.
Occorre preliminarmente distinguere fra l'automazione di singole funzioni, che possono restare sotto il diretto controllo umano, e la vera "autonomia" decisionale e operativa, che basandosi su tecniche di *machine learning*, per la ricerca e selezione di dati fra le enormi quantità reperibili nel web (*big data*), ma non (tutti) disponibili al singolo operatore, nonché su algoritmi anche adattivi, porta ad *output* e comportamenti anche immediatamente eseguiti, caratterizzati, come già detto, da 'imprevedibilità' e possibile 'opacità' del processo che vi è alla base, determinando un'interazione complessa fra uomo e macchina, alla quale il primo si affida.
Escluso il riconoscimento – almeno allo stato attuale dello sviluppo tecnologico - di una soggettività o capacità penale del sistema IA in quanto tale, che non possiede una libertà cosciente di autodeterminazione, invece richiesta a fondamento dell'imputabilità ai fini penali, per cui neppure possibili sanzioni (seppur *sui generis*) potrebbero perseguire, nei suoi confronti, le funzioni (retributiva, o di prevenzione generale e speciale) proprie della pena[36], nondimeno emerge un diaframma fra l'atto umano e l'offesa dei beni giuridici penalmente rilevanti, posta in essere da o tramite detti sistemi IA, cui l'agente umano ed, in particolare, il personale sanitario 'delega' importanti attività, facendovi affidamento, data 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[37].
Ai fini della responsabilità penale per eventi avversi, che possano derivarne, occorre dunque risalire ai soggetti che 'stanno dietro' ai sistemi IA, e che in effetti decidono di utilizzarli e li utilizzano nel proprio interesse o vantaggio, seppur non egoistico, ma riferibile alla miglior terapia o al più efficace trattamento che devono e così possono porre in essere.

6.2. Sul nesso causale

Tale affidamento (o delega) rappresenta un sicuro *fattore causale*, all'origine della catena eziologica che può portare all'evento avverso. Data la menzionata struttura a forma libera dei reati in esame, dal punto di vista del rispetto del principio di legalità è sufficiente, come detto, qualsiasi contributo eziologico alla produzione dell'evento, anche di natura omissiva (*ex* art. 40 capoverso c.p.), ad es. per mancato controllo, 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 relativi alla patologia oggetto di cura e, quindi, ricadano nella sfera degli obblighi di vigilanza ed intervento che su di essi incombono[38].
Pertanto, anche di fronte alle c.d. *black box*, non essendo esimente l'*error in causa*, la scelta dell'operatore di ricorrere all'IA appare integrare quanto meno una condizione da cui dipende la causazione dell'evento, che può inserirsi od aggiungersi alla catena che va dall'ideatore al programmatore, dal produttore al fornitore, fino all'utilizzatore finale del sistema, in conformità al c.d. principio di equivalenza dei contributi causali, ricavabile dal menzionato art. 41 c.p.
In altri termini, benché l'ultimo anello della catena sia determinato dal 'comportamento' del sistema IA, e questo non

---

[35] 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* di cui *supra* a nota 1. In materia, nel dibattito penalistico, si rinvia più in generale ai contributi di BARTOLI, *La responsabilità medica tra individuale e collettivo: rischi, regole, centri di imputazione*, in BIANCHI (a cura di), *Distribuzione del rischio sanitario tra responsabilità dell'organizzazione e responsabilità individuali*, Torino 2021, p. 80 s.; CAPPELLINI, *L'"allocazione della colpa" nella responsabilità penale sanitaria*, ivi, p. 54 s.; PANATTONI, *Profili penali dell'interazione uomo-macchina nell'ambito della responsabilità medica*, in PICOTTI (a cura di), *Automazione, Diritto e Responsabilità*, cit., 269 s. Da ultimo cfr. anche AMORE, ROSSERO, *Robotica e intelligenza artificiale nell'attività medica*, cit., p. 185 s., TERRIZZI, *Medical devices e diritto penale*, cit., p. 177 s. e, volendo, PICOTTI, *Robotica ed intelligenza artificiale in medicina: possibili aspetti di rilievo penale*, in FACCIOLI (a cura di), *Profili giuridici dell'utilizzo della robotica*, cit., p. 89 s.; nel più esplorato campo della responsabilità civile si veda, oltre all'interessante contributo comparatista di GUERRA, *Profili di responsabilità del produttore del robot chirurgico nell'ordinamento americano*, ivi, 57 s., RIZZO, *Strutture della responsabilità civile e intelligenza artificiale: i problemi in medicina*, ivi, p. 1 s.; FACCIOLI, *Principi e categorie della responsabilità sanitaria alla prova della telemedicina*, in PICOTTI (a cura di), *Automazione, Diritto e Responsabilità*, cit., p. 245 s., con ampie indicazioni bibliografiche anche di carattere generale.

