STEFANELLI & STEFANELLI STUDIO LEGALE

Reg. Ue 2024/1967
AI ACT

INTELLIGENZA ARTIFICIALE

Avv. Silvia Stefanelli

Gazzetta ufficiale dell'Unione europea

IT
Serie L

2024/1689

12.7.2024

REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 13 giugno 2024

che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

OBBIETTIVI POLITICI

DIVENTARE UN LEADER MONDIALE

CREARE FIDUCIA NELLA IA

RISPETTARE I DIRITTI DELL'UNIONE

FACILITARE GLI INVESTIMENTI

SVILUPPARE UN MERCATO UNICO

AI ACT è
LEGISLAZIONE DA PRODOTTO

il concetto di fondo è

identificare i rischi del software e della sua utilizzazione
e stabilire i requisiti per gestire i rischi

CREARE FIDUCIA E SICUREZZA NELL'UTILIZZO

OBBIETTIVI GIURIDICI

TITOLO I – DISPOSIZIONI GENERALI

- **Norme armonizzate per l'immissione sul mercato, la messa in servizio** e l'uso di sistemi di intelligenza artificiale («sistemi IA») nell'Unione;
- **Divieti di alcune pratiche** di IA;
- **requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori** di tali sistemi;
- **regole di trasparenza armonizzate** per alcuni sistemi di IA;
- **d bis) norme armonizzate per l'immissione sul mercato di IA per uso generale;**
- **e) Norme sul monitoraggio del mercato, sulla governance della sorveglianza del mercato e sull'applicazione delle norme;**
- **ea) misure a sostegno dell'innovazione,** con particolare attenzione alle PMI, comprese le start-up.

TITOLO I	**DISPOSIZIONI GENERALI**
TITOLO II	**PRATICHE AI AI VIETATE**
TITOLO III	**SISTEMI AI AD ALTO RICHIO**
TITOLO IV	**OBBLIGHI DI TRASPARENZA**
TITOLO V	**MODELLI AI SCOPI GENERALI**
TITOLO VI	**MISURE SOSTEGNO INNOVAZIONE**
TITOLO VII	**GOVERNANCE**
TITOLO VIII	**BANCA DATI UE SISTEMI ALTO RICHIO**
TITOLO IX	**MONITORAGGIO POST-MARKET, CONDIVISIONE, SORVEGLIANZA MERCATO**
TITOLO X	**CODICI CONDOTTA**
TITOLO XI	**DELEGA DI POTERI E PROCEDURE DEL COMITATO**
TITOLO XII	**RISERVATEZZA E SANZIONI**
TITOLO XIII	**DISPOSIZIONI FINALI**

ART. 2 - AMBITO DI APPLICAZIONE

a) ***ai fornitori*** *che immettono sul mercato o mettono in servizio sistemi di IA immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;*

b) ***ai deployer*** *dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione;*

c) ***ai fornitori e ai deployer*** *di sistemi di IA che hanno il loro luogo di stabilimento o sono* ***situati in un paese terzo****, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione;*

