NEURAL NEXUS Review
Rivista scientifica ufficiale di **ENIA**
Ente Nazionale per l'Intelligenza Artificiale
https://neuralnexus-review.org/

Data di ricezione: 10.06.25 / Data accettazione: 29.09.25 / Data di pubblicazione: 18.11.25
doi: 10.82015/NNR.2025.100109

Intelligenza artificiale in sanità: introduzione all'approccio dell'AI Act per la sua regolamentazione

Artificial Intelligence in medicine: an introduction to the AI Act approach to regulating the matter

Silvia Stefanelli[1]

Sintesi

Il documento affronta tematiche legate all'intelligenza artificiale per finalità generali, con un focus specifico sulle implicazioni normative, etiche e tecnologiche. Vengono analizzati i principali rischi associati all'adozione di modelli di AI generativa, inclusi aspetti di sicurezza, trasparenza e protezione dei dati. Si presta particolare attenzione al quadro regolatorio europeo, con riferimento all'AI Act e al General-purpose AI Code of practice. Il testo propone inoltre linee guida per la governance responsabile dell'IA suggerendo approcci interdisciplinari che bilancino innovazione e tutela dei diritti fondamentali. Infine, si discutono scenari futuri e strategie di mitigazione dei rischi sistemici legati agli sviluppi rapidi della tecnologia ai.

Parole chiave: Legge sull'IA; GPAI; Approccio basato sul rischio; Codici di Condotta per l'IA e scopo generale; Sistemi di IA ad alto rischio.

[1] Avvocata, abilitata al patrocinio presso la Corte di Cassazione e fondatrice dello studio legale Stefanelli & Stefanelli. È specializzata in diritto sanitario, con particolare competenza in sanità digitale, dispositivi medici, pubblicità sanitaria, contratti con la pubblica amministrazione, protezione dei dati e intelligenza artificiale. E-mail: s.stefanelli@studiolegalestefanelli.it.

Abstract

The document addresses issues related to general artificial intelligence, with a specific focus on regulatory, ethical, and technological implications. It analyzes the main risks associated with the adoption of generative AI models, including aspects of security, transparency, and data protection. Particular attention is paid to the European regulatory framework, with reference to the AI Act and the General-purpose AI Code of Practice. The text also proposes guidelines for responsible AI governance, suggesting interdisciplinary approaches that balance innovation and the protection of fundamental rights. Finally, it discusses future scenarios and strategies for mitigating the systemic risks associated with rapid developments in AI technology.

Keywords: AI Act; GPAI; Risk Based Approach; General purpose ai codes of conduct; High risk ai systems.

1. Introduzione

L'Intelligenza Artificiale (IA) sta trasformando profondamente il settore sanitario, offrendo soluzioni innovative che spaziano dalla diagnosi precoce alla personalizzazione delle terapie, dall'ottimizzazione dei processi amministrativi al supporto decisionale per i clinici. L'analisi avanzata dei dati, la capacità di individuare pattern nascosti e la possibilità di automatizzare compiti ripetitivi stanno già migliorando la qualità delle cure, aumentando l'efficienza delle strutture e rendendo l'assistenza più centrata sul paziente.

Alcuni campi in cui sta avvenendo tale rivoluzione sono quelli della medicina predittiva, della diagnostica e della diagnostica per immagini. Infatti, l'analisi predittiva tramite l'IA può analizzare i dati provenienti da dispositivi per il monitoraggio continuo del glucosio da e altri dispositivi indossabili per prevedere i picchi di zucchero nel sangue nell'ambito di terapie per la gestione del diabete (Kwon and Moon2025; Zahedani et al. 2023; Maiorino et al. 2020); nella diagnostica avanzata, l'IA può essere in grado di anticipare una diagnosi di Alzheimer grazie all'analisi incrociata di scansioni cerebrali, cartelle cliniche e modelli di linguaggio, identificando precocemente sintomi o segni della malattia, altrimenti non rilevabili per mezzo dei metodi tradizionali (Li et al. 2024); infine, la capacità di analisi dell'IA ha raggiunto livelli di precisione straordinari anche nella diagnostica per immagini, permettendo di identificare in immagini mediche le anomalie che potrebbero altrimenti sfuggire all'occhio umano[2].

Dal punto di vista concreto si riportano qui alcuni casi già attivi in Istituti di Ricovero e Cura a Carattere Scientifico (di seguito IRCCS) o Ospedali universitari:

- IRCCS San Raffaele Milano sta lavorando sui Progetti AI-SCoRE e AI-HOPE AI-SCoRE (Artificial Intelligence – Sars Covid Risk Evaluation)[3] – il primo è una

[2] Pesheva, E. (2024). *Does AI Help or Hurt Human Radiologists' Performance? It Depends on the Doctor*. Harvard Medical School. https://shorturl.at/yc1V5.

[3] HSR Research (2020). *AI-SCORE, a project to calculate prognostic risk from Covid-19*. IRCCS Ospedale San Raffaele: scientific research. https://shorturl.at/ai0gt.

piattaforma di apprendimento autonomo che analizza varie informazioni cliniche relative ad un paziente per determinare il rischio che sviluppi forme grave di COVID-19, mentre il secondo progetto mira all'efficientamento dell'assistenza sanitaria fornita (Palmisano et al. 2022);

- IRCCS Mario Negri Milano - Progetto I3LUNG - strumento decisionale per aiutare medici e pazienti nella selezione della migliore cura per il tumore polmonare[4];
- Ospedale Cardarelli e Università Federico II di Napoli - sistema di IA per interpretare TAC del pancreas e identificare tumori anche di dimensioni inferiori ai 2 centimetri (Romano 2023);
- Università di Torino e Ospedale Molinette – sistema di IA per la predizione del rischio cardiovascolare (De Ferrari et al. 2021);
- CNR in collaborazione con l'Università di Firenze – studio per l'individuazione precoce dell'Alzheimer attraverso l'apprendimento automatico (Conti et al. 2024).

Al tempo stesso, più di recente la sanità ha visto anche la diffusione e lo sviluppo di sistemi che utilizzano la c.d. IA generativa. Alcuni esempi già attivi in Italia di questo genere sono:

- IEO e Centro Cardiologico Monzino - Clinical Data Platform con MedLM di Google - Utilizzo di MedLM, il Large Language Model di Google specifico per la sanità, per analizzare grandi quantità di dati non strutturati[5];
- SIICP – MedQuestio – Piattaforma di IA generativa sviluppata dalla Società Italiana Interdisciplinare per le Cure Primarie specificatamente per medici italiani[6].