[36] Per riferimenti sia consentito rinviare per brevità a L. Picotti, *Intelligenza artificiale e diritto penale*, cit., p. 295 s.

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

[38] Sull'ambito di rilevanza penale di tale sfera di obblighi cfr. CAPUTO, *Colpa penale del medico e sicurezza delle cure*, Torino 2017; sui fondamenti generali già FORTI, *Colpa ed evento nel diritto penale*, Milano, 1990, nonché GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, Padova, 1993, con i necessari richiami ai molteplici autorevoli contributi precedenti.

sia assimilabile ad un mero strumento passivo, non può escludersi il nesso eziologico, in quanto con l'eliminazione mentale dell'antecedente o degli antecedenti in esame, verrebbe meno l'evento stesso.
L'autonomia dell'IA non può considerarsi, infatti, un fattore del tutto *eccezionale* ed assolutamente imprevedibile, tale da interrompere (*ex* art. 41, capoverso, c.p.) il nesso causale, salvo che anomalie, che abbiano tali caratteristiche, possano far risalire la responsabilità agli anelli anteriori della menzionata catena.
Ma nonostante la tracciabilità tecnica dell'*iter* che ha portato all'evento, può residuare una difficoltà di prova nella precisa ricostruzione ed individuazione delle caratteristiche e cause delle anomalie che lo abbiano determinato.
Per superare tali difficoltà, può sopperire la disciplina della responsabilità da prodotto difettoso, che la recente direttiva europea in materia estende anche a vizi del *software*[39], ferma la sussidiarietà della sanzione penale, rispetto alla tutela risarcitoria di natura civile. Anche la prima dovrebbe però potersi configurare, per l'esposizione a grave rischio di beni primari, se del caso con opportune scelte di politica criminale indirizzate ad un adattamento della disciplina positiva, che delimiti le condizioni e garanzie di utilizzo di detti sistemi.
Ad esempio, si potrebbero introdurre fattispecie che anticipino la soglia della tutela penale, per sanzionare quali "reati preparatori" l'impiego di "dispositivi medici", in cui rientrano anche i sistemi IA, non autorizzati o pericolosi, od irregolarmente acquisiti tramite appalti non rispettosi della disciplina in materia, finalizzata anche a garantire elevati *standard* di sicurezza.

6.3. Sulla colpa "personale"

Fondamentali principi di garanzia in materia di responsabilità penale richiedono che la sua attribuzione si basi, oltre che sull'elemento oggettivo sopra delineato, su di un rimprovero giuridico "personale", quantomeno di natura colposa, come si ricava dall'art. 27, commi 1 e 3, Cost., oltre che dagli artt. 42 e 43 c.p.
Colpa penale che diverge da quella civile, essendo esclusa ogni forma di responsabilità per fatto altrui, ad es. del dipendente, o di responsabilità c.d. per posizione, anziché per la propria azione od omissione, come pure qualsivoglia ricorso a presunzioni.
Come si è già sottolineato a proposito del ruolo del consenso al trattamento sanitario (*supra* par. 2), ci troviamo nel campo di attività lecite di base, dato che l'invasione anche materiale della sfera corporea del paziente non costituisce una "lesione" personale, ai sensi dell'art. 582 c.p., non essendo causa di una "malattia" ma, al contrario, essendo un intervento a favore del paziente stesso e della sua salute, data la funzione, più che la semplice "finalità" terapeutica della condotta stessa, diretta a curare la patologia preesistente, con i debiti adattamenti rispetto alla chirurgia ed ai trattamenti estetici.
In tale contesto, l'impiego di sistemi IA offre la massima utilità, per l'entità e qualità di informazioni, ampie ed aggiornate, di cui possono e devono disporre in tempo reale, con limitazione della possibilità di errore ed incremento della precisione e rapidità di diagnosi ed intervento.
Il nodo problematico è quello dell'eventuale violazione delle c.d. regole cautelari che devono essere rispettate, anche nel ricorso ai sistemi IA, trattandosi comunque di attività 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 colpa ai fini penali - non appare applicabile ai sistemi IA in quanto tali, che non sono persone umane ed operano con proprie caratteristiche e modalità tecniche.
Per cui il parametro di riferimento deve essere, piuttosto, quello assai ampio della "miglior scienza ed esperienza" del settore in cui intervengono.
Ma la negligenza, imprudenza ed imperizia punibili non possono imputarsi direttamente ai sistemi IA. Per cui occorre – come si è detto - risalire all'agente umano che "sta dietro", al quale potrebbe rimproverarsi, oltre che l'eventuale esito infausto o lesivo, anche di non aver fatto ricorso, potendolo, ai sistemi IA disponibili.
Una particolare questione pone al riguardo il tema cruciale della perizia, dato che, come si è ricordato, non è punibile l'imperizia quando si seguano 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*" (art. 590-*sexies* c.p.).
È evidente che questi precetti non sono essere diretti ai sistemi IA, ma al personale sanitario che "vi sta dietro", la cui osservanza fonda l'esonero da responsabilità[40]. Per cui occorrerà che le predette raccomandazioni ed, eventualmente, buone pratiche clinico-assistenziali da rispettare, siano integrate ed aggiornate con riferimento all'impiego delle tecnologie in questione, includendo i casi e modi in cui si debba o possa fare ricorso ai sistemi IA disponibili, nonché le caratteristiche che debbano possedere, da impostare e garantire già a monte del loro concreto utilizzo.