d) *agli importatori e ai distributori di sistemi di IA;*

ART. 3 - DEPLOYER

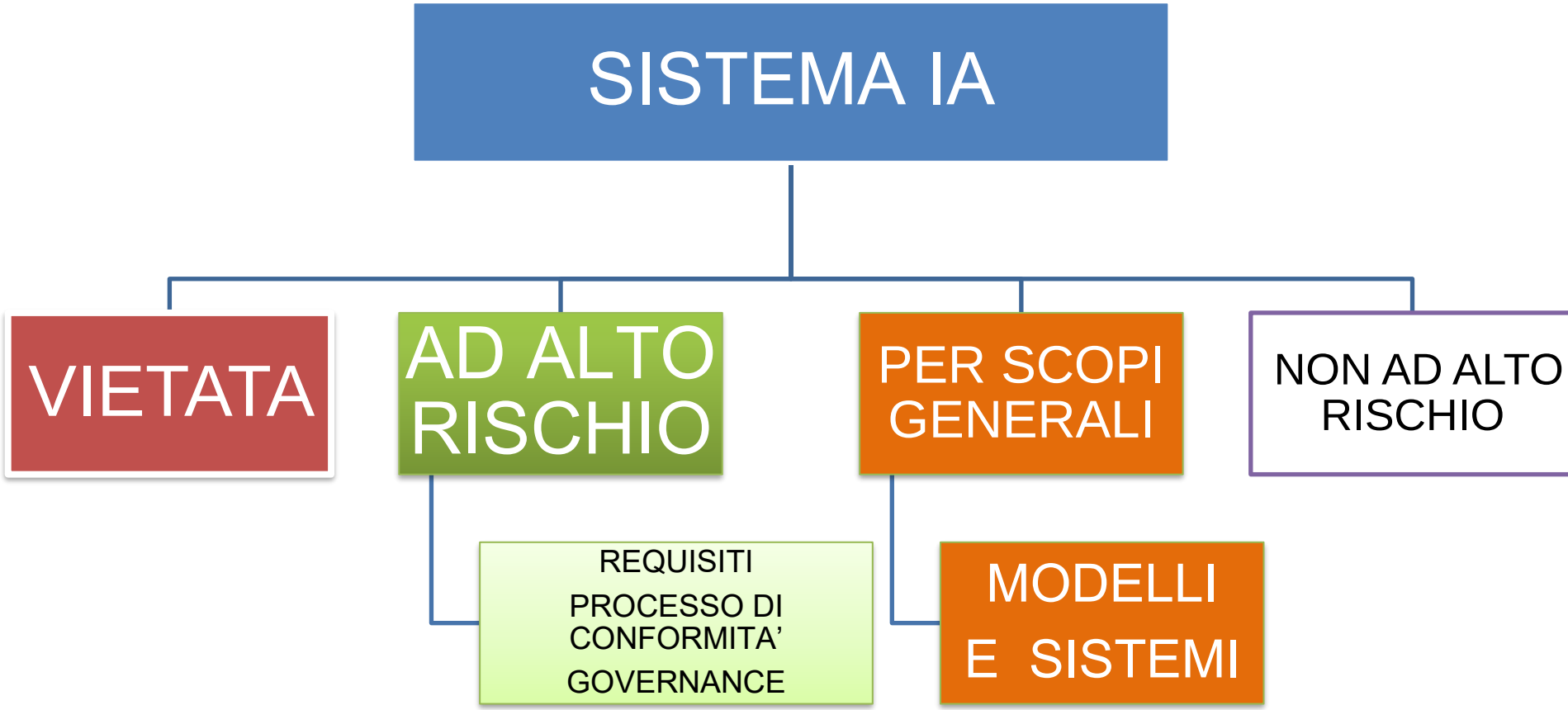
4) *«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che* ***utilizza*** *un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;*

DEFINIZIONE

Art. 3
«sistema di IA»

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;

ARCHITETTURA GIURIDICA



IA VIETATA

PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE

Art. 5

Sono vietate le seguenti pratiche di intelligenza artificiale:

- IA che utilizza tecniche subliminali o tecniche manipolative/ingannevoli con l'obiettivo di distorcere il comportamento di una persona o di un gruppo di persone compromettendo in modo significativo la capacità di prendere una decisione informata;
- IA che sfrutta una qualsiasi delle vulnerabilità di un gruppo specifico di persone;
- IA che usi sistemi di categorizzazione biometrica che classifichi individualmente le persone fisiche sulla base dei loro dati biometrici per dedurne origine razziale, opinioni politiche, appartenenza sindacale, ecc;
- IA per la valutazione o la classificazione dell'affidabilità delle persone fisiche per un certo periodo di tempo sulla base del loro comportamento sociale o delle loro caratteristiche personali, che porti a conseguenze pregiudizievoli, ingiustificate o sproporzionate per le stesse;
- Sistemi di identificazione biometrica a distanza "in tempo reale" in spazi accessibili al pubblico, a meno che il loro uso sia strettamente necessario per:
  - Ricerca mirata di vittime di rapimento, tratta di esseri umani, ecc;
  - Prevenzione di una minaccia specifica all'incolumità di persone fisiche o minaccia di attacco terroristico;
  - Localizzazione o identificazione di persona sospettata di commissione di determinati reati gravi ai fini della conduzione di un'indagine penale;
- Sistemi di IA per effettuare valutazione del rischio della commissione di un reato da parte di una persona fisica, basandosi esclusivamente sul profilo della persona;
- IA usati per creare o ampliare banche dati di riconoscimento facciale attraverso lo scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;
- Sistemi di IA per dedurre le emozioni di una persona sul posto di lavoro e nelle istituzioni scolastiche, tranne che per motivi medici o di sicurezza.