[4] Istituto Mario Negri (2022). I3LUNG: un progetto HORIZON EUROPE per l'implementazione di cure mediche personalizzate basate sull'intelligenza artificiale (AI) nei pazienti con tumore al polmone.
[5] IEO-Monzino: Converting unstructured clinical data into structured data for scientific research with Google Cloud (https://cloud.google.com/customers/ieo-monzino).
[6] MedQuestio fornisce contenuti da pubblicazioni scientifiche *peer-reviewed*, validati dal Comitato Scientifico SIICP e corredati da riferimenti bibliografici puntuali per ogni risposta clinica. Sito ufficiale SIICP: www.siicp.it; Sito MedQuestio: www.medquestio.it.

Le importanti innovazioni sopra descritte, destinate a cambiare il volto della sanità italiana, dovranno però confrontarsi con il nuovo Regolamento UE 2024/1689 (c.d. AI Act) che disciplina l'immissione sul mercato e l'utilizzazione dei sistemi di IA e dei modelli IA per finalità generali. Nei paragrafi che seguono si analizzano la normativa di riferimento e le sue conseguenze per il settore sanitario.

2. AI Act: inquadramento generale

L'AI Act rappresenta il primo framework normativo globale per la regolamentazione dell'IA. Pubblicato in Gazzetta Ufficiale dell'Unione Europea il 12 luglio 2024.
Questo regolamento segna l'inizio di una nuova era per i software basati su sistemi di IA, stabilendo per la prima volta a livello mondiale regole precise per la progettazione, la realizzazione e l'immissione sul mercato dei prodotti intelligenti.
L'approccio adottato dall'Unione Europea è sicuramente ambizioso. Peraltro, l'ambito soggettivo di applicazione della normativa, per come definito all'articolo 2 c. 1 lett. a) dell'AI Act, comprende non soltanto i fornitori di sistemi di IA stabiliti nell'Unione Europea, ma anche quelli con sede extra-UE che tuttavia immettono tali sistemi nel mercato europeo. Ciò potrebbe comportare un'estensione dell'influenza dell'approccio normativo adottato, ed eventualmente delle stesse norme di cui al nuovo regolamento, anche al di fuori dei confini europei, potenzialmente a livello internazionale.
L'AI Act adotta una struttura normativa consolidata, seguendo l'architettura giuridica del New Legislative Framework comunitario, nell'ambito del quale rientrano anche il Regolamento UE 2017/745 (c.d. MDR)[7] e il Regolamento UE 2017/746 (c.d. IVDR)[8].

[7] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.
[8] Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione

Coerentemente con l'impostazione di tale quadro generale, con il quale l'Europa si è data l'obiettivo di migliorare il mercato interno dei prodotti e facilitare la libera circolazione delle merci tra gli Stati membri attraverso una costellazione di regolamentazioni di prodotto, anche l'AI Act adotta un approccio basato sul rischio (c.d. risk-based approach).

Anche grazie all'impostazione descritta, l'AI ACT si inserisce in modo coerente nel panorama della legislazione di prodotto a livello europeo, ed in particolare, per quanto rilevante in ambito sanitario, con quella che disciplina la commercializzazione di dispositivi medici e diagnostici in vitro, facilitando così l'implementazione per gli operatori già attivi in questo campo.

Il regolamento si articola attraverso diverse sezioni: dopo aver stabilito l'ambito di applicazione, e dunque aver fornito una definizione di cosa si debba intendere per IA (o meglio, "sistema di IA", nelle parole della normativa), esso identifica il gruppo delle pratiche di AI vietate e, successivamente, si divide in due macro-gruppi di norme: quelle dedicate ai sistemi di IA c.d. *ad alto rischio*, e quelle invece relative ai modelli e sistemi di IA per finalità generali.

Il presente contributo intende proprio focalizzarsi sulla descrizione e il commento di questa struttura di base. Dopo una breve introduzione alla definizione di IA adottata dall'AI Act e al *risk-based approach*, si procederà prima alla descrizione della classificazione effettuata dalla normativa per i sistemi ad alto rischio e poi di quella scelta per i modelli/sistemi per finalità generali.

3. Le scelte definitorie dell'AI Act

Definire esattamente cosa dovesse intendersi per "Intelligenza Artificiale" è stato per il legislatore europeo un compito assai arduo. Ciò non soltanto in ragione della mancanza di un generale consenso in merito, a livello tecnico-scientifico, etico-filosofico oppure giuridico, ma anche per la necessità di identificare una definizione che fosse un

adeguato bilanciamento tra i vari interessi in gioco e, in ultima istanza, che non comportasse né sotto- né sovra-regolamentazione. Infatti, se da un lato definire "IA" nel modo più ampio possibile, ossia tale da ricomprendere il maggior numero di sistemi, contribuisce a tutelare al massimo i diritti fondamentali delle persone coinvolte nel suo sviluppo ed utilizzo, dall'altro comporta anche che un maggior numero di prodotti software ricadono nell'ambito oggettivo della nuova normativa, con potenziali ripercussioni in termini di aumento degli obblighi per gli operatori economici coinvolti, delle prescrizioni da rispettare, dei requisiti di prodotto e, in ultimo, dei potenziali profili sanzionatori (Presno Linera e Meuwese 2025; Rangone e Megale 2025).

La sintesi effettuata dall'AI Act ha comportato la definizione di due macro-gruppi di prodotti-IA: i *sistemi di IA,* definiti come "*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*" (articolo 3 par. 1); i *sistemi di IA per finalità generali*, ossia "*un sistema di IA basato su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA*" (articolo 3 par. 66) dove per *modello di IA per finalità generali* deve intendersi "*un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato*" (articolo 3 par. 63).

La definizione di sistema di IA è stata poi più approfonditamente analizzata dalla Commissione europea nel documento *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, in cui

viene ulteriormente chiarito che sono sette gli elementi chiave per la caratterizzazione di un software come *sistema di IA,* ossia: che il sistema sia automatizzato; sia progettato per operare con diversi livelli di autonomia; possa anche manifestare ad attività durante il suo ciclo di vita, pur non essendo questo un elemento fondamentale; abbia obiettivi espliciti o impliciti; elabori dati in input per generare output in base a inferenze; produca previsioni, contenuti, raccomandazioni o decisioni; possa influenzare ambienti fisici o virtuali.

Soltanto, dunque, quei software che presentano tutte le caratteristiche identificate dall'AI Act come necessarie e sufficienti per la qualificazione come *sistema di IA* dovranno rispettare la nuova regolamentazione, sia in termini di requisiti di prodotto che di obblighi a carico degli operatori economici coinvolti. La valutazione resta da effettuarsi, inevitabilmente, caso per caso[9].