---

[39] 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.

[40] È stato prospettato ed enfatizzato in dottrina il cambio di paradigmi che comporterebbe il ricorso massivo ai sistemi AI 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 nel 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 devolve 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 (cfr. AMORE, ROSSERO, *Robotica e intelligenza artificiale nell'attività medica*, cit., p. 199 s., 215 s.). Pur suggestiva nella prospettiva avveniristica in cui si colloca, la tesi non appare 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, che si sta in effetti incontrovertibilmente delineando a livello interno e sovranazionale.

Per questo, si dovrebbe prevedere ed implementare uno specifico sistema di autorizzazioni e di verifiche di "conformità" ad elevati *standard* di precisione ed accuratezza, di competenza dell'Autorità sanitaria, con obbligo di monitoraggio e segnalazione di eventi avversi anche a carico di chi li utilizza, compresi gli enti ospedalieri e sanitari in genere, secondo meccanismi già collaudati in altri settori, come quello della circolazione dei veicoli a guida autonoma, introdotto ad es. in Germania.

La violazione di una siffatta disciplina extrapenale potrebbe essere fonte di responsabilità penale pur di fronte a comportamenti "imprevisti" dei sistemi in questione, che sono quelli maggiormente temibili, non occorrendo, per l'imputazione a titolo di colpa, che questa sia "cosciente", vale a dire implichi la previsione concreta dell'evento causato, e che costituisce un'eventuale circostanza aggravante propria dei reati colposi (*ex* art. 61, n. 2 c.p.). In generale, è sufficiente la "possibilità di prevedere" vale a dire la c.d. prevedibilità non già del singolo evento concreto che si possa verificare, ma della tipologia di eventi cui esso appartenga e che le misure cautelari hanno per l'appunto la finalità di evitare.

Il modello più adeguato appare, in questo contesto, quello della c.d. colpa specifica, che presuppone la formulazione in regole scritte di comportamento di dette misure cautelari, aventi funzione di prevenzione o, quantomeno, riduzione dei rischi ad un livello accettabile (quello del c.d. rischio consentito), tenuto conto dei vantaggi che porta l'impiego di tali sistemi IA: regole che possono o anzi debbono essere fornite già dai produttori e manutentori, anche privati, oltre che dalle Autorità competenti al rilascio delle autorizzazioni al loro uso ed al loro controllo.

Si tratta di una prospettiva che include anche la responsabilità per negligenza ed imprudenza, rispetto a cui non opererebbe l'esonero stabilito dal controverso art. 590 *sexies* c.p., e che pare integrarsi con il modello più generale della c.d. "colpa di organizzazione" basata su un previo *risk assessment* (come sostanzialmente delineato dall'*AI Act* per qualsiasi utilizzazione lecita di sistemi IA). Gli operatori, in ogni ambito in cui agiscono, devono infatti identificare previamente non solo le tipologie ed i livelli dei rischi connessi alla produzione ed all'utilizzazione dei predetti sistemi nelle specifiche attività in cui vanno impiegati, ma anche di "organizzare" ogni ente ed impresa, che intervenga nella loro fase di vita, dall'ideazione e programmazione, fino alla produzione, distribuzione, manutenzione ed utilizzazione finale, in modo tale che siano stabilite ed efficacemente attuate e controllate - con una chiara attribuzione di competenze ed istituzione di appositi organismi interni - le più adeguate misure organizzative e cautelari, in funzione specificamente preventiva, necessarie per ridurre e contenere i predetti rischi nell'ambito di quelli accettabili o "consentiti" nel bilanciamento con i vantaggi che offrono.