IA AD ALTO RISCHIO

QUALI SONO

Art. 6
Un sistema di IA è considerato ad alto rischio se sono soddisfatte **entrambe le seguenti condizioni:**

(a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un prodotto, coperto dalla legislazione di armonizzazione dell'Unione elencata nell'**Allegato I;**

(a) il prodotto ……, **deve essere sottoposto a una valutazione di conformità d**a parte di terzi in vista dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'Allegato I.

Oltre ai sistemi ad alto rischio di cui al paragrafo 1, **sono considerati ad alto rischio anche i sistemi di IA di cui all'Allegato III.**

ALLEGATO II

LEGISLAZIONE DI ARMONIZZAZIONE DELL'UNIONE BASATA SUL NUOVO QUADRO LEGISLATIVO – allegato I

MDR e IVDR

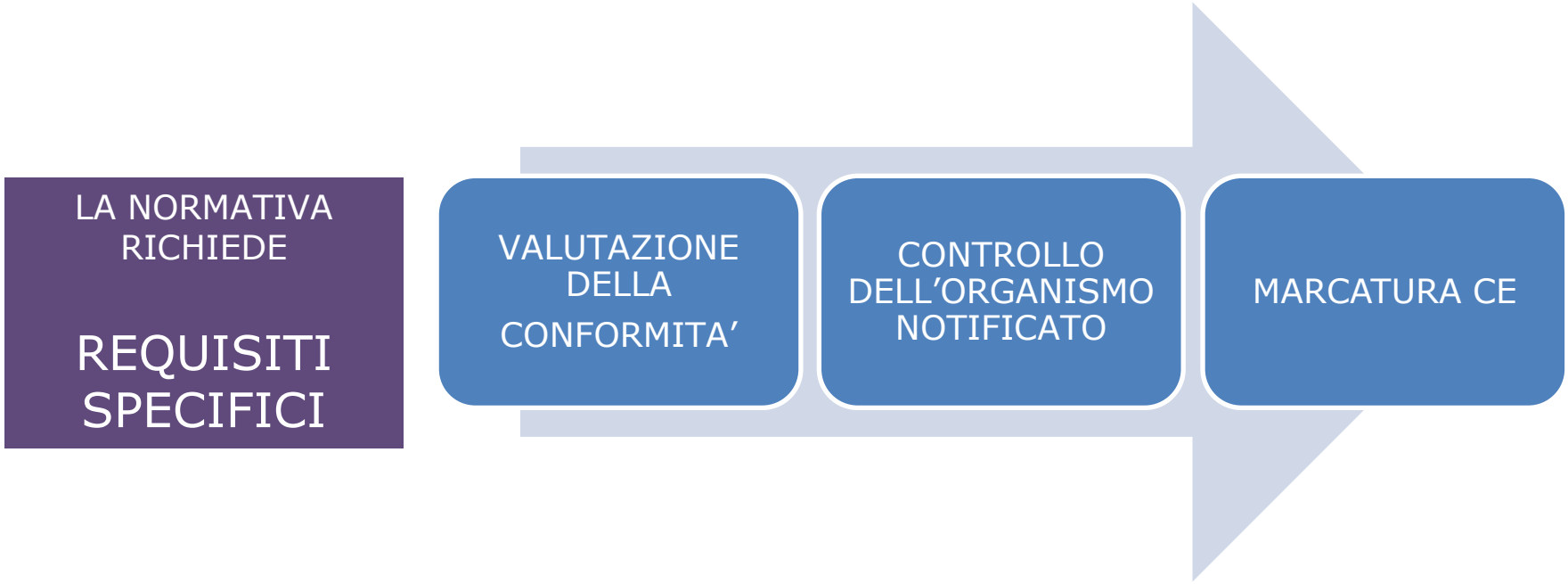
ALLEGATO IIII

1. Biometria (sistemi di identificazione biometrica a distanza; sistemi di IA destinati ad essere utilizzati per la categorizzazione biometrica; sistemi di IA destinati ad essere utilizzati per il riconoscimento delle emozioni);
2. Infrastrutture critiche;
3. Istruzione e formazione professionale;
4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo;
5. Accesso e godimento dei servizi privati essenziali e dei servizi e benefici pubblici (compresa assistenza sanitaria)
6. Applicazione della legge;
7. Gestione della migrazione, asilo e controllo delle frontiere;
8. Amministrazione della giustizia e processi democratici.

IA AD ALTO RISCHIO

QUALE ARCHITETTURA GIURIDICA E' STATA SCELTA?

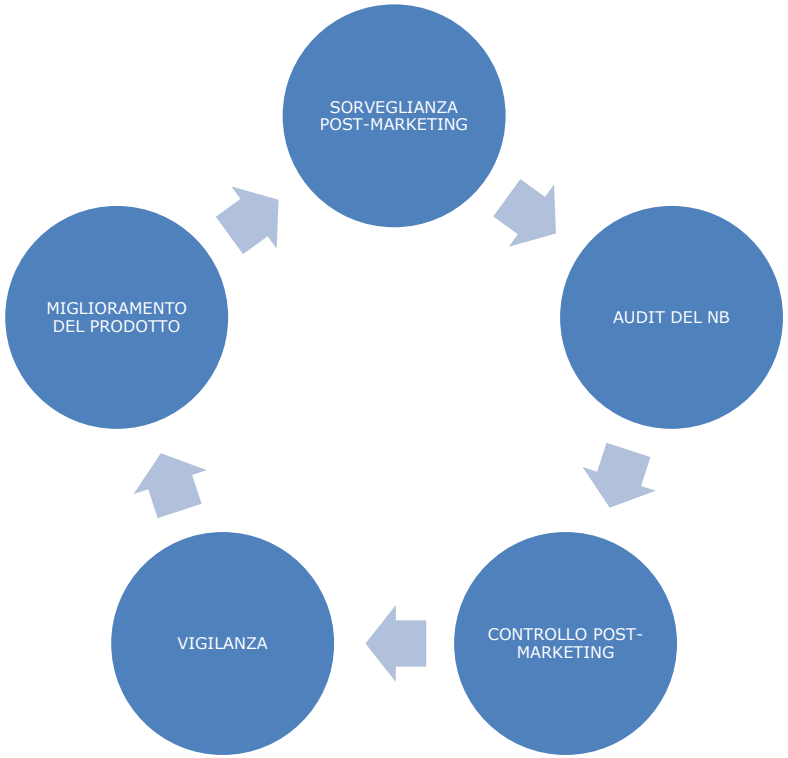
DIRETTIVE DA PRODOTTO
NUOVO QUADRO LEGISLATIVO - 2008



IA AD ALTO RISCHIO

QUALI ARCHITETTURA GIURIDICA E' STATA SCELTA?

DIRETTIVE DA PRODOTTO
NEW LEGISLATIVE FRAMEWORK - 2008



IA AD ALTO RISCHIO

REQUISITI PER I SISTEMI IA AD ALTO RISCHIO (ART. 8-15)

- **Conformità ai requisiti (art. 8)**
- **Sistema di gestione del rischio (art. 9)**
- **Dati e governance dei dati (art. 10)**
- **Documentazione tecnica e tenuta dei registri (art. 11)**
- **Conservazione delle registrazioni (art. 12)**
- **Trasparenza e fornitura di informazioni ai deployer (art. 13)**
- **Sorveglianza umana (art. 14)**
- **Precisione, robustezza e cybersicurezza (ar. 15)**

IA AD ALTO RISCHIO

OBBLIGHI DI FORNITORI E UTILIZZATORI (ART. 16-29a)

- Obblighi dei fornitori (art. 16-21)
- Rappresentanti autorizzati (art. 22)
- Obblighi degli importatori (23)
- Obblighi dei distributori (art. 24)
- Obblighi dei deployer utilizzatori dei sistemi IA ad alto rischio (art. 26)
- Valutazione di impatto sistemi IA ad alto rischio sui diritti fondamentali (art. 27)

LA FIGURA DEL DEPLOYER

Articolo 4

Alfabetizzazione in materia di IA

I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.

ENTRA IN VIGORE IL 2 FEBBRAIO 2025

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

1. I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 3 e 6.

2. I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

5. I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto.

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

6. I deployer di sistemi di IA ad alto rischio conservano i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

11. Fatto salvo l'articolo 50 del presente regolamento i deployer dei sistemi di IA ad alto rischio di cui all'allegato III che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche informano queste ultime che sono soggette all'uso del sistema di IA ad alto rischio.

12. I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad alto rischio ai fini dell'attuazione del presente regolamento.

Articolo 27

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, *……., ……effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre.*

A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti:

a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;

b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;

c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;

d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;

e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;

f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

ALLEGATO III

Accesso e godimento dei servizi privati essenziali e dei servizi e benefici pubblici (compresa assistenza sanitaria)

Articolo 27

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

L'obbligo di cui al paragrafo 1 si applica al primo uso del sistema di IA ad alto rischio.

Il deployer può, in casi analoghi, basarsi su valutazioni d'impatto sui diritti fondamentali effettuate in precedenza o su valutazioni d'impatto esistenti effettuate da un fornitore. Se, durante l'uso del sistema di IA ad alto rischio, ritiene che uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il deployer adotta le misure necessarie per aggiornare le informazioni.

Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati.

ALLEGATO III

Accesso e godimento dei servizi privati essenziali e dei servizi e benefici pubblici (compresa assistenza sanitaria)

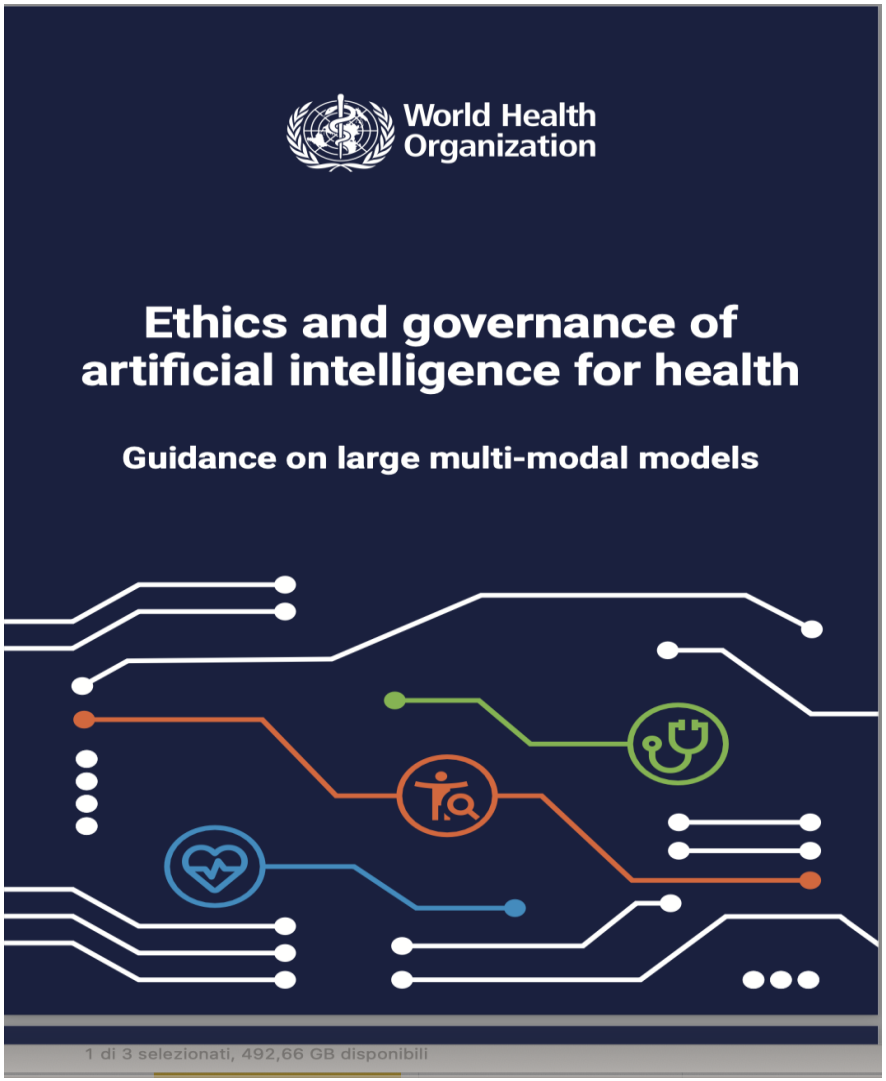
TEMPI ATTUAZIONE

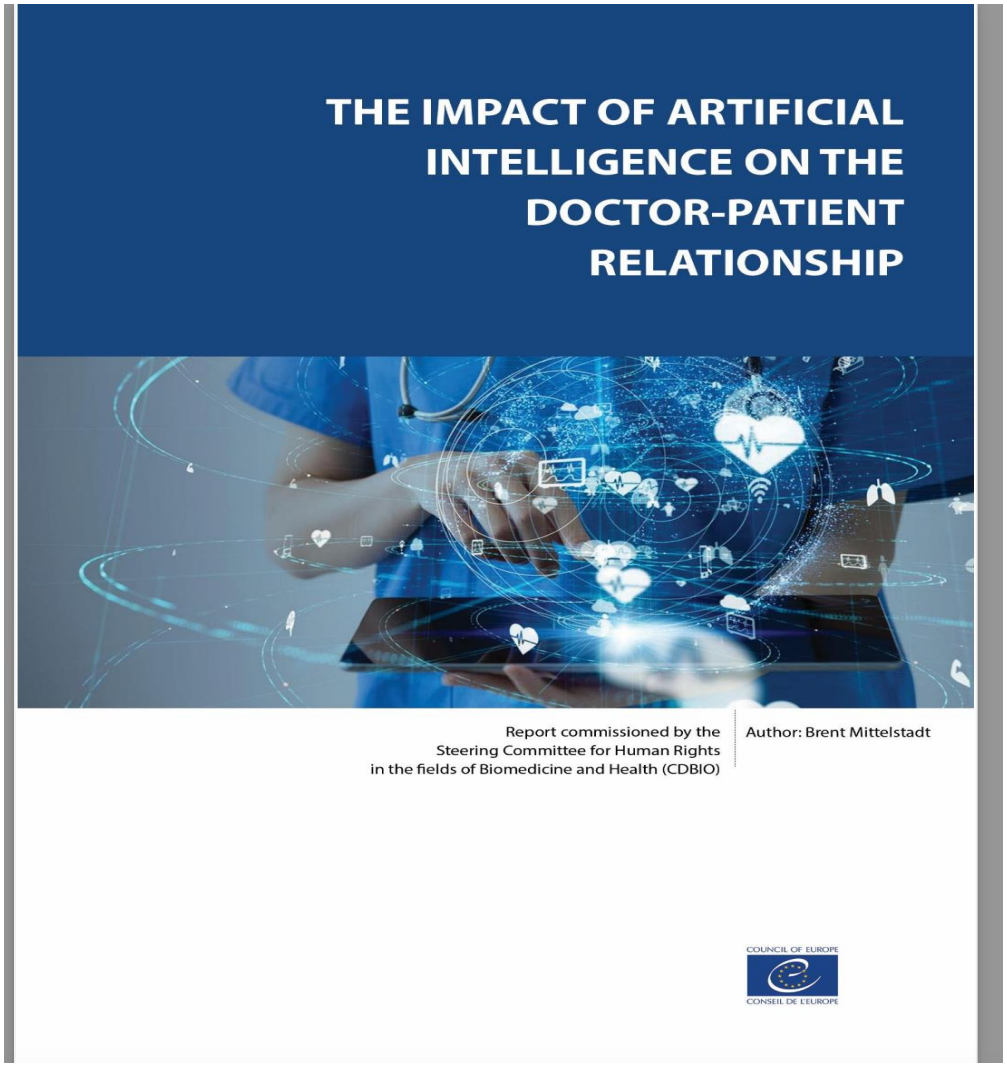
SISTEMI AI ALTO RISCHIO – ALLEGATO III
2 agosto 2026

SISTEMI AI–DISPOSITIVI MEDICI AD ALTO RISCHIO
2 agosto 2027

SISTEMI AI–DISPOSITIVI MEDICI AD ALTO RISCHIO
immessi sul mercato prima del 2 agosto 2026
solo se sono sottoposti a modifiche significative

PER TUTTI
Il termine ultimo è il 2 agosto 2030


World Health Organization
Ethics and governance of artificial intelligence for health
Guidance on large multi-modal models
1 di 3 selezionati, 492,66 GB disponibili


THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE DOCTOR-PATIENT RELATIONSHIP
Report commissioned by the Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO)
Author: Brent Mittelstadt
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

HEALTH AND HEALTHCARE

How generative AI and large language models can close the gap between data and outcomes in healthcare

Jan 9, 2024

Grazie per l'attenzione

avv. Silvia Stefanelli
www.studiolegalestefanelli.it