D'altra parte, per quanto concerne invece i sistemi e modelli di IA per finalità generali, è intervenuto il documento *Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)* a chiarire ulteriormente alcuni concetti base. Innanzitutto, viene ribadito che tali modelli sono addestrati su grandi quantità di dati (anche tramite autoapprendimento su larga scala) e che essi mostrano una significativa generalità, nonché capacità di eseguire un'ampia gamma di compiti distinti. Ciò, dunque, in contrasto con quei sistemi che possono essere definiti a scopo specifico, per i quali invece la destinazione d'uso sia ben identificata (Triguero et al. 2023).

Viene poi ribadita l'esclusione di quei modelli che, pur ricadendo nella definizione di cui all'AI Act, siano tuttavia sviluppati ed utilizzati per ricerca, sviluppo o prototipazione prima della loro commercializzazione. La Linea Guida, inoltre, propone il criterio del training compute per identificare quando un modello sia da considerarsi *per finalità generali,* ovvero quello della quantità di operazioni in virgola mobile (FLOP) necessarie

[9] Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).

per addestrare il modello, identificando il valore soglia di 10231023 FLOP. A tale criterio, poi, occorre aggiungere quello della capacità del modello di generare linguaggio, immagini o video da testo.

3. Il Risk-based approach e la sua applicazione all'IA

Il fondamento strutturale dell'AI Act è il c.d. *risk-based approach*, in base al quale le norme, che stabiliscono divieti, obblighi o adempimenti, vengono tutte calibrate in ragione del conseguente rischio posto dall'oggetto della norma stessa a diritti fondamentali delle persone fisiche in vario modo coinvolte oppure a principi considerati di rango "costituzionale" (Ebers 2025).

Le ragioni dell'adozione di tale approccio risiedono principalmente nell'esigenza di bilanciare la spinta dell'innovazione, il progresso scientifico ed una certa libertà del mercato, con la protezione di interessi rilevanti che potrebbero essere violati da pratiche commerciali o prodotti (sistemi di IA, in questo caso) non adeguatamente controllati (Kusche 2024).

Il risk-based approach come fondamento della regolamentazione, come detto, non è nuovo. Si ritrova infatti a più riprese nella regolamentazione di prodotto, come ad esempio nel MDR, dove al crescere della classe di rischio del dispositivo medico considerato aumentano anche e di conseguenza le norme da seguire e gli obblighi da rispettare per gli operatori economici, ma anche, come autorevolmente rilevato, nella normativa in materia di trattamento dei dati personali (Regolamento UE 2016/670 – General Data Protection Regulation o GDPR) (Gellert 2021).

Nel contesto specifico dell'AI Act, il *risk-based approach* ha informato in primis e a monte la suddivisione e classificazione delle varie tipologie di IA: relativamente ai sistemi di IA sono stati previsti *sistemi di IA vietati*, per i quali il legislatore europeo ha ritenuto che il rischio dal loro utilizzo fosse eccessivo e dei quali sono stati dunque radicalmente vietati, *sistemi di IA ad alto rischio*, identificati dall'articolo 6 con precisi

criteri, ed inoltre due categorie individuate indirettamente, ossia i *sistemi di IA a rischio minimo* e quelli *senza rischio*; per i modelli/sistemi di IA per finalità generali, la classificazione prevede i gruppi di quelli con e senza rischio sistemico.

3.1. Sistemi di IA – I sistemi di IA vietati

La prima categoria è quella dei sistemi di AI vietati, ossia quelli che sono stati considerati dal legislatore europeo come un rischio inaccettabile per i diritti fondamentali e gli interessi di rilevanza costituzionale. Il novero dei sistemi di IA vietati è dunque a numero chiuso, con elenco contenuto all'articolo 5 AI Act.

Tra questi si segnalano in particolare: sistemi che utilizzano tecniche subliminali o manipolative per alterare il comportamento umano in modo da causare danni rilevanti, compromettendo la libertà e l'autonomia personale; sistemi che sfruttano vulnerabilità specifiche come età, disabilità o particolari condizioni socioeconomiche, creando situazioni di sfruttamento o discriminazione; sistemi di "social scoring", che valutano o classificano persone basandosi su comportamenti o caratteristiche personali, con conseguenze discriminatorie o ingiustificate.; sistemi di identificazione biometrica remota in tempo reale in spazi pubblici senza autorizzazione, con rischi di sorveglianza di massa che ledono la privacy e le libertà fondamentali; sistemi che estraggono dati biometrici non mirati da fonti online o telecamere per creare database di riconoscimento facciale senza consenso; sistemi di riconoscimento delle emozioni usati in contesti come scuola o lavoro, che violano la privacy e la dignità degli individui; sistemi di polizia predittiva basati su profiling che possono ledere la presunzione di innocenza e il diritto a un giusto processo; sistemi che classificano persone usando informazioni sensibili come razza, religione, orientamento politico.

Sulla base dell'elenco di tale articolo 5 AI Act è possibile derivare un elenco di diritti fondamentali o interessi considerati di rilevanza costituzionale che vengono protetti dall'individuazione di tali divieti, indicati nel recente documento *Commission Guidelines*

on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act): la dignità umana e la libertà individuale, dal momento che alcune ipotesi dell'articolo 5 sono volte a tutelare la capacità decisionale autonoma e la libertà di scelta degli individui; la non discriminazione e l'uguaglianza; la privacy e la protezione dei dati personali; la sicurezza pubblica e la tutela della legalità; la tutela della vulnerabilità di persone fragili, come minori, anziani o disabili, impedendo l'uso di IA che sfruttino tali vulnerabilità.

4.1.1. I sistemi di AI ad alto rischio

La seconda categoria è quella dei sistemi di AI ad alto rischio, tra cui rientrano molti dei software utilizzati in ambito sanitario (c.d. SAMD - *software as medical device*).
L'articolo 6 AI Act prevede due gruppi di sistemi di IA ad alto rischio.
Relativamente al primo gruppo, per determinare quando un sistema di IA debba essere considerato *ad alto rischio* sono stabiliti due criteri cumulativi*:* (i) quando sia un prodotto regolato da una delle normative elencate nell'Allegato I, oppure sia destinato ad essere utilizzato come componente di sicurezza di un prodotto e (ii) la valutazione di conformità ai sensi di tale normativa prevede il coinvolgimenti di un *Notify Body*, ossia l'ente designato a livello europeo per effettuare prove, ispezioni, certificazioni e controlli di conformità di prodotti che, secondo il legislatore europeo, pongono un rischio per l'utilizzatore e che sono regolati da una normativa del New Legislative Framework, prima che vengano immessi sul mercato, garantendo così la protezione della salute, della sicurezza e dei diritti fondamentali degli utenti. Solo dopo aver superato con esito positivo questa valutazione, i prodotti possono infatti essere marcati CE e commercializzati nell'Unione Europea. Specificamente, in ambito sanitario sono quindi considerati ad alto rischio i SAMD (o componenti di sicurezza di un dispositivo medico) che rientrino in classe IIa, IIb e III nel MDR, o di classi B, C e D nell'IVDR.
Per quanto invece riguarda il secondo gruppo, l'articolo 6 stabilisce che sono

considerati automaticamente *ad alto rischio* tutti quei sistemi di IA elencati nell'Allegato III, che include, per l'ambito sanitario, i sistemi destinati a gestire l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e la fruizione degli stessi (ossia "*i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche 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*" e "*i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza*").

I sistemi di IA ad alto rischio sono soggetti a una serie di requisiti stringenti pensati per garantire sicurezza, affidabilità e tutela dei diritti fondamentali. Tali requisiti, dettagliati nella sezione 2, capo III dell'AI Act, includono: la dotazione di un sistema di gestione dei rischi (articolo 9); requisiti in materia di governance dei dati e qualità degli stessi (articolo 10); documentazione tecnica e registrazione dei log (articolo 11-12); trasparenza e informazione (articolo 13); supervisione umana (articolo 14); accuratezza, robustezza e cybersicurezza (articolo 15). Più specificamente, l'articolo 9 stabilisce che ogni sistema di IA ad alto rischio deve essere supportato da un sistema di gestione dei rischi continuo e iterativo, di cui deve dotarsi il provider (ossia colui che progetta, o fa progettare, e commercializza il sistema di IA, ai sensi dell'articolo 3 par. 3). Questo processo deve identificare, analizzare, valutare e mitigare i rischi noti o prevedibili posti dal sistema di IA, sia nella fase di progettazione che durante l'intero ciclo di vita del sistema, inclusa la fase di monitoraggio post-immissione sul mercato.

L'AI Act contiene poi all'articolo 10, e con innovazione rispetto ad altre normative di prodotto, norme che riguardano la qualità dei dati da utilizzare per "addestrare, validare e testare il sistema" e i principi di governance degli stessi. In particolare, il

regolamento prescrive che questi siano "*di alta qualità, rappresentativi, privi di bias e rilevanti per l'ambito di applicazione*". I successivi articoli 11 e 12, inoltre, stabiliscono che i provider devono predisporre e mantenere aggiornata una documentazione tecnica dettagliata che permetta alle autorità di valutare la conformità del sistema alle norme applicabili. Inoltre, diviene obbligatoria la registrazione delle attività dell'IA ad alto rischio (log) per garantire la tracciabilità delle operazioni e facilitare eventuali audit o indagini. L'articolo 13 disciplina gli obblighi di trasparenza e informazione che gravano sui provider e sugli utilizzatori di sistemi di IA ad alto rischio.

Riassumendo, quello che l'AI Act richiede è che da un lato tali sistemi siano progettati in modo che il loro funzionamento sia sufficientemente chiaro per gli utenti e gli utilizzatori, soprattutto in termini di capacità, significato del risultato fornito e limiti del sistema stesso. Viene poi richiesto che i sistemi di IA ad alto rischio siano dotati di istruzioni, anche in formato digitale, che forniscano informazioni concise, complete, chiare e corrette, e che siano esse stesse pertinenti, facilmente accessibili e comprensibili per i deployer designati, al fine di assicurare un utilizzo consapevole e sicuro del sistema. Infine, da un lato l'obbligo di garantire un adeguato livello di supervisione umana viene dettato dall'articolo 14, al fine di consentire all'uomo di intervenire, monitorare e, se necessario, interrompere il funzionamento del sistema per prevenire o mitigare rischi per la sicurezza o i diritti fondamentali, dall'altro l'articolo 15 richiede che i sistemi di IA ad alto rischio siano tutti progettati e sviluppati conformemente ad elevati livelli di accuratezza, e cybersicurezza, prevenendo quanto più possibile malfunzionamenti, errori e manipolazioni. Devono inoltre essere adottate misure di cybersicurezza per proteggere il sistema da accessi non autorizzati, attacchi informatici e altre minacce. Per quanto infine concerne gli obblighi dei provider per la corretta immissione in commercio di tali prodotti, il rispetto dei menzionati requisiti deve essere valutato nel contesto della c.d. valutazione di conformità, analisi tradizionalmente richiesta da tutte le regolamentazioni di prodotto, la quale può essere svolta in autonomia dal provider oppure congiuntamente con un Notified Body a ciò

designato, in base alla tipologia e all'ambito di applicazione (articolo 43). È infine previsto un obbligo di monitoraggio continuo del sistema, per verificare che la sua conformità all'AI Act si mantenga costante nel tempo, e l'obbligo di aggiornare le misure di sicurezza in base all'evoluzione delle minacce poste dal sistema e ad eventuali vulnerabilità dello stesso.

4.1.2. I sistemi di IA a rischio limitato e a rischio minimo/nullo

L'AI Act direttamente non menziona la categoria dei sistemi di IA a rischio limitato oppure nullo. Queste ultime possono tuttavia ricavarsi in via interpretativa dalla struttura del Regolamento e dalle sue norme, dal momento che l'articolo 52 risulta applicabile a tutte le IA che non si qualifichino come *ad alto rischio*, ma che comunque ricadano nell'ambito di applicazione del Regolamento.
L'articolo 52, infatti, prescrive obblighi di trasparenza per tutti quei sistemi di IA che possano in qualche modo influenzare le scelte o i comportamenti degli utenti, quali ad es. chatbot, sistemi che danno raccomandazioni, ecc.
Anche in questo caso, come in quello dell'articolo 5 per i sistemi di IA vietati, l'elenco di sistemi di IA per cui viene stabilito l'obbligo di trasparenza è chiuso, con indicazione specifica di quale attività debba svolgere ciascuno perché tale obbligo sia previsto a carico di provider e/o deployer.
Di conseguenza, la categoria dei sistemi di IA a rischio nullo può essere identificata soltanto per sottrazione, e cioè come composta da tutti quei software che rientrino nella definizione di *sistema di IA* ai sensi dell'AI Act, ma non siano ad alto rischio (perché non rispondendi ai requisiti ivi previsti) e nemmeno a rischio limitato (perché non presentano le funzionalità specificamente elencate nell'articolo 52). Rientrano in questa categoria, ad esempio, filtri antispam, videogiochi abilitati con l'IA, ecc e a tali prodotti non si applicherà l'AI Act, bensì soltanto le eventuali norme che regolano la sicurezza dei prodotti in generale, quali ad esempio il Regolamento UE 2023/988.

4.2 I modelli di IA per finalità generali con e senza rischio sistemico

In data 30 novembre, mentre erano in corso i lavori di approvazione dell'AI Act, è stato lanciato ChatGPT (Marr 2023), ossia il modello di intelligenza artificiale conversazionale sviluppato da OpenAI e progettato per interagire con le persone attraverso il linguaggio naturale, e, che è in grado di comprendere domande, fornire risposte, creare testi, tradurre, scrivere codice, e molto altro — simulando una conversazione umana in modo fluido e coerente.

Si tratta, più specificamente, di un modello di IA per finalità generali, posto che rientrano nella suddetta categoria, come visto, tutti quei modelli progettati per eseguire un'ampia gamma di compiti che non sono limitati a uno specifico scopo, ma possono essere adattati a molti contesti e applicazioni diverse (articolo 3, par. 63 AI Act)

Per tale ragione, il legislatore comunitario ha dunque aggiunto al Capo V una disciplina specifica dedicata proprio a tale tipologia di modelli, diventata pienamente efficacie il 2 agosto 2025. Proprio a partite da questa data troveranno quindi applicazione tutti gli obblighi previsti per i modelli in oggetto. È evidente, allora, come l'argomento risulti di particolare attualità e urgenza per tutti gli operatori del settore.

Si presume che un modello di IA per finalità generali abbia capacità di impatto elevato a norma del paragrafo 1, lettera a), quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10.

Il regolamento distingue tra modelli generici e modelli che presentano rischi sistemici, introducendo obblighi progressivamente più stringenti. Le regole di classificazione sono quelle fornite dall'articolo 51 AI Act, che stabilisce che un modello di IA per finalità generali, nella definizione sopra descritta, è classificato come *a rischio sistemico* se sono rispettate almeno una delle due condizioni previste alle lettere a) e b): "*a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento",* dove per impatto elevato il successivo comma 2 chiarisce che deve intendersi "*quando la quantità cumulativa di*

calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10^25 FLOPS"; e *b) sulla base di una decisione della Commissione, ex officio o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII*".

I fornitori di modelli per finalità generali devono adempiere a una serie di obblighi specifici che includono la redazione e il mantenimento di documentazione tecnica aggiornata, il supporto ai fornitori che intendono integrare il modello nei loro sistemi di IA, e la pubblicazione di una sintesi dettagliata dei contenuti utilizzati per l'addestramento (articolo 53 AI Act) (Gstrein, Haleem e Zwitter 2024). Inoltre, per i modelli a rischio sistemico, gli obblighi previsti dal regolamento risultano maggiormente stringenti, dal momento che questi sono tenuti a compiere una valutazione secondo protocolli standardizzati, a svolgere test di contraddittorio per individuare rischi sistemici, implementare misure di valutazione e attenuazione dei rischi, tracciare e sono altresì tenuti alla documentazione di eventuali incidenti gravi, garantendo pure un'adeguata protezione della cybersicurezza (articolo 55 AI Act).

L'articolo 56 stabilisce poi che l'Ufficio dell'IA (articolo 64) ha il compito di creare Codice di condotta per lo sviluppo di modelli di IA per finalità generali: questi Codici dovranno mantenere aggiornate le informazioni sull'IA, descrivere come utilizzare i dati per addestrare l'IA e come identificare e gestire potenziali rischi.

3. Il Codice di condotta per i modelli di IA per finalità generali

Come anticipato, i modelli di IA per finalità generali sono modelli assai versatili, abilitati allo svolgimento di compiti diversi e utilizzabili in molteplici contesti e applicazioni[10].

[10] Per un approfondimento sull'approccio dell'AI Act alla regolamentazione dell'intelligenza artificiale (AI) per uso generico, si veda: Gstrein O. J., Haleem N., and Zwitter A. (2024) *General-purpose AI regulation and the European Union AI Act*, *Internet Policy Review*, 13(3), 1-26.

La potenza e l'adattabilità che li caratterizzano rendono quindi necessaria una particolare attenzione, soprattutto in termini di governance e regolamentazione.
Compito dei Codice di condotta è proprio quello di regolamentare lo sviluppo, la distribuzione e l'uso dei suddetti modelli, prima della definitiva entrata in vigore di obblighi legali più stringenti – quali quelli previsti dall'AI Act – fungendo da vero e proprio strumento di transizione atto a preparare il terreno in vista della regolamentazione obbligatoria.
In data 10 luglio 2025 sono stati pubblicato le versioni definitive del Codice di Condotta per le GPAI, adottati su base volontaria, e che contengono una serie di indicazioni e di misure volte a garantire che i modelli GPAI siano sviluppati e utilizzati in modo sicuro, trasparente, affidabile e responsabile[11].
Elaborati da quattro gruppi di lavoro presieduti da esperti indipendenti, il documento si articola in tre sezioni principali – Trasparenza, Copyright e Gestione del rischio e sicurezza – e si rivolge ai fornitori dei modelli in oggetto, la cui adesione alle indicazioni ivi contenute favorisce l'obiettivo generale di "migliorare il funzionamento del mercato interno, promuovere l'adozione di un'intelligenza artificiale incentrata sull'uomo e affidabile, garantendo al contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la tutela dell'ambiente, contro gli effetti negativi dell'IA nell'Unione, e sostenere l'innovazione a norma dell'articolo 11) della legge sull'IA".

3.1. Trasparenza: informazione e documentazione

La sezione dedicata alla trasparenza stabilisce tre misure fondamentali che i fornitori devono adottare per rispettare gli obblighi previsti dalla normativa europea.
La prima misura riguarda la redazione e il mantenimento aggiornato della

[11] https://digital-strategy.ec.europa.eu/it/policies/contents-code-gpai

documentazione del modello. Più specificamente, all'atto dell'immissione del modello sul mercato, il fornitore è chiamato a predisporre una documentazione tecnica completa, che dia atto di tutti gli aspetti più significativi che lo caratterizzano. A tal fine, il Codice fornisce in appendice un apposito modulo, suddiviso in diverse sezioni che, compilato dal fornitore, consente di adempiere alla suddetta misura.

La documentazione relativa modello andrà periodicamente aggiornata – soprattutto laddove il modello subisca modifiche significative – e le versioni precedenti dovranno essere conservate per un periodo minimo di dieci anni[12].

La seconda misura si concentra sulla fornitura di informazioni pertinenti ai fornitori.

In particolare, il Codice richiede ai fornitori di divulgare tramite il proprio sito web le informazioni di contatto dell'Ufficio IA e dei fornitori a valle per richiedere accesso alle informazioni pertinente contenute nella documentazione del modello o altre informazioni comunque necessarie[13].

È inoltre specificato che, su richiesta dei fornitori a valle, i firmatari del Codice sono tenuti a fornire informazioni ulteriori rispetto a quelle contenute nella documentazione del modello, qualora queste si rendano necessarie alla piena comprensione delle capacità e dei limiti del modello di IA per finalità generali, nonché all'adempimento degli obblighi ai sensi dell'AI Act.

La terza ed ultima misura assicura la qualità, sicurezza e integrità delle informazioni documentate. La qualità e l'integrità di tutte le informazioni documentate devono infatti essere oggetto di apposito controllo, e proprio a tal fine i firmatari sono incoraggiati all'adozione di appositi protocolli e standard stabiliti, sia in fase di elaborazione ed aggiornamento delle informazioni, sia in sede di controllo della qualità e della sicurezza delle informazioni e dei registri[14].

È evidente, quindi, l'obiettivo di questa prima sezione del Codice, ossia quello di

[12] Commissione Europea. Codice di condotta per i modelli di IA per finalità generali, Capitolo sulla trasparenza, Misura 1.1, p. 5.
[13] Ivi, p. 5.
[14] Ivi, p. 6.

agevolare l'attività di ispezione e supervisione dei modelli. L'intento è infatti quello di fornire alle Autorità competenti, l'AI Office, e agli altri soggetti interessati (come *downstream provider*) gli elementi tecnici necessari per verificare la sicurezza, i rischi, i *bias* e la correttezza del modello, promuovendone un uso responsabile.

3.1. Copyright: conformità e rispetto dei diritti

La sezione copyright introduce misure specifiche per garantire conformità alla disciplina unionale sul diritto d'autore ed è quindi direttamente collegato all'articolo 53(1)(c) dell'AI Act, che impone ai fornitori di modelli GPAI di dotarsi di una politica sul copyright che rispetti la legislazione dell'UE e dei paesi membri (Scalzini 2025; Lucchi 2024; Yang e Zhang 2024).

Il capitolo prevede un unico impegno generale – articolato, a sua volta, in cinque misure specifiche – che tutti i fornitori di GPAI devono rispettare[15]. A questi ultimi viene innanzitutto richiesto di redigere, mantenere aggiornata e attuare una specifica politica sul copyright, che identifichi i responsabili organizzativi per l'implementazione e la supervisione[16].

Le misure operative previste in questo capitolo pongono inoltre particolare attenzione all'attività di raccolta dei dati dal web e, con particolare attenzione alle attività di *web crawling*, ossia di scansione o indicizzazione automatica dal web.

In particolare, quando si raccolgono dati dal web per addestrare modelli, devono essere usati solo contenuti legalmente accessibili, rispettando segnali automatici (come *robots.txt*) ed evitando siti noti per violazioni del copyright[17].

È inoltre previsto l'inserimento di salvaguardie tecniche e operative per evitare che il modello generi contenuti che infrangono il copyright. Attività, quest'ultima, che può

[15] Ivi, p. 4.
[16] Ibidem.
[17] Commissione Europea. Codice di condotta per i modelli di IA per finalità generali, Capitolo sul copyright, Misura 1, p. 5.

concretizzarsi nell' inclusione di filtri, meccanismi di controllo dei contenuti generati, politiche nei termini di servizio che vietino l'uso improprio[18].

Andrà inoltre fornito un punto di contatto dedicato per i titolari di diritti, con modalità chiare per l'invio di reclami e la gestione dei suddetti andrà garantita in modo diligente e entro tempi ragionevoli[19].

Infine, pur non risultando sempre obbligatoria la pubblicazione dell'intera politica, ne viene incoraggiata una versione riassuntiva pubblica, volta a rendere chiari gli impegni e a favorire fiducia e trasparenza[20].

Nell'ottica di contribuire ad uno sviluppo dell'IA rispettoso della normativa europea, il capitolo in oggetto traccia quindi una serie di misure che, rendendo i fornitori dei modelli responsabili del rispetto delle norme, orientino ad un uso lecito dei dati di addestramento dei modelli, così favorendone uno sviluppo progressivo e sostenibile.

3.1. Gestione del rischio e sicurezza: il quadro operativo

La sezione più corposa è quella relativa a "sicurezza e protezione", che si concentra su misure, responsabilità e pratiche volte a prevenire l'uso improprio dei modelli, a mitigarne i rischi e a garantire lo sviluppo e la distribuzione dell'IA in modo sicuro e responsabile.

Il quadro si articola in diverse macro-aree che definiscono un approccio sistemico alla gestione del rischio[21]. Si da atto, infatti, non solo di profili relativi alla sicurezza tecnica del modello e al possibile utilizzo improprio dello stesso, ma anche delle modalità attraverso le quali garantirne una distribuzione sicura e un monitoraggio efficiente.

---

[18] Ivi, p. 6.
[19] Ibidem.
[20] Ibidem.
[21] Per una maggiore comprensione del rischio sistemico nella governance dell'IA, si veda: Hacker, P., Kasirzadeh, A., and Edwards, L. (2025). AI, Digital Platforms and the New Systemic Risk, arXiv:2509.17878.

Più specificamente, sono dieci gli impegni che il terzo e ultimo capitolo prevede per i fornitori di modelli di IA per finalità generali a rischio sistemico[22].

Il primo impegno individua il c.d. "Quadro di riferimento per la sicurezza" contenente misure per mantenere i rischi sistemici entro livelli accettabili, criteri di accettazione del rischio sistemico, e procedure di implementazione delle misure[23]. Più specificamente, tale misura fa sì che i firmatari del Codice si impegnino a delineare – proprio attraverso il predetto "Quadro" – i processi e le misure di gestione dei rischi sistemici da essi implementate. L'efficacia del quadro andrà continuamente aggiornata e migliorata attraverso l'applicazione pratica e l'acquisizione di nuove conoscenze, dando atto (nell'apposito registro) delle modifiche effettuate e delle ragioni che le hanno motivate[24].

Il secondo, il terzo ed il quarto impegno riguardano invece tutte quelle attività preposte alla valutazione del rischio sistemico. In particolare, il Codice richiede ai fornitori di selezionare e caratterizzare i rischi sistemici significativi, di svolgere analisi del rischio con diversi gradi di profondità e intensità, e di determinare l'accettabilità confrontandoli con i criteri predefiniti[25].

Tali valutazioni sono essenziale rilevanza, poiché orientano in maniera importante la decisione finale circa la messa a disposizione del modello sul mercato.

Il quinto ed il sesto impegno si occupano invece delle misure volte alla mitigazione del rischio tecnico[26].

Si fa riferimento, quindi, a tutte quelle misure tecniche e operative funzionali alla riduzione dei rischi sistemici a livelli accettabili lungo tutto il ciclo di vota del modello e a quelle nonché a quelle necessarie a proteggere il modello da accessi non autorizzati,

---

[22] Per un approfondimento sulle GPAI a rischio sistemico, si veda Uuk, R., Gutierrez, C. I., Guppy,D., Lauwaert, L., Kasirzadeh, A., Velasco, L., Slattery, P., Prunkl, K. (2024). A Taxonomy of Systemic Risks from General- Purpose AI. arXiv:2412.07780.

[23] Commissione Europea. Codice di condotta per i modelli di IA per finalità generali, Capitolo sulla sicurezza e protezione copyright, Misura 1, p. 6.

[24] Ivi, p. 9.

[25] Ivi, p. 10 e ss.

[26] Ivi, p. 16 e ss.

furti, diffusioni abusive, inclusi i rischi interni. Le migliori pratiche di cybersecurity dovranno dunque essere implementate proprio per contrastare tali tipi di minacce[27].

L'implementazione di mitigazioni tecniche, all'avanguardia e proporzionali ai rischi sistemici, deve inoltre coprire l'intero ciclo di vita del modello e, in caso di incidenti gravi, i fornitori sono però tenuti ad attuare misure aggiuntive.

Gli ultimi impegni di questa sezione del Codice fanno infine riferimento alle misure di mitigazione del rischio di governance.

Questa macro area include anche la predisposizione del "rapporto sul modello di sicurezza e protezione"[28], ossia quel documento tecnico che – comunicato all'Ufficio IA prima dell'immissione del modello sul mercato e, comunque, periodicamente aggiornato – ne descrive, tra l'altro, l'architettura, i rischi sistemici identificati, le mitigazioni applicate, le giustificazioni per accettare certi rischi, le valutazioni per l'assegnazione di responsabilità e risorse proporzionate alla complessità organizzativa, l'ottenimento di valutazioni esterne indipendenti, la segnalazione tempestiva degli incidenti gravi, la protezione dei lavoratori che forniscono informazioni sui rischi e in generale, tutte le informazioni per la comprensione pubblica dei rischi.

Alla luce di questa disamina risulta del tutto evidente l'adozione, anche in sede di redazione del Codice di condotta di un approccio *risk based*. Anziché optare per l'applicazione uniforme dello stesso corpo di regole a tutti i modelli, genericamente intesi, gli impegni e le misure di sicurezza ivi contenute, sono infatti proporzionati al livello di rischio sistemico che il modello può generare.

[27] Per un approfondimento sulle nuove frontiere della cybersecurity nell'ambito delle IA, si veda: Kulothungan, V. (2025). Securing the AI frontier: Urgent Ethical and Regulatory Imperatives for AI-driven Cybersecurity, arXiv:2501.10467.

[28] Commissione Europea. Codice di condotta per i modelli di IA per finalità generali, Capitolo sulla sicurezza e protezione copyright, p. 17 e ss.

3. Conclusioni

L'AI Act europeo stabilisce un precedente mondiale straordinario nella regolamentazione dell'intelligenza artificiale, introducendo un framework normativo che influenzerà significativamente lo sviluppo e l'implementazione di sistemi AI nel settore sanitario.

Nel settore sanitario, l'integrazione dell'IA rappresenta, senza dubbio, una delle sfide e delle opportunità più significative dell'innovazione tecnologica contemporanea. In tale particolare sede, la corretta classificazione dei sistemi è fondamentale per valutarne in modo proporzionato i requisiti di sicurezza, trasparenza e supervisione umana richiesti per ciascuna applicazione.

Per tale ragione, partendo da un inquadramento generale, la disamina in oggetto ha analizzato l'approccio concretamente adottato a livello comunitario per la regolamentazione della materia e, partendo da un focus sulle diverse classificazioni dei sistemi AI si è successivamente spostata sul "tema caldo" del più recente futuro: le GPAI e la loro regolamentazione attraverso il Codice di condotta.

La crescente diffusione di modelli di IA per finalità generali solleva interrogativi assai spinosi sulla tracciabilità degli output, sulla gestione delle responsabilità e sul potenziale riuso in contesti non previsti in fase di sviluppo. Interrogativi, questi ultimi particolarmente rilevante in ambito sanitario, dove le implicazioni etiche, cliniche e legali sono particolarmente sensibili.

È proprio in tal senso, che l'emergere di codici di condotta specifici per i modelli GPAI, come previsto anche dall'AI Act, rappresenta uno strumento normativo e operativo cruciale, posto che si tratta di modelli in grado di che offrire linee guida concrete ai fornitori di sistemi GPAI e agli sviluppatori di soluzioni sanitarie che ne fanno uso, garantendo maggiore affidabilità, sicurezza e rispetto dei diritti fondamentali.

Le scadenze imminenti – e, in particolare, l'entrata in vigore degli obblighi per i modelli AI per finalità generali già in data 2 agosto 2025 – richiedono allora una preparazione

tempestiva da parte di tutti gli stakeholder ed in particolare di quelli del settore sanitario: la complessità della materia impone infatti un approccio multidisciplinare che coinvolga esperti legali, tecnici e clinici per garantire una transizione efficace verso il nuovo paradigma normativo.

Alla luce della disamina svolta, quindi, è evidente che l'adozione responsabile dell'IA in sanità richieda non solo innovazione tecnica, ma anche una solida infrastruttura regolatoria e deontologica. Solo una maggiore convergenza tra classificazioni di rischio, codici di condotta e prassi cliniche potrà infatti garantire che l'uso dell'intelligenza artificiale nel settore sanitario avvenga nel rispetto dell'interesse pubblico e della dignità umana.

Riferimenti bibliografici

1. Commissione Europea (2025). *Codice di condotta per i modelli di IA per finalità generali*, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai.
2. Conti, F., Banchelli, M., Bessi, V., Cecchi, C., Chiti, F., Colantonio, S., D'Andrea, C., de Angelis, M., Moroni, D., Nacmias, B., Pascali, M. A., Sorbi, S., Matteini, P. (2024). Harnessing topological machine learning in Raman spectroscopy: Perspectives for Alzheimer's disease detection via cerebrospinal fluid analysis. *Journal of the Franklin Institute*, 361(18), 107249. https://doi.org/10.1016/j.jfranklin.2024.107249.
3. De Ferrari, G. M., Aldinucci, M., et al. (2021). Machine learning for predicting outcomes in patients with acute myocardial infarction. *The Lancet, 397*, 199.
4. Ebers, M. (2025). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation, 16*(2), 684–703. https://doi.org/10.1017/err.2024.78
5. Gellert, R. (2021). The role of the risk-based approach in the General Data Protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? *Journal of Ethics and Legal Technologies, 3*(2), 15–33. https://doi.org/10.14658/pupj-jelt-2021-2-2.
6. Gstrein, O. J., Haleem, N., and Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review, 13*(3). https://doi.org/10.14763/2024.3.1790
7. Hacker, P., Kasirzadeh, A., and Edwards, L. (2025). AI, digital platforms and the new systemic risk. *arXiv preprint.* https://arxiv.org/abs/2509.17878.
8. Hao, J. , Kwapong, W. R., Shen, T., Fu, H., Xu, Y., Lu, Q., Liu, S., Zhang, J., Liu, Y., Zhao, Y., Zheng, Y., Frangi, A. F., Zhang, S., Qi, H., and Zhao Y. (2024). Early detection of dementia through retinal imaging and trustworthy AI. *npj Digital Medicine, 7*, 281. https://doi.org/10.1038/s41746-024-01292-5
9. HSR Research (2020). *AI-SCORE, a project to calculate prognostic risk from Covid-19*. IRCCS Ospedale San Raffaele: scientific research. https://shorturl.at/ai0gt.
10. IEO-Monzino. Converting unstructured clinical data into structured data for scientific research with Google Cloud - https://cloud.google.com/customers/ieo-monzino.
11. Istituto Mario Negri. (2022). *I3LUNG: Un progetto Horizon Europe per l'implementazione di cure mediche personalizzate basate sull'intelligenza artificiale (AI) nei pazienti con tumore al polmone*.
12. Kulothungan, V. (2025). Securing the AI frontier: Urgent ethical and regulatory imperatives for AI-driven cybersecurity. *arXiv preprint*. https://doi.org/10.1109/BigData62323.2024.10826010.

13. Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI Act: Fundamental rights and risk. *Journal of Risk Research*, 1–14. https://doi.org/10.1080/13669877.2024.2350720.

14. Kwon, S. Y., and Moon, J. S. (2025). Advances in continuous glucose monitoring: Clinical applications. *Medicina, 60*(12), 1951. https://doi.org/10.3803/EnM.2025.2370.

15. Ledro, C., Nosella, A., and Vinelli, A. (2022). Artificial intelligence in customer relationship management: Literature review and future research directions. *Journal of Business and Industrial Marketing, 37*(13), 48–66. https://doi.org/10.1108/JBIM-07-2021-0332

16. Lucchi, N. (2024). ChatGPT: A case study on copyright challenges for generative artificial intelligence systems. *European Journal of Risk Regulation, 15*(Special Issue 3), 602–624. https://doi.org/10.1017/err.2023.59.

17. Maiorino, M. I., Signoriello, S., Maio, A., Chiodini, P., Bellastella, G., Scappaticcio, L., Longo, M., Giugliano, D. and Esposito, K. (2020). Effects of continous glucose monitoring on metrics of glycemic control in diabetes: A systematic review with meta-analysis of randomized controlled trials. *Diabetes Care, 43*(5), 1146–1156. DOI: 10.2337/dc19-1459.

18. Marr, B. (2023). A short history of CHATGPT: How we got to where we are today. *Forbes*. https://shorturl.at/UdoqU.

19. Palmisano, A., Vignale, D., Boccia, E., Nois, A., Gnasso, C., Leone, R., Montagna, M., Nicoletti, V., Bianchi, A. G., Brusamolino, S., Dorizza, A., Moraschini, M., Veettil, R., Cereda, A., Toselli, M., Giannini, F., Loffi, M., Patelli, G., Monello, A., Iannopollo, G., Ippolito, D., Mancini, E. M., Pontone, G., Vignali, L., Scarnecchia, E., Iannacone, M., Baffoni, L., Sperandio, M., de Carlini, C. C., Sironi, S., Rapezzi, C., Antiga, L., Jagher, V., Di Serio, C., Furlanello, C., Tacchetti, C., Esposito, A., (2022). AI-SCoRE (Artificial Intelligence – SARS-CoV-2 Risk Evaluation): a fast, objective and fully automated platform to predict the outcome in COVID-19 patients. *Cardiac radiology*, (127):960-972. https://doi.org/10.1007/s11547-022-01518-0.

20. Pesheva, E. (2024). *Does AI Help or Hurt Human Radiologists' Performance? It Depends on the Doctor*. Harvard Medical School. https://shorturl.at/yc1V5.

21. Presno Linera, M. Á., and Meuwese, A. (2025). Regulating AI from Europe: A joint analysis of the AI Act and the Framework Convention on AI. *The Theory and Practice of Legislation*, 1–20. https://doi.org/10.1080/20508840.2025.2492524.

22. Rangone, N., and Megale, L. (2025). Risks without rights? The EU AI Act's approach to AI in law and rule-making. *European Journal of Risk Regulation*, 1–16. https://doi.org/10.1017/err.2025.13

23. Romano, L. and Università Federico II. (2023). *L'intelligenza artificiale può interpretare le immagini TAC del pancreas, vedendo un tumore duttale che il radiologo può non riuscire a diagnosticare perché troppo piccolo*. Ospedale Cardarelli Napoli - Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione Università Federico II.

24. Scalzini, S. (2025). Scientific authorship e intelligenza artificiale: Questioni e prospettive. *FSE – Online First* (10). https://shorturl.at/KtNVp.

25. Triguero, I., Molina, D., Poyatos, J., Del Ser, J., and Herrera, F. (2023). General purpose artificial intelligence systems (GPAIS): Properties, definition, taxonomy, open challenges and implications. *arXiv preprint*. https://arxiv.org/abs/2307.14283.

26. Uuk, R., Gutierrez, C. I., Guppy, D., Lauwaert, L., Kasirzadeh, A., Velasco, L., Slattery, P., and Prunkl, K. (2024). A taxonomy of systemic risks from general-purpose AI. *arXiv preprint*. https://doi.org/10.2139/ssrn.5030173.

27. Yang, S. A., and Zhang, A. H. (2024). Generative AI and copyright: A dynamic perspective. *arXiv preprint*. https://doi.org/10.2139/ssrn.4716233.

28. Zahedani, A.D., McLaughlin, T., Veluvali, A., Aghaeepour, N., Hosseinian, A., Agarwal, S., Ruan, J., Tripathi, S., Woodward, M., Hashemi, N., and Snyder, M. (2023). Digital health application integrating wearable data and behavioral patterns improves metabolic health. *npj Digital Medicine*, 6, 216. https://doi.org/10.1038/s41746-023-00956-y.