Su tali basi normative extrapenali, il concreto rimprovero di colpa alla persona umana od all'ente che "stanno dietro" all'utilizzazione di questi sistemi da cui sia derivato un evento avverso, non potrebbe più considerarsi quale inammissibile "colpa per non aver previsto l'imprevedibile", come è stato detto[41], ma per la violazione di quelle cautele, anche organizzative, specificamente finalizzate ad evitare che si verifichino eventi della tipologia di quello realizzatosi: violazioni che quindi, in conformità all'essenza normativa della colpa, assorbono i requisiti della prevedibilità ed evitabilità da parte dell'agente, in quanto l'evento stesso realizzerebbe proprio lo specifico rischio che le predette norme extrapenali miravano a contrastare o ridurre, in conformità al loro scopo cautelare.

E questo non esclude, ma anzi consente che, a fondamento della responsabilità penale per colpa, si debba ravvisare anche quella "rimproverabilità giuridica" *soggettiva*, consistente nella disapprovazione dell'ordinamento per non aver agito diversamente da quanto sarebbe stato possibile e doveroso per la singola persona.

Tali considerazioni assumono una chiara rilevanza pratica, se si considera che questi sistemi IA vengono per lo più impiegati o resi disponibili, anche ai singoli operatori sanitari, da strutture organizzate e complesse, come le aziende ospedaliere od i presidi sanitari del territorio. Nel loro ambito è, quindi, possibile individuare sia le posizioni di garanzia assunte da chi è deputato a controllare le specifiche fonti di rischio, in base alle competenze attribuite, non necessariamente coincidenti con le posizioni apicali; sia le eventuali carenze che possano integrare quella "colpa di organizzazione" cui si è fatto riferimento, e che ne può fondare la responsabilità per i fatti colposi che si verifichino, per non aver valutato adeguatamente i rischi, e/o non aver preso le misure organizzative e cautelari, nonché di monitoraggio ed attenzione ai segnali d'allarme per eventi avversi, che devono essere oggetto di adeguati "modelli organizzativi" (c.d. MOG), cui fa riferimento paradigmatico il d.lgs. 231/2001, che prevede e regola la responsabilità "da reato" delle persone giuridiche e degli enti[42].

6.4. Prospettive de jure condendo

De jure condito, il limite di applicazione di questa disciplina nel settore in esame è però duplice.

Innanzitutto, sono ad essa sottratti espressamente gli enti pubblici, salvo che svolgano attività economiche (art. 1, comma 3, d.lgs. 231/2001), e tali non sono considerate le attività sanitarie, che non perseguono fini di lucro. Per cui potrebbe interessare solo le aziende ospedaliere private[43].

---

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

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

[43] Per un caso di estensione a società non soltanto private, ma a partecipazione mista, si veda però – in sede cautelare – Cass., sez. II, 9-21.7.2010, n. 28699, con nota di 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.

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. 231/2001).

Per cui appare necessario ed urgente un intervento del legislatore, che ponga rimedio a tali carenze di disciplina, ed estenda l'elenco dei reati per cui può operare, data la vitale (e crescente) importanza dei sistemi IA in campo sanitario.

Tale intervento novellistico non è invero previsto nel disegno di legge governativo 1146-A, che pur dedica, come si è visto, l'art. 7 all' "*Uso dell'intelligenza artificiale in ambito sanitario e di disabilità*"[44]. E tale norma richiama, al comma 5, il principio antropocentrico, già proclamato in generale dall'art. 1, prevedendo che "*I sistemi di intelligenza artificiale nell'ambito sanitario costituiscono un* supporto *nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la* decisione, *che* è sempre rimessa alla professione medica" [evidenziazioni aggiunte]. Ne dovrebbe discendere la riaffermazione anche dell'eventuale responsabilità penale *personale*, visto altresì che al comma successivo si stabilisce che "*I sistemi di intelligenza artificiale utilizzati nell'ambito sanitario e i relativi dati impiegati devono essere affidabili* e periodicamente verificati e aggiornati *al fine di minimizzare il rischio di errori*" [evidenziazioni aggiunte].

Ma fra le deleghe legislative al Governo previste dall'art. 24, al comma 3 si fa riferimento ad una disciplina soltanto per i "*casi di realizzazione ed impiego* illeciti *di sistemi di intelligenza artificiale*", sulla base dei criteri direttivi enunciati nel successivo comma 5, in cui contraddittoriamente si prevedono alla lettera b) "*autonome fattispecie di reato, punite* a titolo di dolo o di colpa, *incentrate sulla* omessa *adozione o* l'omesso *adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale*" punibili solo se " *da tali* omissioni *deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato*" [evidenziazioni aggiunte]. Reati, quindi, che si configurano soltanto quali "*omissioni*" con evento di pericolo, realizzabili nel contesto di un utilizzo di base *lecito*, come quello che avviene in ambito sanitario, da cui possono peraltro conseguire anche *eventi* avversi causati "*per colpa*". Sarebbe in definitiva auspicabile una maggior chiarezza e coerenza al riguardo.

Mentre è da salutare con favore la previsione - introdotta nei lavori del Senato in sede referente, di cui alla lettera c) dell'art. 24, comma 3 – secondo cui la norma delegata dovrà 'precisare' "*i criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale*". Ma manca poi un'indicazione di criteri direttivi al riguardo, essendo espressa solo l'esigenza generica che si "*tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente*".

Certamente, piuttosto che un'estensione della sfera di responsabilità penale attraverso l'introduzione di nuove fattispecie, od un generalizzato aggravamento di pene, tramite circostanze aggravanti comuni (*ex* art. 26, comma 1, lettera a) o speciali per singoli delitti peraltro dolosi (*ex* art. 26, comma 1, lettera b) e commi 2 e 4 del menzionato d.d.l. 1146 – A) [45], è auspicabile una più attenta rielaborazione ed integrazione dei criteri di imputazione, anche a titolo di colpa, della responsabilità penale o punitiva nell'ambito delle complesse strutture che dispongono, quali *diployer*, dei sistemi IA e del loro utilizzo, estendendo ed adeguando il perimetro di applicazione del d.lgs. 231/2001 all'intero ambito delle attività sanitarie oggetto d'esame.

7. Conclusioni: esigenze di tutela penale ed adeguamento delle categorie penalistiche.

L'importanza della sanzione penale, compresa quella per la responsabilità 'da reato' dell'ente, che può anche prescindere dalla concreta individuazione della singola persona fisica che nel suo ambito lo abbia realizzato (cfr. art. 8 d.lgs. 231/2001), ha un'essenziale funzione di monito e di guida al comportamento corretto, conforme a diritto, e non pare rinunciabile, in coerenza con il criterio guida già richiamato, secondo cui quanto sarebbe penalmente rilevante, se il fatto fosse commesso da una persona umana, non può essere penalmente irrilevante, soltanto perché vi è l'intervento di un sistema AI.

Tanto più che, di fronte ai nuovi impetuosi sviluppi tecnologici ed all'estensione tumultuosa delle relative applicazioni anche nel campo medico-sanitario, si estenderebbero inaccettabili aree di impunità, che lascerebbero sforniti di adeguata tutela beni ed interessi giuridici, nonché diritti fondamentali, quali la vita, l'integrità personale, la libertà di autodeterminazione in campo sanitario, la *privacy*, la sicurezza cibernetica, la fede pubblica, che già sono invece oggetto di una protezione penale che non appare rinunciabile, a favore di quella che potrebbe essere offerta da altre tecniche di tutela, come quelle civilistica ed amministrativistica, specie se si considera anche il profilo processuale dei mezzi di indagine ed acquisizione della prova.

È dunque indispensabile un attento e calibrato adeguamento delle categorie penalistiche, sostenuto da un oculato intervento del legislatore, che dovrebbe a monte sopperire alle lacune riscontrabili, integrandosi con la nuova disciplina europea sopra menzionata, in modo che il ricorso allo strumento penale non sia un demagogico sostituto, ma davvero l'*ultima ratio* di una tutela che trovi solido fondamento nella disciplina organica del settore, innovato in modo così dirompente dall'estesa digitalizzazione e dall'avvento dell'intelligenza artificiale.

E per questo obiettivo, la dottrina ed il confronto interdisciplinare possono dare il necessario contributo ai fini di un compiuto inquadramento sistematico, di un'analisi critica della normativa esistente e di una progettazione futura delle riforme che il legislatore deve introdurre, per sopperire alle lacune riscontrate.

---

[44] Cfr. *supra*, par. 2.1.

[45] È prevista alla lettera c) di detta norma anche l'introduzione di un nuovo delitto doloso, quale art. 612-*quater* c.p., per contrastare il fenomeno del c.d. *deep fake*, denominato di "Illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale".