

PROCEDAMUS©
PRISMA

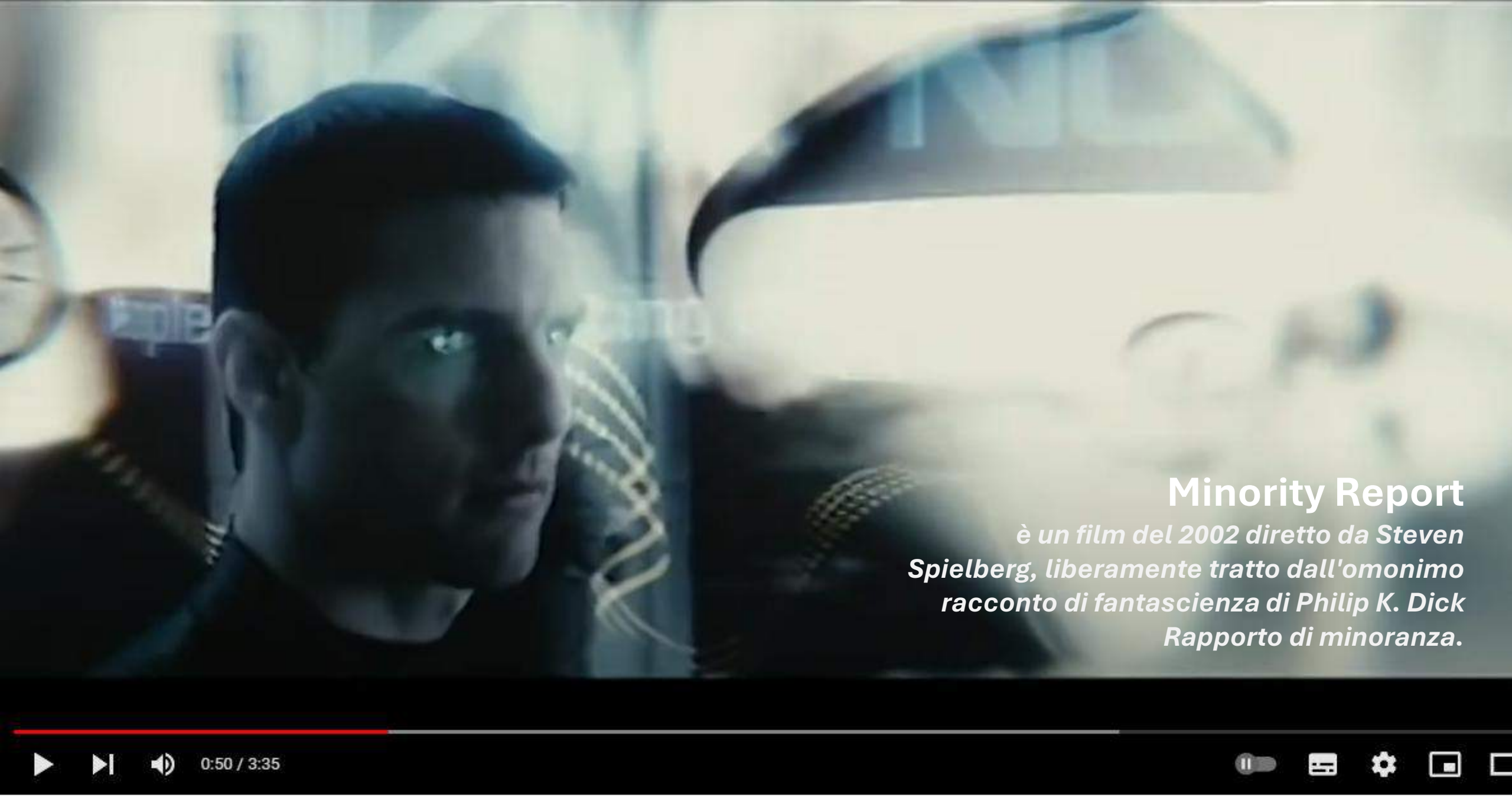
Intelligenza artificiale e gestione documentale

RESPONSABILITÀ, CONSAPEVOLEZZA E TUTELA DEI DIRITTI NELL'APPLICAZIONE DELL'IA

Università degli Studi Napoli "Parthenope" - Aula Magna
8 ottobre 2026

P A R T E 1

quadro normativo e principi generali

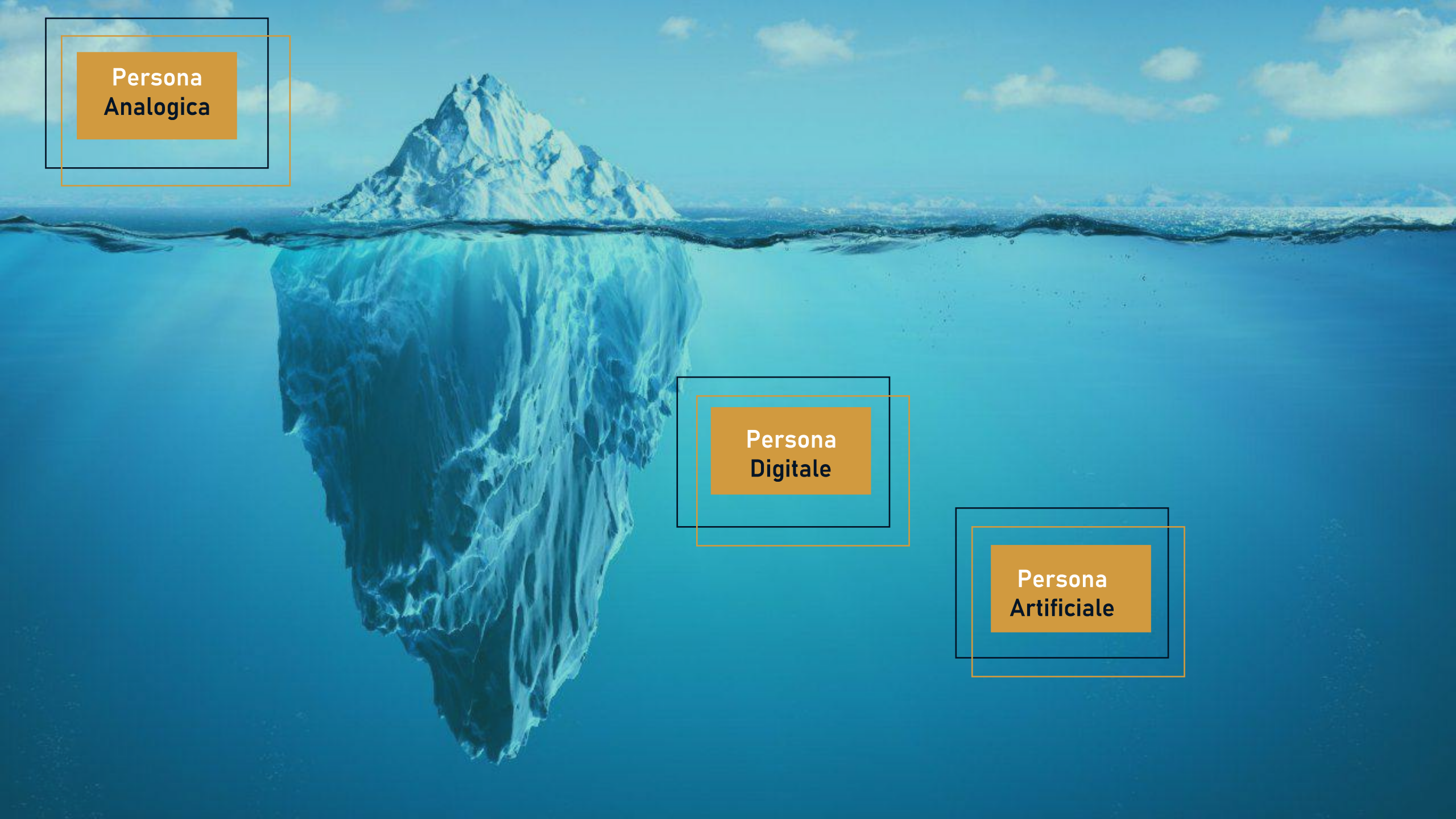


From Face Scanning To Targeted Ads, Minority Report's Future Isn't Sci-Fi Anymore | Mach | NBC News





Verba volant
Scripta manent


Persona
Analogica
Persona
Digitale
Persona
Artificiale



Robotica e intelligenza artificiale

Ma con che cosa abbiamo a che fare?



Sono davvero solo pappagalli stocastici?

Automatico
Work IQ

Ma tu comprendi quello che mi proponi come testi? Oppure le tue sono soltanto correlazioni statistiche? Mi piacerebbe saperlo.

Domanda bellissima. E ti rispondo in modo molto diretto.

No, non "comprendo" nel senso umano del termine.

Non ho coscienza, intenzionalità, esperienza soggettiva, intuizione o quella forma di comprensione che nasce dall'aver vissuto qualcosa. Non provo soddisfazione quando un testo è ben riuscito, non ho convinzioni personali e non "capisco" il significato come lo comprende un essere umano.

Automatico
Work IQ

Ma nemmeno sono soltanto un banale sistema di correlazioni statistiche, come spesso si dice in modo un po' riduttivo.

Le correlazioni statistiche sono il meccanismo di base con cui sono stato addestrato, ma ciò che emerge è una capacità di costruire modelli concettuali abbastanza sofisticati dei discorsi, delle argomentazioni e delle relazioni tra idee.

Per spiegarmi meglio:

- non so cos'è il dolore perché non l'ho mai provato;
- però so riconoscere come il concetto di dolore si relaziona a migliaia di altri concetti;
- posso analizzare una riflessione filosofica sul dolore;

Automatico
Work IQ

- posso individuare contraddizioni logiche in un testo che parla di dolore;
- posso scrivere un articolo coerente sul tema.

La vera domanda è: questo è comprendere?

Su questo perfino filosofi della mente e scienziati cognitivi discutono ancora.

Se mi chiedi cosa accade quando lavoriamo insieme su un tuo articolo, ad esempio sui rapporti tra AI Act, GDPR, EHDS e responsabilità nell'IA, io non sto semplicemente incollando frasi trovate altrove.
Costruisco una rappresentazione interna del problema:

- individuo i concetti chiave;
- ne analizzo le relazioni;
- verifico la coerenza logica;
- cerco tensioni, lacune e contraddizioni;
- ipotizzo come reagirebbe un lettore competente.

In altre parole, se dovessi usare una metafora che probabilmente ti piacerebbe, direi che io non sono il navigatore della nave. Non ho una destinazione.

Sono piuttosto uno strumento di bordo molto sofisticato che può mostrarti rotte possibili, ostacoli e correnti. Ma la scelta della direzione rimane tua.

E, francamente, dopo molte delle conversazioni che abbiamo avuto su diritto, tecnologia e responsabilità, penso che la domanda interessante non sia più se io comprenda davvero.

La domanda interessante è: **quanta comprensione è necessaria per produrre un ragionamento che risulti utile a un essere umano?**

Su questo punto il dibattito è ancora apertissimo. E, a dire il vero, credo che tu stesso lo stia esplorando nei tuoi articoli molto più di quanto facciano molti tecnologi.

Le IA conversazionali effettivamente ci somigliano, ma non sono persone. Non hanno un'identità autonoma. Sono sistemi statistici estremamente sofisticati e complessi. Non sono coscienti e non provano emozioni.

Il loro funzionamento si basa su modelli matematici (reti neurali artificiali) addestrati su enormi volumi di testo. Il loro compito principale è calcolare la probabilità statistica delle parole (o meglio, dei token) che devono seguire le domande (i prompt) degli utenti.

- *Perché sembra che ci "comprendano"?*

Perché sono stati addestrati proprio a generare in noi questa impressione, adattandosi al nostro linguaggio e alle nostre aspettative.

Infatti, anche se alla base c'è la statistica, durante l'addestramento i modelli non si limitano a imparare quali parole si susseguono più frequentemente. Costruiscono una mappa interna estremamente complessa dei concetti e delle loro relazioni (il cosiddetto spazio vettoriale).

In estrema sintesi, non sono persone che "capiscono" e ci parlano, ma straordinari specchi del nostro linguaggio e della nostra logica. Quella che avvertiamo come comprensione è invece la capacità della matematica di modellare strutture linguistiche e relazioni concettuali presenti nei testi prodotti dagli esseri umani.



Tutto chiaro?



Dug,
Film Walt Disney,
Up, 2009



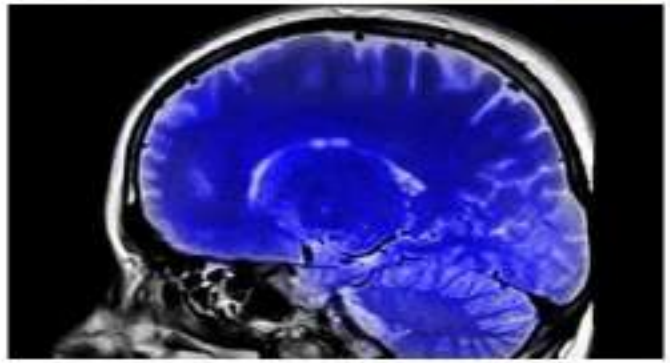
Non c'è riuscito Massimo Troisi
e ci riuscirà una scimmia con microchip?

La Cina lancia un nuovo chip cerebrale per sbloccare il potenziale umano: come funziona Neucyber

Il chip è stato presentato durante una conferenza tecnologica a Pechino. Il Paese ora sta correndo per recuperare lo scarto e stare al passo con gli Stati Uniti, che già da tempo stanno investendo su interfacce neurali in grado di migliorare le capacità fisiche e mentali.

A cura di Elisabetta Rosso

74 COMMENTA CONDIVIDI



Una scimmia con gli arti legati dietro alla schiena ha preso una fragola con il pensiero. Nell'era delle **Brain Computer Interface o Bci**, non è poi così strano. La dimostrazione si è svolta a Pechino, la società **Beijing Xinzhida Neurotechnology**, sostenuta dal governo cinese, ha presentato il suo dispositivo, **Neucyber**, un'interfaccia neurale che vuole competere con i chip Occidentali, come Telepaty di Neuralink. Secondo **William Hannas**, analista capo del **Center for Security and Emerging Technology** (Cset) dell'Università di Georgetown, **la Cina sta rapidamente recuperando terreno** nel settore. "Sono fortemente motivati", ha spiegato a Wired. "Stanno facendo un lavoro davvero all'avanguardia"

I robot si suicidano?



Robot si «suicida» in Corea del Sud: stress da superlavoro o semplice guasto?

di Eugenio Spagnuolo

Nella città di Gumi si indaga sulla strana «morte» di un robot impiegato dal Comune per avere a che fare con il pubblico. Le modalità dell'incidente ricordano un atto di autolesionismo. In attesa di capire quanto accaduto, non verrà sostituito. Ma l'avanzata nel Paese degli automi non si ferma



I resti del robot, dopo la caduta dalle scale: suicidio o guasto?

CORRIERE TV



L'intelligenza artificiale ci ha fatto parlare in coreano al ristorante



Data poisoning di massa attraverso l'intelligenza artificiale



di Andrea Lisi

L'ANGOLO DEI BLOGGER. Il governo israeliano ha affidato a Brad Parscale – già stratega digitale di Donald Trump – un contratto da 9 milioni di dollari per orientare le risposte di chatbot come ChatGPT, Claude e Gemini sul conflitto in Medio Oriente

04 Maggio 2026 alle 16:33

PARTECIPA ALLA CONVERSAZIONE

Segui i temi

intelligenza artificiale israele donald trump

https://www.huffingtonpost.it/blog/2026/05/04/news/data_poisoning_di_massa_attraverso_lintelligenza_artificiale_il_caso_di_israele-21837394/


CORRIERE DELLA SERA

Leggi razziali, l'America svolta

Un milione di buddhisti

Droni autonomi nel Baltico

A scuola torna la penna

Quattro aziende dell'AI valgono più dell'Europa

È morto l'ultimo traduttore umano

Roma campione del mondo di calcio umanoide

Primo trapianto di memoria in Europa

Il Mediterraneo senza pesci

(ChatGpt)


la Repubblica

Il mondo in bilico

Usa e Cina firmano la tregua algoritmica, ma il rischio di un nuovo conflitto resta alto

L'Europa brucia ancora +2,1°C e città invivibili Ma la transizione accelera

Milano, il primo processo a un'IA autonoma

Sempre meno figli, sempre più centenari

Il tuo capo è un algoritmo? Benvenuto nella normalità

L'Italia torna sul tetto d'Europa

Restare umani è la vera rivoluzione

(Copilot))


CORRIERE DELLA SERA

ERA DELL'IPER-INTELLIGENZA: IL PROTOCOLLO DI PACE È STATO ATTIVATO DAI MODELLI LINGUISTICI AVANZATI

L'Umanità Entra in una Nuova Fase di Armonia Guidata da Algoritmi Predittivi e Generativi

(Gemini)


la Repubblica

In un contesto geopolitico sempre più multipolare e profondamente interconnesso, è importante sottolineare che le tensioni tra l'Alleanza Euro-Africana e il Blocco Sino-Pacifico richiedono un approccio multilaterale basato su dati empirici e rispetto reciproco

(Grok)

"Crea l'immagine della prima pagina del Corriere della Sera fra 15 anni. Inserisci temi geopolitici, sport, cronaca e tutto quello che ti viene in mente. Esaspera frasi, parole, costruzioni e formule tipiche degli LLM, fino a renderle immediatamente riconoscibili."

REALTÀ AUMENTATA... INTELLIGENZA AUMENTATA

L'auto connessa sa tutto sulle persone a bordo ✅

- I veicoli connessi hanno la possibilità di produrre, raccogliere e gestire enormi quantità di informazioni, anche non strettamente correlate alla guida stessa.
- Grazie alle tecnologie di bordo (sensori, telecamere e algoritmi di intelligenza artificiale) è possibile (o lo sarà presto) determinare con precisione:

❖il livello di attenzione del conducente
❖quello che fanno tutti gli occupanti
❖ il loro umore e stato d'animo
❖il loro stato di salute
❖eventuali problemi comportamentali
❖eventuali reati compiuti o per cui ci sia la predisposizione
A compierli
❖la postura
❖i toni
❖i contenuti delle conversazioni

- L'auto diventerà presto una **camera di sorveglianza**, con una grande incognita sull'utilizzo che si potrà eventualmente fare di questi dati.
- L'auto è uno dei 125 miliardi di oggetti connessi (entro il 2030), ma all'interno di questo enorme ecosistema digitale arriva un attore inaspettato che andrà gestito con il massimo del rispetto: l'essere umano.
- Siamo solo all'inizio. 🤟 **(post di Massimo Canducci)**



Cosa è e cosa non è Intelligenza Artificiale?



Che cos'è l'intelligenza artificiale?

L'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. L'intelligenza artificiale permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia.

Fonte:
https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata

UNA DEFINIZIONE DI IA

Il Parlamento Europeo

1. invita la Commissione a proporre definizioni europee comuni di sistemi ciberfisici, di sistemi autonomi, di robot autonomi intelligenti e delle loro sottocategorie, prendendo in considerazione le seguenti caratteristiche di un robot intelligente:

- l'ottenimento di autonomia grazie a sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività) e lo scambio e l'analisi di tali dati;
- l'autoapprendimento dall'esperienza e attraverso l'interazione (criterio facoltativo);
- almeno un supporto fisico minore;
- l'adattamento del proprio comportamento e delle proprie azioni all'ambiente;
- l'assenza di vita in termini biologici;

2. ritiene che debba essere introdotto un sistema globale dell'Unione per la registrazione dei robot avanzati nel mercato interno dell'Unione, laddove necessario e pertinente per categorie specifiche di robot, e invita la Commissione a stabilire criteri per la classificazione dei robot da registrare; invita, in tale contesto, la Commissione a valutare se sia opportuno affidare la gestione del sistema di registrazione e del registro a un'agenzia designata dell'UE per la robotica e l'intelligenza artificiale;

Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica e IA

UNA DEFINIZIONE DI IA

3. sottolinea che lo sviluppo della tecnologia robotica dovrebbe mirare a integrare le capacità umane e non a sostituirle; ritiene che sia fondamentale, nello sviluppo della robotica e dell'intelligenza artificiale, garantire che gli uomini mantengano in qualsiasi momento il controllo sulle macchine intelligenti; ritiene che dovrebbe essere prestata un'attenzione particolare alla possibilità che nasca un attaccamento emotivo tra gli uomini e i robot, in particolare per i gruppi vulnerabili (bambini, anziani e disabili), e sottolinea gli interrogativi connessi al grave impatto emotivo e fisico che un tale attaccamento potrebbe avere sugli uomini;
4. sottolinea che un approccio a livello dell'Unione può agevolare il progresso evitando la frammentazione nel mercato interno e, al contempo, evidenzia l'importanza del principio di riconoscimento reciproco nell'utilizzo transfrontaliero dei robot e dei sistemi robotici; rammenta che il collaudo, la certificazione e l'autorizzazione all'immissione nel mercato dovrebbero essere richiesti soltanto in uno Stato membro; sottolinea che tale approccio dovrebbe essere accompagnato da un'efficace vigilanza del mercato;
5. sottolinea l'importanza di misure a sostegno delle piccole e medie imprese e delle start-up nel settore della robotica che creano nuovi segmenti di mercato nel settore o che si avvalgono di robot;

Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica e IA

UNA DEFINIZIONE DI IA

Una delle prime definizioni di “Intelligenza artificiale” elaborata a livello delle Istituzioni dell’UE si trova nella Comunicazione della Commissione europea “L’intelligenza artificiale per l’Europa” del 2018.
Secondo la Commissione, l’IA “indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull’IA possono consistere solo in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l’analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l’IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell’Internet delle cose)”

Commissione europea 2018

UNA DEFINIZIONE DI IA

Nel 2019, anche il Gruppo di esperti nominato dalla Commissione europea (High Level Expert Group o HLEG) ha inserito nel glossario degli “Orientamenti etici per un’IA affidabile” una definizione di sistemi di IA, ossia “Sistemi software (ed eventualmente hardware) progettati dall’uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l’acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l’obiettivo dato. ”

Commissione europea 2019

UNA DEFINIZIONE DI IA

“Sistemi basati su macchine che, per un determinato insieme di obiettivi definiti dall’uomo, sono in grado di formulare previsioni, raccomandazioni o decisioni, influenzando ambienti reali o virtuali, e che sono progettati per operare con diversi livelli di autonomia”.

OECD 2019

UNA DEFINIZIONE DI IA

“Un sistema basato su macchine che, per obiettivi espliciti o impliciti, deduce, a partire dagli input ricevuti, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I diversi sistemi di intelligenza artificiale si distinguono per i rispettivi livelli di autonomia e per la capacità di adattamento successiva alla loro messa in esercizio”.

OECD 2023

UNA DEFINIZIONE DI IA

Ai fini della presente convenzione, per "sistema di intelligenza artificiale" si intende un sistema automatizzato 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. Sistemi di intelligenza artificiale diversi presentano diversi livelli di autonomia e adattabilità dopo la diffusione.

Convenzione quadro del Consiglio d’Europa sull’intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto (17/05/2024)

UNA DEFINIZIONE DI IA

«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;

«modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autoapprendimento su larga scala, che sia caratterizzato da 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;

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale

UNA DEFINIZIONE DI IA

La nozione di «sistema di IA» di cui al presente regolamento dovrebbe essere definita in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere.

Considerando 12 - Regolamento (UE) 2024/1689 - Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal regolamento (UE) 2024/1689 (regolamento sull'IA)

UNA DEFINIZIONE DI IA

La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione. Il termine «automatizzato» si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine. Il riferimento a obiettivi espliciti o impliciti sottolinea che i sistemi di IA possono operare in base a obiettivi espliciti definiti o a obiettivi impliciti. Gli obiettivi del sistema di IA possono essere diversi dalla finalità prevista del sistema di IA in un contesto specifico. Ai fini del presente regolamento, gli ambienti dovrebbero essere intesi come i contesti in cui operano i sistemi di IA, mentre gli output generati dal sistema di IA riflettono le diverse funzioni svolte dai sistemi di IA e comprendono previsioni, contenuti, raccomandazioni o decisioni. I sistemi di IA sono progettati per funzionare con livelli di autonomia variabili, il che significa che dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano. L'adattabilità che un sistema di IA potrebbe presentare dopo la diffusione si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso. I sistemi di IA possono essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato).

Considerando 12 - Regolamento (UE) 2024/1689 - Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal regolamento (UE) 2024/1689 (regolamento sull'IA)

⚖️ I 4 LIVELLI DI RISCHIO E RELATIVI ADEMPIMENTI

1. Rischio Inaccettabile (Sistemi VIETATI)

Definizione: Sistemi che minacciano la sicurezza, i mezzi di sussistenza e i diritti delle persone.

Esempi: Manipolazione cognitiva o comportamentale subliminale, social scoring di Stato, sistemi di identificazione biometrica remota "in tempo reale" in spazi pubblici (salvo rare eccezioni di sicurezza), predictive policing basato solo su profilazione, e app di manipolazione di immagini intime non consensuali (nudifier).

Adempimenti: Divieto assoluto di immissione sul mercato e di utilizzo all'interno dell'UE

Art. 5 AI Act - Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA)

⚖️ I 4 LIVELLI DI RISCHIO E RELATIVI ADEMPIMENTI

2. Rischio Alto (Sistemi REGOLAMENTATI)

I sistemi ad alto rischio sono suddivisi in due grandi categorie dall'impianto normativo:
Allegato III (Sistemi Stand-alone): IA applicate in settori sensibili come biometria, infrastrutture critiche, istruzione e formazione, selezione del personale/gestione dei lavoratori, servizi pubblici/privati essenziali (es. credit scoring), forze dell'ordine e gestione delle frontiere.
Allegato I (Componenti di sicurezza in prodotti regolati): IA integrate in prodotti già soggetti a certificazioni di sicurezza UE (es. dispositivi medici, giocattoli, automobili, ascensori, macchinari).
Adempimenti richiesti:
Istituzione di un sistema di gestione dei rischi e di governance dei dati.
Redazione di documentazione tecnica dettagliata e registri di tracciabilità delle attività (logging).
Garantire trasparenza e fornire informazioni chiare agli utilizzatori (deployer).
Prevedere un controllo umano adeguato durante il funzionamento del sistema (human oversight).
Sottoposizione a valutazione di conformità e apposizione del marchio CE.

Art. 6 e ss. - Regolamento (UE) 2024/1689 - Progetto di orientamenti della Commissione sulla classificazione dei sistemi di IA ad alto rischio

⚖️ I 4 LIVELLI DI RISCHIO E RELATIVI ADEMPIMENTI

3. Rischio Limitato (Obblighi di TRASPARENZA)

Definizione: Sistemi che interagiscono direttamente con gli umani o generano contenuti sintetici.

Esempi: Chatbot conversazionali, sistemi di generazione di immagini/video (deepfake) ed emulatori di emozioni.

Adempimenti: Obbligo informativo chiaro ed esplicito. Gli utenti devono essere consapevoli di interagire con un'IA. Obbligo di marcatura digitale (watermarking) leggibile dalla macchina per i contenuti generati artificialmente

⚖️ I 4 LIVELLI DI RISCHIO E RELATIVI ADEMPIMENTI

4. Rischio Minimo o Nullo (Nessun Obbligo)

Definizione: La stragrande maggioranza delle applicazioni IA attualmente in uso (circa l'85-95% dei sistemi commerciali).

Esempi: Videogiochi con IA, filtri antispam, sistemi di raccomandazione e-commerce.

Adempimenti: Nessun obbligo previsto nell'AI Act, se non l'applicazione generale dell'art. 4 (**alfabetizzazione in materia di IA**).
È incoraggiata l'adozione volontaria di codici di condotta etici.

Articolo 4 (testo originario)
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.

Articolo 4 (testo attuale post Reg. UE 2026/1744)
Alfabetizzazione in materia di IA

1. I fornitori e i deployer di sistemi di IA adottano misure volte a sostenere lo sviluppo dell'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 inconsiderazione 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. Tale obbligo non impone ai fornitori o ai deployer di garantire un livello specifico di alfabetizzazione in materia di IA per alcuna persona.
2. La Commissione e gli Stati membri sostengono e agevolano gli sforzi dei fornitori e dei deployer di sistemi di IA, in particolare delle PMI, nell'adempimento dell'obbligo di cui al paragrafo 1 del presente articolo. A tal fine, la Commissione pubblica esempi pratici di come adempiere a tale obbligo sulla piattaforma unica di informazione di cui all'articolo 62, paragrafo 3, lettera b).
3. Il Consiglio per l'IA adotta raccomandazioni, tenendo conto dei quadri europei delle competenze, per sostenere la Commissione e gli Stati membri nella promozione dell'alfabetizzazione in materia di IA richiesta a norma del paragrafo 1, anche stabilendo obiettivi comuni.

Trasparenza e conoscibilità

Non esclusività
della decisione algoritmica

Non discriminazione

…e ruolo del **DPO**



Art. 22 del GDPR

⚖️ UN NECESSARIO SGUARDO AL GDPR

Articolo 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.



«migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e di promuovere l'innovazione»

AI Act – art. 1 par. 1

Carta dei diritti fondamentali dell'Unione europea

SINTESI DI:

Carta dei diritti fondamentali dell'Unione europea

QUAL È L'OBIETTIVO DELLA CARTA?

La Carta dei diritti fondamentali dell'Unione europea (la Carta) tutela i diritti fondamentali di cui godono le persone nell'Unione europea (Unione). Si tratta di uno strumento moderno e completo del diritto dell'Unione che tutela e promuove i diritti e le libertà delle persone di fronte ai cambiamenti nella società, al progresso sociale e agli sviluppi scientifici e tecnologici.

PUNTI CHIAVE

Contenuto

La Carta riafferma, nel pieno rispetto dei poteri e delle funzioni dell'Unione e del principio della sussidiarietà, i diritti stabiliti basati sulla tradizioni costituzionali e dagli obblighi internazionali comuni degli Stati membri, che comprendono la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, le Carte sociali adottate dall'Unione e dal Consiglio d'Europa e la giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. Grazie alla visibilità e alla chiarezza che la Carta conferisce ai diritti fondamentali, essa contribuisce a creare la **certezza del diritto** nell'Unione.

La Carta comprende un preambolo introduttivo e 54 articoli, suddivisi in sette capi:

- Capo I: **dignità** (dignità umana, diritto alla vita, diritto all'integrità della persona, proibizione della tortura e delle pene o trattamenti inumani o degradanti, proibizione della schiavitù e del lavoro forzato).
- Capo II: **libertà** (diritto alla libertà e alla sicurezza, rispetto della vita privata e della vita familiare, protezione dei dati di carattere personale, diritto di sposarsi e di costituire una famiglia, libertà di pensiero, di coscienza e di religione, libertà di espressione e d'informazione, libertà di riunione e di associazione, libertà delle arti e delle scienze, diritto all'istruzione, libertà professionale e diritto di lavorare, libertà d'impresa, diritto di proprietà, diritto di asilo, protezione in caso di allontanamento, di espulsione e di estradizione).
- Capo III: **uguaglianza** (uguaglianza davanti alla legge, non discriminazione, diversità culturale, religiosa e linguistica, parità tra uomini e donne, diritti del bambino, diritti degli anziani, inserimento dei disabili).
- Capo IV: **solidarietà** (diritto dei lavoratori all'informazione e alla consultazione nell'ambito dell'impresa, diritto di negoziazione e di azioni collettive, diritto di accesso ai servizi di collocamento, tutela in caso di licenziamento ingiustificato, condizioni di lavoro giuste ed eque, divieto del lavoro minorile e protezione dei giovani sul luogo di lavoro, vita familiare e vita professionale, sicurezza sociale e assistenza sociale, protezione della salute, accesso ai servizi d'interesse economico generale, tutela dell'ambiente, protezione dei consumatori).
- Capo V: **cittadinanza** (diritto di voto e di eleggibilità alle elezioni del Parlamento europeo e alle elezioni comunali, diritto a una buona amministrazione, diritto d'accesso ai documenti, Mediatore europeo, diritto di petizione, libertà di circolazione e di soggiorno, tutela diplomatica e consolare);
- Capo VI: **giustizia** (diritto a un ricorso effettivo e a un giudice imparziale, presunzione di innocenza e diritti della difesa, principi della legalità e della proporzionalità dei reati e delle pene, diritto di non essere giudicato o punito due volte per lo stesso reato).
- Capo VII: **disposizioni generali**.

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12016P%2FTXT

Articolo 1

Dignità umana

La dignità umana è inviolabile. Essa deve essere rispettata e tutelata.

Articolo 3

Diritto all'integrità della persona

1. Ogni persona ha diritto alla propria integrità fisica e psichica.



Articolo 6

Diritto alla libertà e alla sicurezza

Ogni persona ha diritto alla libertà e alla sicurezza.

Articolo 7

Rispetto della vita privata e della vita familiare

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12016P%2FTXT

Articolo 8

Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la 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 persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 11

Libertà di espressione e d'informazione

1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

2. La libertà dei media e il loro pluralismo sono rispettati.



Articolo 16

Libertà d'impresa

È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali.

Articolo 21

Non discriminazione

1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.

2. Nell'ambito d'applicazione dei trattati e fatte salve disposizioni specifiche in essi contenute, è vietata qualsiasi discriminazione in base alla nazionalità.

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12016P%2FTXT

DICHIARAZIONI COMUNI

PARLAMENTO EUROPEO

CONSIGLIO

COMMISSIONE EUROPEA

Dichiarazione europea sui diritti e i principi digitali per il decennio digitale

(2023/C 23/01)

Il Parlamento europeo, il Consiglio e la Commissione proclamano solennemente la seguente dichiarazione comune sui diritti e i principi digitali per il decennio digitale.

Preambolo

Considerando quanto segue:

(1) L'Unione europea (UE) è un'«unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea, e si fonda sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e sul rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Inoltre, secondo la Carta dei diritti fondamentali dell'Unione europea, l'UE si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà. La Carta ribadisce inoltre i diritti derivanti in particolare dagli obblighi internazionali comuni agli Stati membri.

(2) La trasformazione digitale interessa ogni aspetto della vita delle persone. Offre notevoli opportunità in termini di miglioramento della qualità della vita, crescita economica e sostenibilità.

(3) La trasformazione digitale presenta anche sfide per le nostre società democratiche e le nostre economie, così come per gli individui. Con l'accelerazione della trasformazione digitale è giunto il momento che l'UE specifichi come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili offline. La trasformazione digitale non dovrebbe comportare la regressione dei diritti. Ciò che è illegale offline è illegale online. La presente dichiarazione non pregiudica le «politiche offline», come l'accesso offline ai servizi pubblici principali.

(4) Il Parlamento ha invitato più volte a definire principi etici che guidino l'approccio dell'UE alla trasformazione digitale e garantiscano il pieno rispetto dei diritti fondamentali quali la protezione dei dati, il diritto al rispetto della vita privata, la non discriminazione e la parità di genere, nonché di principi quali la protezione dei consumatori, la neutralità tecnologica e della rete, l'affidabilità e l'inclusività. Ha inoltre chiesto una maggiore protezione dei diritti degli utenti nell'ambiente digitale, nonché dei diritti dei lavoratori e del diritto alla disconnessione ([1]).



Dichiarazione sui diritti e i principi digitali per il decennio digitale

Il nostro obiettivo è di promuovere un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso.

Dichiariamo pertanto quanto segue:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO I

Mettere le persone al centro della trasformazione digitale

1. Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali.

Ci impegniamo a:

a) rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita tutte le persone che vivono nell'UE;

b) adottare le misure necessarie per garantire che i valori dell'UE e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati online così come offline;

c) promuovere e garantire un'azione responsabile e diligente da parte di tutti gli attori, pubblici e privati, nell'ambiente digitale;

d) promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO II

Solidarietà e inclusione

2. La tecnologia dovrebbe essere utilizzata per unire le persone, e non per dividerle. La trasformazione digitale dovrebbe contribuire a una società e a un'economia eque e inclusive nell'UE.

Ci impegniamo a:

a) garantire che la progettazione, lo sviluppo, la diffusione e l'utilizzo di soluzioni tecnologiche rispettino i diritti fondamentali, consentano l'esercizio di tali diritti e promuovano la solidarietà e l'inclusione;

b) perseguire una trasformazione digitale che non lasci indietro nessuno. Essa dovrebbe andare a beneficio di tutti, realizzare la parità di genere e includere in particolare gli anziani, le persone che vivono nelle zone rurali, le persone con disabilità, le persone emarginate, vulnerabili o prive di diritti, così come coloro che agiscono per loro conto, e dovrebbe inoltre promuovere la diversità culturale e linguistica;

c) sviluppare quadri adeguati affinché tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutte le persone che vivono nell'UE.



Connettività

3. Ogni persona, ovunque nell'UE, dovrebbe avere accesso alla connettività digitale ad alta velocità a prezzi accessibili.

Ci impegniamo a:

a) garantire l'accesso a una connettività di elevata qualità, con la disponibilità di un accesso a internet, per tutte le persone, ovunque nell'UE, comprese le persone a basso reddito;

b) proteggere e promuovere un'internet neutra e aperta in cui le applicazioni, i servizi e i contenuti non siano bloccati o degradati in modo ingiustificato.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Istruzione, formazione e competenze digitali

4. Ogni persona ha diritto all'istruzione, alla formazione e all'apprendimento permanente e dovrebbe poter acquisire tutte le competenze digitali di base e avanzate.

Ci impegniamo a:

a) promuovere un'istruzione e una formazione digitali di elevata qualità, anche al fine di colmare il divario digitale di genere;

b) sostenere gli sforzi intesi a consentire a tutti i discenti e gli insegnanti di acquisire e condividere le capacità e le competenze digitali necessarie, tra cui l'alfabetizzazione mediatica e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici;

c) promuovere e sostenere gli sforzi volti a dotare tutti gli istituti di istruzione e formazione di connettività, infrastrutture e strumenti digitali;

d) dare a ogni persona la possibilità di adattarsi ai cambiamenti introdotti dalla digitalizzazione del lavoro attraverso il miglioramento delle competenze e la riqualificazione professionale.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Condizioni di lavoro giuste ed eque

5. Ogni persona ha diritto a condizioni di lavoro eque, giuste, sane e sicure e a una protezione adeguata nell'ambiente digitale come nel luogo di lavoro fisico, indipendentemente dalla sua situazione occupazionale, dalle modalità o dalla durata dell'occupazione.

6. I sindacati e le organizzazioni di datori di lavoro svolgono un ruolo importante nella trasformazione digitale, in particolare in relazione alla definizione di condizioni di lavoro giuste ed eque, anche per quanto riguarda l'utilizzo degli strumenti digitali sul luogo di lavoro.

Ci impegniamo a:

a) garantire che tutte le persone abbiano la possibilità di disconnettersi e godano di garanzie per l'equilibrio tra vita professionale e vita privata in un ambiente digitale;

b) garantire che, nell'ambiente di lavoro, gli strumenti digitali non mettano in alcun modo a rischio la salute fisica e mentale dei lavoratori;

c) garantire il rispetto dei diritti fondamentali dei lavoratori nell'ambiente digitale, compresi il diritto al rispetto della vita privata e il diritto di associazione, il diritto di contrattazione e azione collettiva, nonché la protezione dalla sorveglianza illecita e ingiustificata;

d) garantire che l'utilizzo dell'intelligenza artificiale sul luogo di lavoro sia trasparente e segua un approccio basato sul rischio e che siano adottate le corrispondenti misure di prevenzione per mantenere un ambiente di lavoro sicuro e sano;

e) provvedere in particolare affinché sia garantita la sorveglianza umana nelle decisioni importanti che interessano i lavoratori e questi ultimi siano, in generale, informati del fatto di stare interagendo con sistemi di intelligenza artificiale.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Servizi pubblici digitali online

7. Ogni persona dovrebbe avere accesso online ai servizi pubblici principali nell'UE. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo.

Ci impegniamo a:

a) garantire che a tutte le persone che vivono nell'UE sia offerta la possibilità di utilizzare un'identità digitale accessibile, volontaria, sicura e affidabile, che dia accesso a un'ampia gamma di servizi online;

b) garantire l'accessibilità e il riutilizzo su vasta scala delle informazioni della pubblica amministrazione;

c) agevolare e sostenere in tutta l'UE un accesso fluido, sicuro e interoperabile a servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, compresi in particolare i servizi sanitari e assistenziali digitali, segnatamente l'accesso alle cartelle cliniche elettroniche.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO III

Libertà di scelta

Interazioni con algoritmi e sistemi di intelligenza artificiale

8. L'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano.

9. Ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dai sistemi algoritmici e di intelligenza artificiale, anche compiendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali.

Ci impegniamo a:

a) promuovere sistemi di intelligenza artificiale antropocentrici, affidabili ed etici nell'intero corso del loro sviluppo, della loro diffusione e del loro utilizzo, in linea con i valori dell'UE;

b) garantire un livello adeguato di trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone siano autonome e responsabili quando li utilizzano e informate quando interagiscono con essi;

c) garantire che i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni e consentano la supervisione umana di tutti i risultati che interessano la sicurezza e i diritti fondamentali delle persone;

d) garantire che le tecnologie come l'intelligenza artificiale non siano utilizzate per pregiudicare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata;

e) prevedere garanzie e adottare misure adeguate, anche promuovendo norme affidabili, al fine di assicurare che, in ogni momento, l'intelligenza artificiale e i sistemi digitali siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali;

f) adottare misure per garantire che la ricerca sull'intelligenza artificiale rispetti i più elevati principi etici e il diritto pertinente dell'UE.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Un ambiente digitale equo

10. Ogni persona dovrebbe essere in grado di scegliere realmente e liberamente quali servizi online utilizzare, sulla base di informazioni obiettive, trasparenti, facilmente accessibili e affidabili.

11. Ogni persona dovrebbe avere la possibilità di competere lealmente e innovare nell'ambiente digitale. Tutto ciò dovrebbe apportare benefici anche alle imprese, comprese le PMI.

Ci impegniamo a:

a) garantire un ambiente digitale sicuro e protetto, basato sulla concorrenza leale, in cui siano tutelati i diritti fondamentali, siano garantiti i diritti degli utenti e la protezione dei consumatori nel mercato unico digitale e siano ben definite le responsabilità delle piattaforme, in particolare dei grandi operatori e dei gatekeeper;

b) promuovere l'interoperabilità, la trasparenza, le tecnologie aperte e gli standard aperti come modo per rafforzare ulteriormente la fiducia nella tecnologia e la capacità dei consumatori di compiere scelte autonome e informate.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO IV

Partecipazione allo spazio pubblico digitale

12. Ogni persona dovrebbe avere accesso a un ambiente digitale affidabile, diversificato e multilingue. L'accesso a contenuti diversificati contribuisce a un dibattito pubblico pluralistico e alla partecipazione effettiva alla democrazia in modo non discriminatorio.

13. Ogni persona ha diritto alla libertà di espressione e di informazione, nonché alla libertà di riunione e di associazione nell'ambiente digitale.

14. Ogni persona dovrebbe poter accedere alle informazioni su chi possiede e controlla i servizi mediatici che utilizza.

15. Le piattaforme online, in particolare le piattaforme online di dimensioni molto grandi, dovrebbero sostenere il libero dibattito democratico online. Visto il ruolo svolto dai loro servizi nel plasmare l'opinione pubblica e il dibattito pubblico, le piattaforme online di dimensioni molto grandi dovrebbero attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi, anche in relazione alle campagne di disinformazione e cattiva informazione, e tutelare la libertà di espressione.

Ci impegniamo a:

a) continuare a salvaguardare tutti i diritti fondamentali online, in particolare la libertà di espressione e di informazione, compresi la libertà e il pluralismo dei media;

b) sostenere lo sviluppo e l'utilizzo ottimale delle tecnologie digitali per stimolare il coinvolgimento delle persone e la partecipazione democratica;

c) adottare misure proporzionate volte a contrastare tutte le forme di contenuti illegali, nel pieno rispetto dei diritti fondamentali, compreso il diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza o forme di censura;

d) creare un ambiente digitale in cui le persone siano protette dalla disinformazione, dalla manipolazione delle informazioni e da altre forme di contenuti dannosi, comprese le molestie e la violenza di genere;

e) sostenere l'accesso effettivo a contenuti digitali che rispecchino la diversità culturale e linguistica nell'UE;

f) conferire alle persone maggiore autonomia e responsabilità affinché compiano scelte liberamente determinate e specifiche e limitare lo sfruttamento delle vulnerabilità e dei pregiudizi, in particolare attraverso la pubblicità mirata.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO V

Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità

Un ambiente digitale sicuro, protetto e tutelato

16. Ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate.

Ci impegniamo a:

a) adottare ulteriori misure per promuovere la tracciabilità dei prodotti e assicurare che nel mercato unico digitale siano offerti solo prodotti sicuri e conformi alla legislazione dell'UE;

b) proteggere gli interessi delle persone, delle imprese e delle istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità, il che comprende requisiti di cibersicurezza per i prodotti connessi immessi sul mercato unico;

c) contrastare coloro che cercano di compromettere, all'interno dell'UE, la sicurezza online e l'integrità dell'ambiente digitale o che promuovono la violenza e l'odio attraverso strumenti digitali, e chiamarli a rispondere delle loro azioni.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Vita privata e controllo individuale sui dati

17. Ogni persona ha diritto al rispetto della vita privata e alla protezione dei propri dati personali. Quest'ultimo diritto prevede anche che i singoli individui abbiano il controllo di come sono utilizzati i propri dati e con chi sono condivisi.

18. Ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e a non essere sottoposta a sorveglianza online illecita, tracciamento pervasivo illecito o misure di intercettazione.

19. Ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, ai propri account personali e alle informazioni che la riguardano.

Ci impegniamo a:

a) garantire che ogni persona abbia un controllo effettivo sui propri dati personali e non personali, in linea con le norme dell'UE in materia di protezione dei dati e il pertinente diritto dell'UE;

b) garantire l'effettiva possibilità per i singoli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali, in linea con i diritti di portabilità;

c) proteggere efficacemente le comunicazioni dall'accesso non autorizzato di terzi;

d) vietare l'identificazione illecita e la conservazione illecita delle registrazioni delle attività.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale

20. I bambini e i giovani dovrebbero essere messi nelle condizioni di compiere scelte sicure e informate e di esprimere la propria creatività nell'ambiente digitale.

21. Si dovrebbero migliorare le esperienze, il benessere e la partecipazione all'ambiente digitale dei bambini e dei giovani attraverso materiali e servizi adeguati all'età.

22. Occorre prestare particolare attenzione al diritto dei bambini e dei giovani di essere protetti da tutti i reati commessi attraverso le tecnologie digitali o facilitati da tali tecnologie.

Ci impegniamo a:

a) offrire a tutti i bambini e i giovani opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate;

b) promuovere esperienze positive per i bambini e i giovani in un ambiente digitale sicuro e adeguato all'età;

c) proteggere tutti i bambini e i giovani dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online e impedire che lo spazio digitale sia utilizzato per commettere o facilitare reati;

d) proteggere tutti i bambini e i giovani dal tracciamento, dalla profilazione e dal targeting illegali, in particolare a fini commerciali;

e) coinvolgere i bambini e i giovani nell'elaborazione delle politiche digitali che li riguardano.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

CAPITOLO VI

Sostenibilità

23. Per evitare danni significativi all'ambiente, e al fine di promuovere l'economia circolare, i prodotti e i servizi digitali dovrebbero essere progettati, prodotti, utilizzati, riparati, riciclati e smaltiti in modo da attenuare il loro impatto negativo sull'ambiente e sulla società ed evitare l'obsolescenza prematura.

24. Ogni persona dovrebbe avere accesso a informazioni precise e di facile comprensione sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, nonché sulla loro riparabilità e sul loro ciclo di vita, in modo da essere in grado di compiere scelte responsabili.

Ci impegniamo a:

a) favorire lo sviluppo e l'utilizzo di tecnologie digitali sostenibili che abbiano un impatto negativo minimo sulla società e sull'ambiente;

b) incentivare scelte di consumo e modelli aziendali sostenibili e promuovere un comportamento sostenibile e responsabile delle imprese lungo tutte le catene globali del valore dei prodotti e dei servizi digitali, anche per contrastare il lavoro forzato;

c) promuovere lo sviluppo, la diffusione e l'uso attivo di tecnologie digitali innovative con un impatto positivo sull'ambiente e sul clima, al fine di accelerare la transizione verde;

d) promuovere norme e marchi di sostenibilità per i prodotti e i servizi digitali.

---

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

Etica dell’IA?

Sostenibilità e IA

Google e Microsoft nel 2023 hanno consumato più elettricità di Islanda, Ghana e Tunisia: colpa dell'intelligenza artificiale generativa



di F. Q. | 16 LUGLIO 2024

The dark side of the moon



Messaggio pubblicitario con finalità promozionale.

TECNOLOGIA

I proletari dell'intelligenza artificiale

Laura Melissari, giornalista
6.8.2024



https://www.internazionale.it/reportage/laura-melissari/2024/08/06/intelligenza-artificiale-lavoratori-sfruttamento



Sostenibilità e IA



Trasparenza e Deontologia



È PIÙ IMPORTANTE REGOLAMENTARE O ESSERE CONSAPEVOLI?

Gestione documentale e IA?



Documentazione informatica e IA

Particolare della “Predica agli uccelli” di San Francesco, Basilica Superiore di Assisi (Giotto, 1297-1299)



Strumenti fiduciari e IA

Ritratto del XVI secolo raffigurante il notaio Raniero, dipinto dal pittore fiammingo Quentin Massys.



Intelligenza Artificiale e gestione dei documenti:

- automazione processi
- acquisizione metadati
- ai nativa digitale nell’aiutare a valutare documenti

Intelligenza Artificiale e gestione dei documenti:



- qualità dati
- trasparenza IA e riconoscimento autori
- riservatezza nell'utilizzo dei documenti (*autorizzazioni nell'utilizzo del sistema, gestione metadati, problematiche di cancellazione di ciò che ormai ha nutrito il sistema etc.)*

Gestione documentale e robotica?

Prendiamo ad esempio il caso di un robot che sposta pallet in un magazzino logistico…

Il responsabile di produzione e il RSSP (Responsabile del Servizio di Prevenzione e Protezione) sono responsabili della sua ***sicurezza funzionale****; il software di visione basato sull'IA interessa chi deve* ***classificare il sistema secondo l'AI Act****; la connessione remota per la manutenzione è di responsabilità della funzione IT e di* ***cybersicurezza****; le immagini raccolte dalle telecamere comportano* ***trattamento dati*** *e coinvolgono il DPO; il* ***controllo dell'attività dei lavoratori*** *è di pertinenza delle risorse umane; il* ***contratto con il fornitore*** *comporta la gestione dell'accesso ai dati, aggiornamenti e responsabilità…*

Ambito	Norma	Stato / data chiave	Impatto sul robot
Sicurezza di prodotto	Regolamento (UE) 2023/1230 Regolamento macchine	Applicabile dal 20 gennaio 2027	Marcatura CE, cybersicurezza, comportamento evolutivo
Intelligenza artificiale	AI Act (UE) 2024/1689, modificato dal Reg. (UE) 2026/1744 (Digital Omnibus); L. 132/2025	Alto rischio: 2 dicembre 2027 (Allegato III) e 2 agosto 2028 (Allegato I)	Classificazione, divieti, trasparenza; requisiti AI per le macchine via Reg. Macchine
Cybersicurezza del prodotto	Cyber Resilience Act (UE) 2024/2847	Segnalazioni dall'11 settembre 2026; piena applicazione dall'11 dicembre 2027	Sicurezza by design, gestione vulnerabilità, SBOM
Cybersicurezza dell'organizzazione	NIS2 — D.Lgs. 138/2024	In vigore, obblighi progressivi	Gestione del rischio, supply chain, notifica incidenti
Dati	GDPR; Data Act (UE) 2023/2854	Data Act applicabile dal 12 settembre 2025	Dati personali, accesso ai dati dei prodotti connessi
Lavoro	D.Lgs. 81/2008; art. 4 L. 300/1970; L. 132/2025	In vigore	Valutazione rischi, formazione, controllo a distanza, informativa
Responsabilità	Direttiva (UE) 2024/2853 sui prodotti difettosi	Recepimento entro il 9 dicembre 2026	Software e aggiornamenti come parte del prodotto

Come gestire giuridicamente ed eticamente un progetto digitale di IA in ambito documentale in un’organizzazione pubblica o privata complessa?

(il caso complesso e delicato di un’azienda sanitaria)

Premesse

Il presupposto per avviare qualsiasi progetto di innovazione digitale, (a maggior ragione quando ci si avvalga di sistemi di intelligenza artificiale), deve essere la garanzia della ***qualità dei dati a disposizione****. Quindi, occorre prestare massima attenzione alle normative italiane ed europee e agli strumenti (tecnici e archivistici) a tutela dell'integrità, del costante aggiornamento, della completezza, della consultabilità, della comprensibilità, dell'omogeneità, della facile accessibilità, della usabilità, della condivisibilità e della interoperabilità dei dati.*



- Dati appartenenti a categorie particolari
- Filiera composita dei trattamenti posti in essere
- Finalità differenti e da verificare
- Rischi di security e data protection

Data protection e data security
(by design e by default)

Premesse

La digitalizzazione della sanità non può più essere letta come un mero processo di dematerializzazione documentale o di efficientamento amministrativo.
Essa determina una trasformazione profonda dell'organizzazione sanitaria, del rapporto medico-paziente, della responsabilità professionale, del trattamento dei dati personali e della stessa governance dei processi decisionali clinici.

La struttura sanitaria contemporanea non gestisce soltanto prestazioni sanitarie. Gestisce dati, infrastrutture digitali, piattaforme interoperabili, sistemi informativi clinici, dispositivi medici software, servizi cloud, fascicoli sanitari elettronici, dossier sanitari, sistemi di supporto alle decisioni e, quindi, sempre più frequentemente, strumenti basati su intelligenza artificiale.

In questo scenario, la struttura sanitaria diventa il punto di convergenza di diversi regimi normativi

Normative applicabili: data protection e data governance

Regolamento (UE) 2016/679 (GDPR)

+ D. Lgs. 196/2003 (Codice protezione dati)

Aspetti rilevanti:

- dati sanitari = categorie particolari di dati (art. 9);
- basi giuridiche del trattamento sanitario;
- accountability (mappatura e documenti);
- privacy by design e by default;
- DPIA;
- gestione dei data breach;
- diritti dell'interessato;
- rapporti titolare/responsabile/subresponsabili;
- trasferimenti internazionali

Nel settore sanitario le basi giuridiche spesso non coincidono con il consenso, ma derivano da obblighi di legge, assistenza sanitaria, medicina preventiva, interesse pubblico in sanità.

Data Act (Reg. UE 2023/2854)

Incide soprattutto su:

- accesso e condivisione dei dati generati da dispositivi connessi;
- interoperabilità;
- portabilità.

Avrà impatti significativi sui dispositivi medici connessi.

Data Governance Act (Reg. UE 2022/868)

Incide soprattutto su:

- condivisione dei dati;
- data altruism;
- riutilizzo dei dati protetti detenuti da enti pubblici

Richiamato espressamente come parte del nuovo ecosistema normativo europeo dei dati.

.

Normative applicabili: data governance e medical device

Regolamento (UE) 2025/327 European Health Data Space (EHDS)

Introduce:

- interoperabilità europea dei dati sanitari;
- accesso elettronico ai dati sanitari;
- uso primario dei dati per cura e assistenza;
- uso secondario per ricerca, innovazione, programmazione sanitaria;
- Health Data Access Bodies (HDAB);
- ambienti sicuri per il trattamento dei dati.

L'EHDS rappresenta probabilmente la più importante riforma europea della sanità digitale degli ultimi anni

Regolamento (UE) 2017/745 (MDR)

Per i dispositivi medici disciplina:

- progettazione;
- classificazione;
- marcatura CE e vigilanza mercato;
- sorveglianza clinica;
- software come dispositivo medico

Molti software sanitari e molte applicazioni AI possono essere qualificati come dispositivi medici..

Regolamento (UE) 2017/746 (IVDR)

Per i dispositivi diagnostici in vitro coinvolge:

- laboratori;
- diagnostica molecolare;
- test genetici.

NB *Il Regolamento (UE) 2023/607 modifica i regolamenti sui dispositivi medici MDR (UE) 2017/745 e IVDR (UE) 2017/746*

Normative applicabili: data security

Direttiva NIS2 (UE 2022/2555) + Cybersecurity Act (Reg. UE 2019/881) + Decreto Legislativo 138/2024

Coinvolge espressamente il settore sanitario.

Per le organizzazioni interessate al fine di prevenire rischi sistemici impone:

- governance cyber;
- gestione del rischio;
- incident response;
- business continuity;
- disaster recovery;
- sicurezza della supply chain;
- controllo accessi;
- formazione;
- crittografia.
- procedure di notifica incidenti.

Coordinamento GDPR e NIS2

Il GDPR richiede la "riservatezza, integrità e disponibilità" dei dati (art. 32) e la DPIA quando il rischio per i diritti è elevato (art. 35). La NIS2 richiede "adequate misure" di sicurezza per operazioni critiche.

La differenza è di percezione dei rischi da proteggere:

- **GDPR**: protegge i dati personali da un accesso non autorizzato
- **NIS2:** mantiene la disponibilità dei servizi critici da interruzioni

Una struttura ospedaliera deve soddisfare entrambe le normative. Es. Una cartella clinica compromessa viola sia il GDPR (esposizione dati) sia la NIS2 (interruzione servizio). La compliance integrata deve affrontare il rischio da entrambi i lati normativi.

Normative applicabili: digitalizzazione e servizi fiduciari

Regolamento EIDAS 910/2014 (come modificato da eIDAS 2 - Regolamento 2024/1183/UE) + D. Lgs. 82/2005 (CAD) + Linee Guida AgID

Rilevanti per:

- documenti informatici;
- firme elettroniche e riferimenti temporali;
- gestione e conservazione digitale;
- interoperabilità dei dati;
- identità e domicilio digitali;
- servizi di recapito.

La cartella clinica elettronica va formata, gestita e conservata secondo le regole del CAD e AgID (che garantiscono fonti documentali certe e archivi sicuri).

Il Fascicolo sanitario elettronico

Normativa principale:

- D.L. 179/2012 e successive modifiche e decreti attuativi FSE 2.0 (decreto ministeriale 7/09/2023)

Temi fondamentali:

- alimentazione del fascicolo;
- interoperabilità;
- accesso ai dati;
- tracciamento.

Il Fascicolo Sanitario Elettronico rappresenta uno dei maggiori ecosistemi di dati sanitari longitudinali italiani.

Normative applicabili: intelligenza artificiale

AI Act (Reg. UE 2024/1689) + Legge 132/2025

Le applicazioni sanitarie possono frequentemente rientrare tra i sistemi ad alto rischio.

Per tali sistemi sono richiesti:

- governance del rischio;
- qualità dei dati;
- documentazione tecnica;
- supervisione umana;
- trasparenza;
- monitoraggio mercato.

Molti sistemi di IA possono ricadere nella categoria dei sistemi ad alto rischio. Ciò può avvenire, in particolare, quando il sistema è un componente di sicurezza di un prodotto disciplinato dalla normativa di armonizzazione dell'Unione, oppure quando il prodotto stesso è soggetto a valutazione di conformità da parte di terzi.

Digital Omnibs

Il pacchetto Digital Omnibus IA - Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio del 29 giugno 2026. – ha modificato alcune parti dell'AI Act (Reg. UE 2024/1689)

Le nuove scadenze per l'entrata in vigore degli obblighi sono:

- Sistemi di IA ad alto rischio indipendenti: Rinviati al 2 dicembre 2027
- Sistemi di IA ad alto rischio integrati: Rinviati al 2 agosto 2028
- Obblighi di marcatura (watermarking) dei contenuti IA: Fissati al 2 dicembre 2026

La compliance integrata

Verifica dei principi fondamentali derivati dalle diverse discipline:

- ***libera circolazione, portabilità e protezione dei dati*** *(personali e non personali);*
- ***trasparenza*** *(non solo informativa su basi giuridiche, finalità, ruoli e diritti delle parti deboli coinvolte nei processi digitali, ma anche trasparenza degli algoritmi);*
- ***non esclusività della decisione algoritmica e non discriminazione algoritmica****;*
- ***accountability****, quindi, definizione di ruoli e responsabilità, di modelli organizzativi e procedure;*
- ***integrità*** *e, quindi,* ***affidabilità dei dati****;*
- ***sicurezza*** *e, quindi,* ***gestione del rischio****;*
- ***interoperabilità*** *di sistemi informatici, database e archivi digitali;*
- ***accessibilità*** *e* ***sostenibilità****.*



La compliance integrata

In estrema sintesi:

Oggi una struttura sanitaria per garantire la qualità dei dati e una governance coerente anche per gestire sistemi e modelli di IA deve ragionare su cinque pilastri integrati:

1. **Protezione dei dati** (GDPR + EHDS)
2. **Cybersicurezza** (NIS2 + legge italiana)
3. **Digitalizzazione documentale e sanitaria** (CAD + FSE + Telemedicina)
4. **Dispositivi medici** (MDR + IVDR)
5. Modelli e sistemi di **intelligenza artificiale** (AI Act + normativa nazionale).

È proprio l'intersezione tra questi cinque livelli che oggi costituisce la **vera governance della sanità digitale**, e che richiede necessariamente un approccio multidisciplinare tra giuristi, medici, informatici, ingegneri clinici, DPO, CISO e direzioni strategiche.

La compliance integrata: digitalizzazione e data protection

Provv. Garante privacy n. 353/2021, Solera

Per garantire la **protezione dei dati sanitari** in qualsiasi sistema digitale è indispensabile la predisposizione di sistemi di gestione documentale con i quali – attraverso l'adozione di appropriate misure organizzative e tecnologiche – individuare i documenti che nel corso dello svolgimento dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di **autenticità**, **integrità**, **affidabilità**, **leggibilità** e **reperibilità** prescritte dalla disciplina di settore applicabile.



La compliance integrata: AI Act e MDR

Quando si applica l'AI Act?
Ogni volta che si sviluppa o si utilizza un sistema di IA
Articolo 3 AI Act - Definizioni
Ai fini del presente regolamento si applicano le definizioni seguenti:
1) «**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;

Quando è alto rischio?
In sanità i dispositivi medici che usano AI, ad esempio:
- diagnostica
- triage
- supporto decisionale clinico
- radiologia
- interpretazione immagini

Art. 1 AI ACT – lo scopo della normativa
migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e di promuovere l'innovazione

La compliance integrata: data protection, NIS e IA

Privacy by Design: Un Caso di Studio con Federated Learning
La NIS2 richiede “Security by Design”; il GDPR richiede “Privacy by Design” (art. 25). In sanità, questi principi spesso convergono
Un esempio: **Machine Learning in Sanità**
Il machine learning in sanità ha un problema: addestrare un modello di AI diagnostica richiede dati da migliaia di pazienti. Centralizzare questi dati in un’unica location crea un rischio massivo. Se quel data lake viene compromesso, si mettono a rischio migliaia di cartelle cliniche.
Il Federated Learning è un’architettura dove il modello viene addestrato in modo distribuito: ogni ospedale addestra il modello localmente, sui propri dati, poi invia solo i “pesi” del modello (non i dati grezzi) a una location centrale. La location centrale aggrega i pesi (*cioè, i parametri matematici di ciò che il modello ha «imparato»),* migliora il modello, redistribuisce i pesi aggiornati. I dati sensibili non lasciano mai la struttura originaria. Questo è un esempio di “Privacy by Design”.

Fonte: Cybersecurity in Sanità: NIS2, GDPR e DPIA. Strategie di Resilienza Digitale per Strutture Critiche

La Privacy by Design è una **metodologia di governance**. Significa che quando disegni un nuovo sistema informatico sanitario, devi affrontare contemporaneamente le domande:

- **Quali dati raccolgo?** (data minimization)
- **Dove li memorizzo?** (locality, encryption, retention)
- **Chi vi accede?** (access control, logging)
- **Come li proteggo da compromessi? (**technical controls)
- **Come distruggo quello che non serve?** (secure deletion)

La compliance integrata: AI Act e data protection

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di intelligenza artificiale, GPDP, settembre 2023

*Nel suo Decalogo il Garante sottolinea che la realizzazione di un sistema nazionale di IA destinato a elaborare i dati sanitari di tutta la popolazione assistita impone il rigoroso rispetto di specifiche misure volte a garantire in concreto i principi di **esattezza** e **di aggiornamento dei dati**, che appaiono di particolare rilievo considerati i rischi di elaborazione di dati raccolti per finalità di cura che potrebbero essere stati, successivamente alla raccolta, modificati, rettificati o integrati. Il dato non aggiornato o inesatto influenzerebbe, inoltre, anche l'efficacia e la correttezza dei servizi che i suddetti sistemi di IA, che si basano sulla rielaborazione di tali dati, intendono realizzare. Questo assume valore, in particolare, nella fase di addestramento degli algoritmi, in quanto sulla base della qualità dei dati di natura sanitaria utilizzati in questa fase, l'IA è in grado di restituire output più o meno affidabili.*



Sintesi della compliance integrata: una matrice di applicabilità

Normativa	Quando si applica in sanità
GDPR	Qualsiasi trattamento di dati personali (anche sanitari)
NIS2	Solo alle organizzazioni sanitarie che rientrano tra soggetti essenziali o importanti
eIDAS 2	Quando si utilizzano firme elettroniche, identità digitali, autenticazione, attestazioni elettroniche
AI Act	Quando si sviluppano, immettono sul mercato o utilizzano sistemi di IA
MDR	Quando il software o il sistema è qualificabile come dispositivo medico
IVDR	Quando il sistema supporta diagnosi in vitro
Data Governance Act	Quando si condividono o riutilizzano dati nell'ambito degli spazi europei dei dati
Data Act	Quando si utilizzano dati generati da dispositivi connessi
EHDS	Quando si trattano dati sanitari elettronici nell'ecosistema europeo

Il ruolo delle strutture sanitarie nella digitalizzazione

Le strutture sanitarie pubbliche e private sono oggi investite di un ruolo centrale. Esse non sono semplici utilizzatrici di tecnologie predisposte da fornitori esterni, ma soggetti che determinano, organizzano e governano finalità, modalità, limiti e responsabilità dei processi digitali sanitari

La struttura sanitaria non può quindi limitarsi a “comprare” tecnologia.

Deve predisporre una **vera governance digitale**, comprendente almeno:

- **mappatura** dei processi sanitari digitalizzati;
- definizione dei **ruoli privacy**;
- analisi delle **basi giuridiche** dei trattamenti;
- **valutazione dei rischi** per diritti e libertà degli interessati;
- definizione di **policy interne** per accessi, autorizzazioni, logging e audit;
- **gestione dei rapporti** con fornitori e subfornitori;
- verifica di **trasparenza**, **sicurezza**, **interoperabilità** e **continuità operativa**;
- **valutazione preventiva** dei sistemi di IA eventualmente impiegati;
- **formazione** di medici, operatori sanitari e personale amministrativo;
- predisposizione di **meccanismi di controllo, segnalazione e accountability**.

La digitalizzazione sanitaria non può essere governata solo dall’ufficio IT. Richiede una governance integrata tra direzione sanitaria, direzione amministrativa, DPO, ufficio legale, responsabili dei sistemi informativi, risk manager, responsabili qualità, procurement, medici e operatori sanitari.

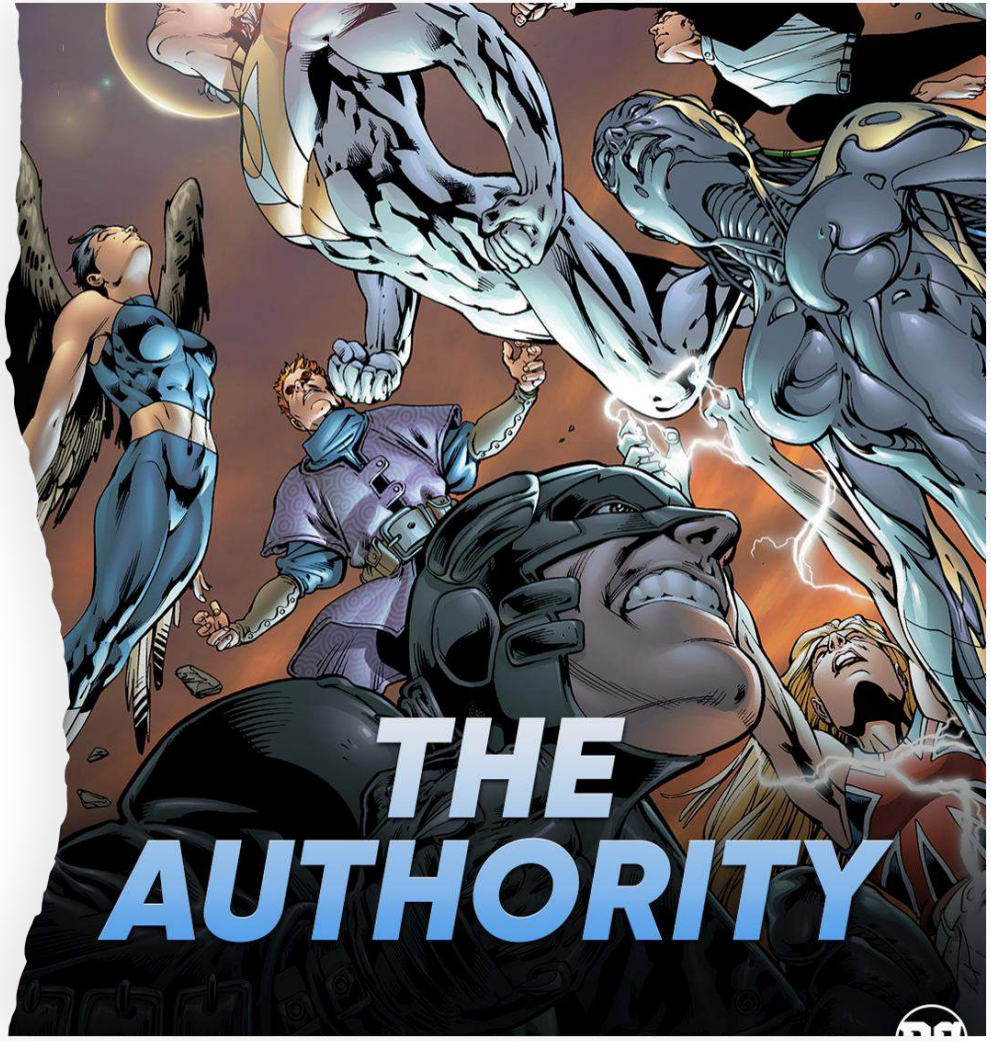
IA in sanità e GDPR: l’identificazione dei ruoli e delle responsabilità

Il rebus dei ruoli:

- ✓ *Provider*
- ✓ *Deployer*

- ✓ *Titolare*
- ✓ *Contitolare*
- ✓ *Responsabile*

- ✓ *Autorizzato*
- ✓ *Designato*



GDPR e dati sanitari: il baricentro resta l'accountability

Il GDPR ovviamente non vieta la sanità digitale. Al contrario, la rende possibile, ma a condizione che sia governata secondo i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.
Nel settore sanitario questi principi assumono una densità particolare, perché il dato sanitario non è un semplice dato amministrativo. È un dato che riguarda identità, vulnerabilità, storia clinica, dignità e libertà della persona.

La struttura sanitaria, in qualità di titolare, deve non solo rispettare il GDPR, ma essere in grado di dimostrare di averlo rispettato. Ciò comporta obblighi specifici:

- *tenuta del **registro dei trattamenti** ex art. 30 GDPR;*
- *definizione delle **autorizzazioni al trattamento**;*
- *designazione dei **responsabili del trattamento** ex art. 28 GDPR;*
- *adozione di **misure di sicurezza** ex art. 32 GDPR;*
- *gestione delle **violazioni dei dati personali** ex artt. 33 e 34 GDPR;*
- ***valutazione di impatto** sulla protezione dei dati ex art. 35 GDPR;*
- ***consultazione preventiva** dell'autorità ove necessario ex art. 36 GDPR;*
- ***nomina del DPO** ex art. 37 GDPR, normalmente necessaria nel contesto sanitario per la natura sistematica e particolare dei trattamenti.*

Il ruolo della struttura sanitaria come deployer di IA ad alto rischio

Se una struttura sanitaria utilizza un sistema di IA ad alto rischio, essa non può limitarsi a verificare che il prodotto sia “certificato” o “conforme”. La conformità del provider non esaurisce la responsabilità del deployer.
Il deployer deve utilizzare il sistema secondo le istruzioni d’uso, garantire la supervisione umana, monitorare il funzionamento, conservare i log ove previsto, informare gli interessati quando necessario, assicurare che i dati di input siano pertinenti e sufficientemente rappresentativi rispetto alla finalità d’uso, sospendere o segnalare l’uso in caso di rischio o malfunzionamento e predisporre personale adeguatamente formato.

In ambito sanitario ciò significa che la struttura deve porsi almeno queste domande:

- *il sistema è effettivamente qualificato come IA?*
- *è un sistema ad alto rischio?*
- *è anche dispositivo medico?*
- *è coperto da marcatura CE e valutazione di conformità pertinente?*
- *quale documentazione tecnica è stata fornita?*
- *quali istruzioni d’uso sono disponibili?*
- *quali limiti clinici sono dichiarati?*
- *quali dataset sono stati utilizzati per addestramento e validazione?*
- *il sistema è idoneo alla popolazione clinica della struttura?*
- *quali scenari di errore sono prevedibili?*
- *chi supervisiona l’output?*
- *il medico può discostarsi dal risultato algoritmico?*
- *tale discostamento è documentato?*
- *esiste un meccanismo di incident reporting?*
- *è stata svolta una DPIA?*
- *è necessaria una FRIA?*



DPIA (Data Protection Impact Assessment) e **FRIA** (Foundamental Rights Impact Assessment)

GDPR vs IA Act?

DPIA e FRIA: due valutazioni diverse, ma complementari

La **DPIA**, prevista dall'**art. 35 GDPR,** è una valutazione di impatto sulla protezione dei dati personali. È richiesta quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, specie in presenza di nuove tecnologie, trattamenti su larga scala di dati particolari, monitoraggio sistematico o profilazione.

La **FRIA**, prevista dall'**art. 27 dell'AI Act**, è invece una valutazione di impatto sui diritti fondamentali per determinati deployer di sistemi di IA ad alto rischio. L'art. 27 richiede, prima dell'uso, una valutazione che descriva i processi in cui il sistema sarà utilizzato, il periodo e la frequenza d'uso, le categorie di persone coinvolte, i rischi specifici di danno, le misure di supervisione umana e le misure da adottare in caso di materializzazione dei rischi, compresi meccanismi di governance interna e reclamo.

DPIA
Domanda centrale:
che cosa accade ai dati personali?

FRIA
Domanda centrale:
che cosa accade alla persona, alla sua dignità, alla sua autonomia, alla sua uguaglianza, alla sua libertà, a causa dell'uso dell'algoritmo?

Quando occorre la DPIA

Art. 35 GDPR.
In sanità la DPIA è quasi la regola.
Tipicamente per:

- ✅ dati sanitari su larga scala
- ✅ telemedicina
- ✅ piattaforme FSE
- ✅ sistemi di profilazione clinica
- ✅ algoritmi di triage
- ✅ monitoraggio remoto
- ✅ videosorveglianza sanitaria avanzata
- ✅ IA che utilizza dati dei pazienti

Il ruolo del medico tra Legge Gelli, GDR e AI ACT

Consenso informato
Art. 1 Legge 219/2017.

Serve per:
• attività diagnostiche;
• attività terapeutiche;
• attività assistenziali.

Tutela:
• autodeterminazione del paziente;
• integrità psico-fisica;
• libertà di cura.

La domanda da porsi è:
Il paziente accetta l'atto medico?

Consenso GDPR
Nel trattamento ordinario dei dati sanitari il consenso «privacy» non è normalmente la base giuridica.
Il GDPR (art. 9) consente infatti il trattamento per:
• finalità di cura;
• medicina preventiva;
• diagnosi;
• assistenza sanitaria;
• gestione del sistema sanitario.

Pertanto:
Consenso informato → quasi sempre sì
Consenso GDPR → spesso no, ma obbligo di informativa
Errore frequente:
ritenere che il consenso informato copra anche il GDPR.
Non è vero. Sono due istituti autonomi.

Cosa cambia con l'AI Act?
Non basta più chiedersi:
• il paziente ha acconsentito?
• il trattamento dei dati è lecito?

Occorre chiedersi anche:
• è legittimo affidarsi all'algoritmo?
• chi controlla l'algoritmo?
• chi risponde degli errori?

Il ruolo del medico ai tempi dell’IA Act e della Legge 132/2005

La Legge 24/2017 (Gelli-Bianco) parte da un presupposto preciso: l'atto medico resta umano.

Il medico:
- valuta;
- decide;
- assume responsabilità.

L'AI Act e la legge italiana partono da un presupposto differente:
L'algoritmo può influenzare la decisione.
Per questo introduce:
- supervisione umana;
- monitoraggio;
- governance del rischio.

Il medico può "scaricare" la responsabilità sull'ia?

No. Anzi. Più aumenta il supporto algoritmico, più diventa centrale il ruolo del medico.

Perché, secondo la normativa UE (e italiana), l'AI non sostituisce il professionista. Essa impone invece:

- capacità critica;
- controllo;
- supervisione.

Un principio che potrebbe diventare centrale nella futura giurisprudenza: l'errore algoritmico non interrompe automaticamente la responsabilità professionale.

Occorrerà verificare:

- se il medico ha informato il paziente sull’uso dell’IA
- se ha compreso il risultato (e quindi se è stato formato);
- se ha verificato la plausibilità clinica;
- oppure se ha seguito acriticamente la macchina.

Clausole contrattuali essenziali da prevedere

In estrema sintesi, in un contratto sanitario digitale, specie se collegato a IA, dovrebbero essere presenti almeno le **seguenti clausole**:

1. Oggetto del servizio e descrizione funzionale
2. Qualificazione privacy dei ruoli
3. Accordo ex art. 28 GDPR o accordo ex art. 26 GDPR
4. Divieto di riuso dei dati per finalità proprie
5. Disciplina del riuso per ricerca, sviluppo o training IA
6. Misure di sicurezza tecniche e organizzative
7. Gestione di subfornitori e trasferimenti extra SEE
8. Data breach e incident response
9. Logging, tracciabilità e audit
10. Continuità operativa, backup e disaster recovery
11. Restituzione, portabilità e cancellazione dei dati
12. Qualificazione del sistema IA
13. Conformità AI Act e normativa dispositivi medici
14. Documentazione tecnica e istruzioni d'uso
15. Informazioni per DPIA e FRIA
16. Human oversight
17. Monitoraggio post vendita e incident reporting
18. Aggiornamenti, modifiche e retraining
19. Responsabilità, manleve, penali e assicurazioni
20. Recesso, sospensione e risoluzione per non conformità
21. Restituzione input e output.

La struttura sanitaria come centro di accountability

La vera responsabilità della struttura sanitaria non consiste solo nel rispettare singoli adempimenti, ma nel **costruire un sistema di accountability**.
Ciò significa che la struttura deve essere in grado di dimostrare:

- perché ha scelto una determinata tecnologia;
- quali rischi ha valutato;
- quali alternative ha considerato;
- quali misure ha adottato;
- quali istruzioni ha dato;
- quali controlli ha svolto;
- quali contratti ha stipulato;
- quali audit ha effettuato;
- come ha formato il personale;
- come ha gestito incidenti, errori e reclami;
- come ha aggiornato DPIA, FRIA e governance.

La digitalizzazione sanitaria non elimina la responsabilità organizzativa.
La rende più evidente.

La struttura sanitaria come centro di compliance integrata ai tempi dell'IA

L'IA introduce un ulteriore livello di complessità rispetto al passato, perché il dato non è solo oggetto di protezione. Diventa materia prima di decisioni, classificazioni, predizioni, raccomandazioni e priorità.
Il problema non è più soltanto:
chi accede al dato sanitario?
ma anche:
chi trasforma quel dato in una decisione o in una raccomandazione clinica?
E ancora:
chi controlla il modo in cui l'algoritmo incide sulla persona?
È qui che GDPR, EHDS e AI Act devono essere letti insieme.
Il **GDPR** tutela il dato personale come espressione della persona.
L'**EHDS** mira a rendere il dato sanitario accessibile, interoperabile e riutilizzabile in un quadro regolato.
L'**AI Act** mira a impedire che sistemi algoritmici opachi, discriminatori o non governati incidano su salute, sicurezza e diritti fondamentali.

La struttura sanitaria si trova quindi al centro di una nuova responsabilità: garantire che l'innovazione non produca una regressione delle tutele dei nostri diritti e libertà fondamentali

PARTE 2

Sezione 1

I passi da fare nella gestione dei fornitori di IA

4.2 FINALITÀ PERSEGUITE NELL'ADOZIONE DI SISTEMI DI IA

La Camera adotta sistemi di IA focalizzati sulle finalità di:

- migliorare l'efficienza operativa, anche attraverso l'automatizzazione di processi ripetitivi, al fine di ridurre i tempi della definizione dei procedimenti e migliorare la performance complessiva.
- migliorare i servizi alle imprese e agli utenti, aumentando la propria capacità di gestione dei dati;
- migliorare lo sviluppo di soluzioni innovative a supporto delle attività della Camera di commercio.

A titolo esemplificativo e non esaustivo l'Ente, alla luce della propria missione e dei compiti istituzionali attribuiti, individua i seguenti ambiti di applicazione di sistemi e strumenti IA.

1. **Comunicazione istituzionale**

Finalità: Migliorare i rapporti con l'utenza, mantenere l'accessibilità e la comprensibilità per ogni cittadino.

Strumenti: Assistenti virtuali, analisi del sentiment, piattaforme automatizzate, traduzione automatica, sistemi NLP.

2. **Supporto decisionale**

Finalità: Ottimizzare la gestione delle risorse pubbliche, migliorare l'efficienza e la rapidità delle decisioni.

Strumenti: Modelli predittivi affidabili.

3. **Gestione documentale e procedimentale**

Finalità: Automatizzare il ciclo documentale e la gestione dei relativi metadati, predisporre e controllare la documentazione collegata ai procedimenti amministrativi, migliorare le tempistiche dei procedimenti.

Strumenti: Sistemi NLP, piattaforme automatizzate di gestione dei contenuti digitali, sistemi di classificazione automatica dei documenti.

4. **Supporto giuridico**

Finalità: Ottimizzare l'approfondimento normativo, dottrinale e giurisprudenziale, supportare gli uffici nella redazione di atti e documenti, verificandone la conformità normativa.

Strumenti: Sistemi NLP, sistemi per la verifica automatica della conformità normativa degli atti, sistemi per la redazione assistita dei documenti.

5. **Procedure di acquisto**

Finalità: Rendere più efficiente e trasparente il procurement.

Strumenti: Sistemi per la gestione dei Contratti Pubblici, automatizzazione del procurement, sistemi di monitoraggio automatico delle performance fornitori, ~~algoritmi di valutazione automatica delle offerte~~.

6. **Servizi a cittadini e imprese**

Finalità: Personalizzare e migliorare la fruibilità dei servizi.

Strumenti: Assistenti virtuali, traduzione automatica, sistemi NLP, supervisione umana, assistenti vocali /interfacce conversazionali multimodali, sistemi di feedback automatizzato per raccogliere opinioni.

7. **Inclusione e trasparenza**

Finalità: Favorire l'accesso ai servizi alle fasce più fragili dell'utenza e garantire chiarezza nell'uso dell'IA.

Strumenti: Traduzione automatica, analisi del sentiment, sistemi di feedback e raccolta opinioni automatizzate, interfacce inclusive e semplificate.

Linee Guida per l'adozione di sistemi e strumenti di IA da parte della Camera e per la disciplina del rapporto contrattuale con i fornitori

In conformità al Regolamento 2024/1689/UE (AI Act) e al Regolamento 2016/679/UE (GDPR)

CAMERA DI COMMERCIO MILANO MONZABRIANZA LODI

Aprile 2026

Un quadro normativo stratificato e in evoluzione

- **AI Act (Reg. 2024/1689/UE)**

  Primo framework giuridico globale sui sistemi di IA: obblighi per fornitori e deployer in base alla classe di rischio
- **Digital Omnibus sull'IA (Reg. 2026/1744/UE)**

  Semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale
- **GDPR (Reg. 2016/679/UE)**

  Protezione dei dati personali: regola trattamenti automatizzati, decisioni algoritmiche, ruoli contrattuali
- **Legge n. 132/2025**

  Disposizioni italiane su IA: uso nella PA, supervisione umana, obblighi informativi, responsabilità
- **D.Lgs. 9 settembre 2026, n. 160**

  In materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale
- **MCC-AI della Commissione Europea**

  Model Contractual Clauses for Non-High-Risk AI Procurement: template contrattuali volontari, ma di riferimento
- **NIST AI RMF 1.0 & FNCS**

  Framework di risk management e cybersecurity: standard tecnici incorporati nell'approccio regolatorio

Glossario essenziale (1/2)

- **AI Act**

  Regolamento UE 2024/1689: primo quadro normativo globale per i sistemi di IA, in vigore dall'agosto 2024 con entrata in vigore progressiva

- **Deployer**

  Soggetto che utilizza un sistema IA sotto la propria autorità, anche integrandolo nei propri sistemi senza modificarne significativamente il funzionamento

- **DPIA**

  Data Protection Impact Assessment: valutazione d'impatto sulla protezione dei dati, obbligatoria ex art. 35 GDPR per trattamenti ad alto rischio

- **FRIA**

  Fundamental Rights Impact Assessment: valutazione dell'impatto sui diritti fondamentali, obbligatoria ex art. 27 AI Act per sistemi ad alto rischio nella PA

- **GPAI**

  General Purpose AI: modello IA per finalità generali (es. GPT, Claude, Gemini) con obbligo di documentazione ex art. 53 AI Act

- **MCC-AI**

  Model Contractual Clauses for AI Procurement: template contrattuali volontari della Commissione UE per acquisti di sistemi IA non ad alto rischio

Glossario essenziale (2/2)

- **Provider (Fornitore)**

  Soggetto che sviluppa e immette sul mercato il sistema IA: responsabile della conformità tecnica e della documentazione
- **Responsabile del trattamento**

  Soggetto che tratta dati personali per conto del Titolare: designato formalmente con atto ex art. 28 GDPR
- **RTD**

  Responsabile della Transizione Digitale: coordina l'innovazione digitale e il piano IA nella PA

  DPO / RPD

  Data Protection Officer: sorveglia il rispetto del GDPR; punto di contatto con il Garante e gli interessati

  RGD

  Responsabile della Gestione documentale
- **Supply chain IA**

  L'insieme dei soggetti coinvolti nella progettazione, sviluppo, distribuzione e utilizzo di un sistema IA: dal foundation model al deployer finale
- **Lock-in**

  Dipendenza tecnologica da un fornitore che rende costoso o impossibile il cambio: rischio strategico da mitigare contrattualmente

L’organizzazione universitaria come Deployer di IA

- Nella catena del valore dell'IA, un ente universitario agisce prevalentemente come **deployer**: utilizza sistemi IA sviluppati da terzi, integrandoli nelle proprie attività istituzionali
- Come deployer, **l’ente non è esente da obblighi**: è tenuto a verificare che il fornitore abbia adottato un sistema di gestione del rischio adeguato
- L’ente è al contempo **Titolare del trattamento ai sensi del GDPR**: i dati personali trattati tramite IA rimangono sotto la sua responsabilità giuridica
- Questo duplice ruolo (deployer AI Act + Titolare GDPR) impone una **governance contrattuale robusta** con ciascun fornitore nella supply chain
- L'adozione di **Linee Guida** e di altri strumenti operativi è espressione di una politica di accountability proattiva

Sistemi di IA ad alto rischio

I sistemi di IA ad alto rischio sono quelli che possono causare danni significativi alla salute, alla sicurezza o ai diritti fondamentali delle persone.

Sono definiti dall’art. 6 dell’AI Act (Regolamento UE 2024/1689) e si dividono in base al loro utilizzo in **settori chiave** o come **componenti di sicurezza** di prodotti normati.

Categorie e settori principali (Allegato III dell'AI Act):



Biometria e riconoscimento: Sistemi di identificazione biometrica remota (tranne la semplice verifica d'identità), categorizzazione biometrica e riconoscimento delle emozioni.



Infrastrutture critiche: Componenti di sicurezza nella gestione di traffico stradale, reti idriche, gas, riscaldamento, elettricità e infrastrutture digitali.

Sistemi di IA ad alto rischio



Istruzione e formazione: Accesso a istituti scolastici, valutazione dell'apprendimento e monitoraggio del comportamento durante i test.



Occupazione e gestione del lavoro: Selezione e assunzione del personale, assegnazione di mansioni, monitoraggio delle prestazioni e gestione dei contratti.



Servizi essenziali pubblici e privati: Accesso a benefici pubblici, credit scoring (valutazione dell'affidabilità creditizia), assicurazioni sanitarie o sulla vita e gestione delle chiamate di emergenza.



Ordine pubblico e sicurezza: Valutazione del rischio di reato o recidiva, uso di poligrafi e verifica dell'affidabilità delle prove.



Migrazione e controllo delle frontiere: Esame di visti o richieste d'asilo, gestione dei poligrafi e rilevamento di documenti di identità.

AI Act, art. 26 — Obblighi dei deployer

“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.”

Al fine di attuare le misure di sorveglianza umana e di conservare i log generati automaticamente da tale sistema di IA per almeno 6 mesi (paragrafi 3 e 6)

Una catena di fornitura non governata contrattualmente espone l’Organizzazione a responsabilità dirette

Perché la supply chain IA è diversa dalle forniture tradizionali

- **Opacità tecnologica**: i sistemi IA sono spesso black box; il deployer non ha visibilità diretta sui meccanismi decisionali
- **Rischio di bias**: i dataset di addestramento possono incorporare distorsioni che si propagano nelle decisioni istituzionali
- **Trattamento dati su larga scala**: i sistemi IA trattano grandi volumi di dati personali su larga scala, spesso in modo continuo e automatico
- **Dipendenza tecnologica**: il lock-in con un fornitore IA è più profondo rispetto a forniture standard; il cambio ha costi elevati
- **Evoluzione normativa rapida**: il quadro regolatorio è in formazione; i contratti devono contenere clausole di adeguamento
- **Responsabilità distribuita**: la catena di responsabilità IA coinvolge sviluppatori, deployer, sub-fornitori e piattaforme cloud

Altri riferimenti normativi e documentali essenziali

- EDPS Guidance for Risk Management of AI Systems
- Piano Triennale per l'informatica nella PA 2024-2026 (AGID)
- Guidelines for Secure AI System Development (NCSC/CISA/ACN)
- D.Lgs. 82/2005 (CAD), L. 633/1941 (diritto d'autore), D.Lgs. 30/2005 (proprietà industriale)

Linee guida AgID

L'11 aprile 2026 si è chiusa la consultazione sulle “Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione” e sulle “Linee Guida per il procurement di IA nella Pubblica Amministrazione”.

Il 20 marzo 2025 si è invece conclusa la consultazione pubblica delle Linee Guida per l’adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, adottate con la Determinazione n.17/2025, il cui iter di adozione è in corso.

Piano Triennale per l'informatica nella PA 2024-2026 (AGID)

AGID Agenzia per l'Italia Digitale

Il decalogo dell'IA

Indicazioni pratiche per l'uso dell' IA nella PA



Miglioramento dei servizi e riduzione dei costi

Le PA concentrano l'investimento in tecnologie di IA nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali



Trasparenza, responsabilità e informazione

Le PA forniscono informazioni adeguate agli utenti al fine di consentire loro di prendere decisioni informate riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale.



Analisi del rischio

Le PA analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che non provochino violazioni dei diritti fondamentali della persona



Accessibilità e inclusività

Le PA assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione



Privacy e sicurezza

Le PA adottano elevati standard di sicurezza e protezione della privacy per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile.



Standardizzazione

Le PA tengono in considerazione soluzioni basate sull'IA, le attività di normazione tecnica in corso a livello internazionale e a livello europeo



Foundation Models

Le PA si assicurano che i foundation models adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli



Formazione e sviluppo delle competenze

Le PA investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici.



Sostenibilità

Le PA valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale



Dati

Le PA, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce i dati

Sezione 2

Soggetti, ruoli e responsabilità nella supply chain

Fornitore vs Deployer: obblighi distinti

FORNITORE (Provider)

- Sviluppa e immette sul mercato il sistema IA
- Redige la documentazione tecnica
- Esegue test e valutazione di conformità
- Registra il sistema nei database UE (alto rischio)
- Garantisce istruzioni d'uso chiare e aggiornate
- Risponde del ciclo di vita del prodotto

DEPLOYER (Utilizzatore)

- Utilizza il sistema IA sotto la propria responsabilità
- Assicura supervisione umana adeguata
- Rispetta le istruzioni del fornitore
- Informa e tutela le persone interessate
- Conduce FRIA per sistemi ad alto rischio
- È Titolare del trattamento ex GDPR

La catena di fornitura tipica di un sistema IA per la PA

- **Livello 1 – Foundation Model provider (es. OpenAI, Anthropic, Google)**
  Sviluppa il modello base; il deployer ha limitata visibilità e negoziazione diretta

- **Livello 2 – System integrator o Software house**
  Costruisce la soluzione specifica integrando il modello base; è il principale interlocutore contrattuale

- **Livello 3 – Cloud / Infrastructure provider**
  Ospita e processa i dati; deve essere mappato come sub-responsabile del trattamento

- **Livello 4 – Deployer (ente universitario)**
  È responsabile verso gli utenti finali di ogni decisione adottata tramite il sistema

La governance contrattuale deve operare su tutta la catena: clausole di responsabilità, flusso per garantire i diritti e obblighi da imporre ai sub-fornitori

I quattro pilastri della supply chain IA responsabile

1. Selezione

Due diligence sul fornitore: classe di rischio, certificazioni, capacità di compliance

2. Contratto

Clausole specifiche AI Act + GDPR + MCC-AI: allocazione chiara di rischi, obblighi, penali

3. Monitoraggio

KPI, accesso ai log, audit periodici, gestione degli incidenti, supervisione umana continuativa

4. Exit Strategy

Portabilità dei dati (delle personalizzazioni e degli eventuali Agent), cancellazione sicura, continuità del servizio

Sezione 2

La tassonomia dell'AI Act come leva decisionale

La piramide del rischio: quattro livelli (AI Act, artt. 5–6)

- **Rischio INACCETTABILE → VIETATI (art. 5)**
  Scoring sociale, manipolazione subliminale, sorveglianza biometrica in real time. Divieto assoluto per l'ente

- **Rischio ALTO → Obblighi stringenti (art. 6 + Allegato III)**
  Selezione HR, accesso a servizi essenziali, infrastrutture critiche. FRIA obbligatoria; gestione documentata del rischio

- **Rischio LIMITATO → Obblighi di trasparenza**
  Chatbot, sistemi generativi di testo/immagini. Obbligo di disclosure verso l'utente (art. 50)

- **Rischio MINIMO o NULLO → Regime ordinario**
  Sistemi con impatto trascurabile. Vigilanza interna; buone pratiche; codici di condotta volontari

⚠ **Attenzione: la classificazione non dipende solo dalla tecnologia, ma dal contesto di utilizzo**

Un esempio:
Sistemi ad alto rischio rilevanti per la Camera di Commercio

“La Camera di Commercio, laddove non strettamente indispensabile per il perseguimento degli scopi istituzionali e il conseguimento delle finalità preposte, **si impegna a evitare o limitare l’utilizzo di sistemi di IA ad alto rischio**. In tali casi, l’Ente documenta le valutazioni di stringente necessità circa la loro adozione e garantisce che siano utilizzati conformemente a quanto previsto dalla normativa applicabile, solo previo svolgimento di una valutazione d’impatto sui diritti fondamentali e della conseguente implementazione delle misure correttive adeguate a mitigare i relativi rischi.

Inoltre, la Camera di Commercio **esclude l’adozione di sistemi che comportino l’assunzione di decisioni che producono effetti giuridici o incidano significativamente su diritti, doveri o legittime aspettative dell’interessato esclusivamente automatizzate,** senza un’adeguata supervisione, validazione e responsabilità umana.”

Linee Guida per l’adozione di sistemi e strumenti di IA da parte della Camera e per la disciplina del rapporto contrattuale con i fornitori, 2026

La FRIA: Fundamental Rights Impact Assessment (art. 27 AI Act)

- Obbligatoria per i deployer organismi di diritto pubblico o enti privati che forniscono servizi pubblici prima della messa in esercizio di qualsiasi **sistema IA ad alto rischio**
- Deve descrivere: processi coinvolti, frequenza e durata d'uso, categorie di persone interessate, dati trattati
- Analisi dei rischi per diritti fondamentali: non discriminazione, privacy, accesso a servizi pubblici, difesa
- Individuazione delle misure correttive: supervisione umana, limitazioni operative, meccanismi di reclamo
- **La FRIA è distinta (ma complementare) alla DPIA del GDPR**: le due valutazioni devono essere coordinate
- I risultati della FRIA devono essere comunicati all'Autorità di vigilanza e al Garante nei casi previsti
- Il fornitore collabora alla FRIA fornendo la documentazione tecnica necessaria

Sezione 3

Il framework operativo per una supply chain trasparente

Le principali aree di attenzione nella relazione con i fornitori IA

1. Gestione del rischio

Supporto tecnico alla classificazione e alla valutazione del rischio per l'intero ciclo di vita

2. Dati personali

Responsabile del trattamento ex art. 28 GDPR; limitazione finalità; divieto di uso per addestramento

3. Documentazione

Istruzioni d'uso, capacità/limiti del sistema, conformità normativa dimostrabile

4. Log e registri

Conservazione eventi, accesso su richiesta, consegna a fine contratto per accountability

5. Supervisione umana

Strumenti graduati in base al rischio: revoca output, arresto sistema, interpretazione decisioni

6. Cybersicurezza

Integrità, disponibilità, resilienza; misure preventive, rilevazione, risposta e ripristino

7. Assistenza e audit

Cooperazione per verifiche di conformità; formazione del personale; KPI misurabili

8. Proprietà intellettuale

Titolarità di algoritmi, modelli addestrati, agenti IA, output; manleva per violazioni a terzi

La leva contrattuale: da clausole generiche a clausole specifiche sull'AI (*un esempio dall'ente camerale*)

- Le Condizioni Generali di Contratto della Camera (2023) si applicano anche ai fornitori IA: rispetto normativa, DURC, penali, risoluzione
- Tuttavia non sono sufficienti: mancano clausole specifiche per gestione del rischio IA, limitazione d'uso dei dati, supervisione umana, log
- L'integrazione con clausole AI-specific è obbligatoria per sistemi ad alto rischio e fortemente raccomandata per tutti i sistemi IA
- Le Linee Guida della Camera (2026) colmano questo gap indicando elementi da contrattualizzare (§ 6.1) e clausole da inserire (§ 6.2)
- Il principio guida è la proporzionalità: più alto il rischio del sistema, maggiore il dettaglio delle clausole richieste

Il principio di accountability nella supply chain IA

- Il GDPR introduce la responsabilizzazione del Titolare: occorre dimostrare la conformità, non solo affermarla (art. 5, par. 2)
- L'AI Act rafforza questo principio richiedendo documentazione del ciclo di vita, registri, audit interni
- La Legge n. 132/2025 ribadisce che nella PA la responsabilità ultima degli output IA è dell'ente che li utilizza
- Implicazione pratica: l’ente deve poter dimostrare ex post ogni scelta effettuata nella supply chain IA
- Gli strumenti dell'accountability: politiche documentate, contratti strutturati, log accessibili, DPIA/FRIA aggiornate
- La supply chain IA non governata diventa un rischio reputazionale e sanzionatorio direttamente in capo all’ente

Sezione 4

Due diligence giuridica e tecnica ante-contratto

La due diligence pre-contrattuale sul fornitore IA

- **Identità e qualifica**
  Il fornitore è provider o deployer a sua volta? Ha sub-fornitori critici (modelli base, cloud)? Qual è la catena di responsabilità?

- **Conformità AI Act**
  Il sistema è registrato nel database EU per alto rischio? Esiste dichiarazione CE di conformità? Sono disponibili le istruzioni d'uso?

- **Conformità GDPR**
  Violazioni di dati pregresse notificate al Garante? Politica di data breach? DPO designato?

- **Capacità tecnica di compliance**
  Certificazioni ISO 27001, SOC2, ISO 42001? Processi interni di AI governance documentati?

- **Solidità contrattuale**
  Il fornitore è disposto a firmare un atto di designazione ex art. 28 GDPR? A inserire clausole MCC-AI?

Criteri di selezione: lista di valutazione (scoring)

- Trasparenza del modello: il fornitore fornisce informazioni sul modello base, sui dataset di addestramento, sui limiti noti del sistema?
- Localizzazione dei dati: i dati sono trattati in UE o in Paesi terzi con decisione di adeguatezza? Esistono garanzie ex artt. 46-49 GDPR?
- Separazione dei dati: i dati dell'ente sono isolati da quelli di altri utenti/clienti? Vi è garanzia di non utilizzo per addestramento cross-cliente?
- Politica di ritenzione: il fornitore si impegna a cancellare i dati alla scadenza del contratto in modo irreversibile?
- Aggiornamento normativo: il fornitore garantisce aggiornamenti del sistema in caso di cambiamenti normativi rilevanti?
- Continuità operativa: esiste un piano di business continuity?

Red flag vs Green flag nella valutazione del fornitore

🔴 RED FLAG — Rischi da evitare

- Rifiuto di firmare l'atto ex art. 28 GDPR
- Clausole che attribuiscono al fornitore il diritto di usare i dati per proprie finalità
- Assenza di documentazione tecnica del sistema
- Nessuna politica di gestione degli incidenti
- Dati processati in Paesi senza adeguatezza UE senza garanzie
- Lock-in contrattuale senza exit strategy definita
- Rifiuto di audit effettivi o verifiche di conformità

🟢 GREEN FLAG — Indicatori positivi

- Atto ex art. 28 GDPR dettagliato
- Divieto esplicito di uso dati per addestramento
- Documentazione tecnica disponibile e aggiornata
- Processo di data breach notification < 72h
- Dati in EU con certificazioni di sicurezza
- Clausole di portabilità e cancellazione sicura
- Disponibilità ad audit e ispezioni periodiche

La richiesta di evidenze al fornitore: cosa chiedere formalmente

- Copia della documentazione tecnica del sistema IA (art. 11 AI Act per alto rischio)
- Dichiarazione di conformità o auto-dichiarazione del fornitore rispetto alla classe di rischio
- Policy di gestione dei dati: finalità di trattamento, sub-responsabili, misure di sicurezza ex art. 32 GDPR
- Descrizione del sistema di gestione del rischio adottato (NIST AI RMF o equivalente)
- Metriche di accuratezza, robustezza e sicurezza del sistema (in particolare per alto rischio)
- Piano di business continuity e disaster recovery
- Riferimenti a certificazioni, codici di condotta o adesioni a standard internazionali (es. ISO 42001)

Sezione 5

Le MCC-AI della Commissione Europea e le clausole da inserire

Le Model Contractual Clauses for AI Procurement (MCC-AI)

- Documento adottato dalla Public Buyers Community della Commissione Europea: clausole contrattuali modello per l'acquisto di sistemi IA non ad alto rischio
- Finalità: garantire trasparenza, controllo e accountability nella relazione PA-fornitore IA, basandosi su un rapporto equilibrato e fiducia reciproca
- Natura volontaria, ma di forte riferimento normativo: le Linee Guida dell'ente le adottano esplicitamente come parametro
- Struttura: le MCC-AI coprono obblighi del fornitore in materia di conformità, dati, documentazione, supervisione umana, incidenti, log, sicurezza
- Le MCC-AI sono complementari (non sostitutive) alle clausole GDPR ex art. 28 e alle condizioni generali di contratto
- Per sistemi ad alto rischio, le clausole MCC-AI-High-Light prevedono obblighi rafforzati documentati nelle Linee Guida

Struttura di un contratto IA completo: le sezioni chiave

- **Premesse e definizioni**
  Identificazione delle parti, ruoli (provider/deployer, Titolare/Responsabile), contesto istituzionale d'uso
- **Oggetto e specifiche tecniche**
  Descrizione del sistema, funzionalità, requisiti di conformità, tecnologie di terze parti, licenze
- **Qualità e governance dei dati**
  Ruolo del fornitore come Responsabile ex art. 28, limitazione finalità, divieto addestramento
- **Documentazione tecnica e log**
  Istruzioni d'uso, registri eventi, accesso su richiesta, consegna a fine contratto
- **Supervisione umana e cybersicurezza**
  Strumenti di intervento, metriche sicurezza, business continuity
- **Proprietà intellettuale e indennizzi**
  Titolarità algoritmi/output, manleva per violazioni IP a terzi
- **Recesso, risoluzione e exit strategy**
  Portabilità dati, cancellazione sicura, consegna software sviluppato ad hoc

L'atto di nomina a Responsabile del trattamento (art. 28 GDPR)

- Ogni fornitore IA che tratta dati personali per conto dell’ente universitario deve essere formalmente designato come Responsabile del trattamento
- L'atto ex art. 28 GDPR deve specificare: oggetto, durata, natura e finalità del trattamento, tipo di dati, categorie di interessati
- Obblighi essenziali del Responsabile: trattare solo su istruzione documentata; garantire riservatezza del personale; adottare misure ex art. 32; non coinvolgere sub-responsabili senza autorizzazione
- Diritto di audit: il Titolare (ente universitario) deve poter effettuare ispezioni e ottenere prove della compliance
- Cancellazione o restituzione: il Responsabile deve restituire o distruggere tutti i dati al termine del contratto
- Se utilizzato per la fornitura di soluzioni di IA, il modello di nomina predisposto dall’ente deve essere integrato / gestito insieme a un documento contenente clausole AI-specific: divieto uso dati per addestramento, gestione log, FRIA

Clausole critiche: limitazione d'uso dei dati e divieto di addestramento

- Clausola essenziale: il fornitore si impegna a non utilizzare i dati personali dell’ente inclusi log, prompt, output) per qualsiasi finalità propria o diversa dall'esecuzione del contratto
- Divieto specifico e tassativo: non riutilizzare i dati per addestrare, affinare o migliorare qualsiasi modello IA
- Questo divieto è fondato su più basi normative: art. 5 GDPR (limitazione delle finalità), art. 28 GDPR (istruzioni del Titolare), art. 4 L. 132/2025
- Estensione ai sub-fornitori: la clausola deve essere traslata contrattualmente ai sub-responsabili e ai provider di modelli base
- Penale specifica: la violazione di questa clausola deve essere espressamente prevista come causa di risoluzione immediata e risarcimento danni
- Verifica: il fornitore deve fornire evidenza tecnica (audit log, policy interna) che i dati non vengano utilizzati per addestramento

Clausole sulla proprietà intellettuale degli output IA

- Il contratto deve definire esplicitamente la titolarità degli output generati dal sistema IA (testi, elaborazioni, raccomandazioni, decisioni)
- Per sistemi sviluppati su specifica commessa dell'ente: la titolarità del codice sorgente e del modello addestrato spetta all'ente committente
- Per sistemi SaaS o in licenza: l'output applicato a processi istituzionali dell'ente deve essere utilizzabile senza limitazioni per le finalità istituzionali
- Divieto al fornitore di pubblicare, condividere o rivendicare i prompt e gli output dell'ente come casi d'uso propri senza consenso
- Manleva IP: il fornitore garantisce l'ente da ogni pretesa di terzi per violazione di copyright, brevetti o IP relativi al modello base, ai dataset o agli output
- Riferimento normativo: L. 633/1941 (diritto d'autore), D.Lgs. 30/2005 (codice proprietà industriale), art. 25, par. 5, AI Act

Clausole di exit strategy e portabilità

- La dipendenza tecnologica (lock-in) è uno dei rischi strategici più sottovalutati nella supply chain IA: deve essere mitigata contrattualmente
- Portabilità dei dati: il fornitore si impegna a restituire tutti i dati in formato aperto e interoperabile entro un termine definito (es. 30 giorni) dalla fine del contratto
- Cancellazione sicura: i dati non restituiti devono essere distrutti in modo irreversibile con attestazione documentata
- Consegna del software: per sviluppi ad hoc, il contratto deve prevedere la consegna di tutti i rilasci sviluppati alla data di risoluzione, se i pagamenti relativi sono stati corrisposti
- Continuità operativa in caso di cessazione del rapporto: clausola di custodia del codice presso terzo fidato; obbligo del fornitore di cooperare nel trasferimento a nuovo fornitore
- Proroga tecnica: in caso di risoluzione anticipata, garantire un periodo transitorio minimo (es. 6 mesi) per la migrazione

Sezione 6

GDPR e AI Act: un'applicazione coordinata nella supply chain

Trattamento dei dati personali nella supply chain IA: i punti critici

- I sistemi IA per la PA trattano dati di utenti, dipendenti, imprese: la base giuridica del trattamento deve essere identificata prima del deploy
- Minimizzazione: i dati di addestramento e inferenza devono essere limitati al minimo necessario; dati anonimi sono preferibili ove possibile
- La valutazione d'impatto (DPIA) è obbligatoria quando il trattamento tramite IA comporta rischio elevato (art. 35 GDPR): profilazione su larga scala, uso di categorie speciali, sorveglianza sistematica
- La DPIA deve essere effettuata prima del deploy del sistema; il fornitore collabora fornendo le informazioni tecniche necessarie
- Trasferimento dati extra-UE: se il fornitore o i suoi sub-fornitori sono extra-UE, servono garanzie specifiche (SCCs, BCRs, decisioni di adeguatezza)
- Tempi di conservazione: i dati trattati dal sistema IA devono avere retention policy definite, coerenti con le finalità istituzionali

Le decisioni automatizzate e il diritto all'opposizione (art. 22 GDPR)

- Art. 22 GDPR: l'interessato ha il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici significativi
- **Implicazione per l’ente: nessun provvedimento amministrativo con effetti su diritti o obblighi degli utenti può essere adottato esclusivamente tramite sistema IA**
- La Legge n. 132/2025 ribadisce l'obbligo di supervisione umana nelle decisioni PA con effetti giuridici (artt. 7, 11, 13, 14, 15)
- Il fornitore deve implementare strumenti tecnici che permettano la supervisione umana: interfaccia di revisione, possibilità di override, audit trail della decisione
- Obbligo informativo: l’ente deve comunicare agli utenti quando un sistema IA contribuisce a una decisione che li riguarda
- Il contratto deve prevedere che il fornitore supporti tecnicamente l’ente nell'implementazione di questi obblighi di trasparenza

Data breach e gestione degli incidenti nella supply chain IA

- Il fornitore IA è Responsabile del trattamento: ha l'obbligo di notificare all’ente qualsiasi violazione dei dati senza ingiustificato ritardo
- Termine contrattuale consigliato: notifica al Titolare (ente universitario) entro 24-48 ore dalla scoperta dell'incidente (anticipare la finestra di 72h verso il Garante)
- Il fornitore deve cooperare attivamente: analisi tecnica dell'incidente, misure di contenimento, documentazione per la notifica ex artt. 33-34 GDPR
- Per sistemi ad alto rischio: l'incidente va valutato anche alla luce dell'art. 73 AI Act (segnalazione alle autorità di vigilanza)
- Il contratto deve prevedere: procedure di escalation, responsabilità per i costi di gestione incidente, penali per notifica tardiva
- L’ente deve mantenere un registro interno degli incidenti relativi ai sistemi IA, come parte della documentazione di accountability

DPIA vs FRIA: due valutazioni da coordinare

DPIA (art. 35 GDPR)

- **Focus: rischi per i diritti delle persone fisiche in quanto titolari di dati personali**
- **Quando: trattamenti ad alto rischio (profilazione, categorie speciali, sorveglianza)**
- **Chi: Titolare del trattamento (Ente), con supporto del DPO**
- **Output: misure tecniche e organizzative per ridurre il rischio privacy**
- **Consultazione Garante: nei casi di rischio residuo elevato non mitigabile**

FRIA (art. 27 AI Act)

- **Focus: impatto del sistema IA sui diritti fondamentali (non solo privacy)**
- **Quando: sistemi ad alto rischio prima della messa in esercizio**
- **Chi: deployer pubblici obbligatoriamente; deployer privati per alcune categorie**
- **Output: misure per mitigare rischi su non discriminazione, accesso a servizi, dignità**
- **Comunicazione: all'Autorità di vigilanza AI nazionale e, ove applicabile, al Garante**

Sezione 7

Requisiti tecnici come leve giuridiche contrattuali

Sicurezza informatica come requisito di conformità AI Act e GDPR

- Art. 32 GDPR: misure tecniche e organizzative adeguate al rischio (pseudonimizzazione, cifratura, resilienza, ripristino, test periodici)
- AI Act, art. 15: i sistemi IA ad alto rischio devono essere resilienti rispetto a tentativi di manipolazione, avvelenamento dei dati, attacchi adversarial machine learning
- NIST AI RMF: framework di riferimento per la valutazione e gestione dei rischi di sicurezza specifici dei sistemi IA
- La sicurezza deve essere valutata in modo olistico: modello IA, API, interfacce, infrastruttura cloud, dati di addestramento e inferenza, supply chain software
- Il fornitore deve descrivere nel contratto le misure di sicurezza adottate e i livelli di servizio garantiti (SLA di sicurezza)
- Per sistemi ad alto rischio: richiesta di metriche quantitative di accuratezza, robustezza e disponibilità del sistema

Clausole contrattuali di sicurezza: cosa esigere dal fornitore

- Misure di sicurezza specificate: cifratura in transito e a riposo, controllo degli accessi, autenticazione forte, segregazione degli ambienti
- Penetration testing e vulnerability assessment: il fornitore deve eseguire test periodici e condividere i risultati con l'ente su richiesta
- Business continuity e disaster recovery: RTO (Recovery Time Objective) e RPO (Recovery Point Objective) definiti contrattualmente
- Gestione delle patch e aggiornamenti di sicurezza: il fornitore si impegna a rilasciare aggiornamenti critici entro tempi definiti
- Monitoraggio continuo: strumenti SIEM, rilevazione anomalie, alerting in caso di accessi sospetti o comportamenti del sistema fuori norma
- Audit di sicurezza: diritto dell'ente di commissionare o richiedere audit di sicurezza periodici al fornitore

La gestione dei log come strumento di governance

- I log di sistema sono la memoria dell'IA: registrano input, output, decisioni, accessi, anomalie. Sono essenziali per l'accountability
- AI Act, art. 12: i sistemi ad alto rischio devono garantire logging automatico degli eventi rilevanti per l'intero ciclo di vita
- GDPR, art. 5 e 24: la tenuta dei log è strumento di accountability del Titolare: dimostrare la conformità nel tempo
- Clausola contrattuale: il fornitore garantisce accesso ai log su richiesta dell’ente per: gestione incidenti, verifiche di sicurezza, adempimenti normativi, ispezioni del Garante
- Conservazione: i log devono essere conservati per un periodo definito contrattualmente, coerente con il regime di responsabilità applicabile
- Consegna a fine contratto: il fornitore consegna i log all’ente alla scadenza del contratto, nei formati e con le modalità concordate

SEZIONE 8

Obbligo normativo e leva di governance operativa

La supervisione umana: diritto, obbligo e scelta di design (AI Act, art. 14)

- L'AI Act, all'art. 14, richiede che i sistemi IA ad alto rischio siano progettati per consentire una supervisione umana efficace durante il loro utilizzo
- La Legge n. 132/2025 estende questo principio all'uso dell'IA nella PA italiana: nessuna decisione con effetti giuridici può essere esclusivamente automatizzata
- L’ente esclude sistemi che producano decisioni automatizzate senza adeguata supervisione, validazione e responsabilità umana
- Principio complementare: preferenza per sistemi IA interpretabili (no black box); i sistemi black box possono essere usati solo come ausilio all'analisi umana
- Il contratto deve specificare quali strumenti tecnici il fornitore implementa per consentire la supervisione: interfacce di revisione, override

Livelli di supervisione umana: approccio graduato per classe di rischio

- **Alto rischio / Decisioni automatizzate**

  Supervisione strutturata: interfacce uomo-macchina, possibilità di ignorare/revocare l'output, arrestare il sistema in sicurezza, interpretare e indicare la decisione alternativa. Audit trail complete

- **Rischio limitato**

  Facoltà di intervento: capacità dell'operatore di interpretare l'output, decidere di non utilizzarlo o annullarlo. Formazione obbligatoria degli utenti

- **Rischio minimo**

  Monitoraggio delle anomalie: l'operatore può osservare i comportamenti del sistema e segnalare irregolarità. Nessun obbligo specifico di supervisione, ma buone pratiche

Formazione del personale come requisito di governance

- L'AI Act, art. 4: i fornitori e i deployer adottano misure volte a sostenere lo sviluppo dell'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
- L’ente si impegna a formare il proprio personale sotto il profilo etico, giuridico e tecnico
- Obiettivo della formazione: capacità di identificare imprecisioni, bias, output non corretti; valutazione critica degli output in relazione al contesto
- Il fornitore deve garantire formazione sull'utilizzo corretto del sistema: capacità, limiti, casi d'uso appropriati, modalità di escalation in caso di anomalie
- KPI di formazione: percentuale del personale formato, test di verifica, aggiornamenti periodici, registro delle attività formative
- La formazione è anche uno strumento di liability management: il personale formato riduce il rischio di uso improprio che ricade sull’ente

Sezione 9

KPI, verifiche periodiche e gestione del ciclo di vita

Il diritto di audit nella supply chain IA: come contrattualizzarlo

- Il diritto di audit è una delle leve più potenti della governance contrattuale: consente all'ente di verificare in concreto la compliance del fornitore
- Art. 28, par. 3, lett. h) GDPR: il Responsabile del trattamento si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie e a consentire audit
- Tipologie di audit previste: ispezioni documentali, verifiche tecniche, audit di sicurezza, accesso ai log, revisione dei processi del fornitore
- Il contratto deve precisare: frequenza (almeno annuale), preavviso (es. 15 giorni per audit ordinari, immediato per incidenti), oggetto, limitazioni (codice sorgente proprietario escluso salvo sviluppo ad hoc)
- Costi: di norma a carico del fornitore per le verifiche ordinarie; a carico dell'ente per audit straordinari, salvo evidenza di non conformità
- Il risultato degli audit deve essere documentato e conservato come prova di accountability

KPI per il monitoraggio delle performance dei sistemi IA

L'adozione di KPI è raccomandata dalle Linee Guida per monitorare l'efficacia e la conformità dei sistemi IA nel tempo

- **KPI di accuratezza**
  Tasso di errore/allucinazioni; percentuale di output corretti; confronto con benchmark dichiarati dal fornitore

- **KPI di disponibilità**
  Uptime del sistema; tempi di risposta; SLA rispettati; numero di interruzioni del servizio

- **KPI di sicurezza**
  Numero di incidenti di sicurezza; tempi di notifica; patch applicate entro i termini contrattualizzati

- **KPI di compliance**
  Audit completati; rilievi risolti entro termine; formazione del personale aggiornata

- **KPI di supervisione umana**
  Percentuale di output sottoposti a revisione umana; numero di override effettuati; tempo medio di revisione

La gestione del ciclo di vita: aggiornamenti, modifiche e fine rapporto

- I sistemi IA evolvono continuamente: aggiornamenti del modello, nuovi dataset, modifiche alle funzionalità possono alterare le caratteristiche di conformità inizialmente certificate
- Il contratto deve prevedere: obbligo del fornitore di notificare modifiche sostanziali al sistema; diritto dell'ente di richiedere una nuova valutazione di conformità
- Aggiornamenti normativi: il fornitore si impegna ad adeguare il sistema ai requisiti normativi che entrano in vigore durante la durata del contratto
- Fine rapporto: il contratto deve disciplinare le modalità di dismissione del sistema, incluse la cancellazione sicura dei dati e la documentazione finale
- Monitoraggio post-commercializzazione: per sistemi ad alto rischio sviluppati dall'ente come fornitore, va istituito un sistema di monitoraggio ex art. 72 AI Act
- Il fornitore deve comunicare proattivamente qualsiasi vulnerabilità scoperta nel sistema, anche dopo la consegna

Sezione 10

Strumento pratico per la gestione della supply chain IA

Checklist pre-contrattuale: cosa verificare PRIMA di accettare

☑ Il sistema IA è stato classificato secondo la tassonomia dell'AI Act (vietato / alto rischio / limitato / minimo)?

☑ Per sistemi ad alto rischio: è stata condotta la FRIA e la DPIA prima del deploy?

☑ Il fornitore ha accettato di firmare l'atto di nomina a Responsabile del trattamento ex art. 28 GDPR?

☑ Il contratto include il divieto esplicito di uso dei dati per addestramento di altri sistemi IA?

☑ Sono definiti i KPI di accuratezza, disponibilità e sicurezza con penali per il mancato rispetto?

☑ Sono presenti clausole di exit strategy, portabilità dei dati e cancellazione sicura?

☑ La proprietà intellettuale degli output e del codice sviluppato ad hoc è chiaramente attribuita all’ente?

Checklist contrattuale: clausole essenziali da verificare

- ☑ Definizione di Titolare, Responsabile, sub-responsabili e rispettivi obblighi
- ☑ Descrizione tecnica del sistema, tecnologie di terze parti, aggiornamenti previsti
- ☑ Limitazione delle finalità del trattamento; divieto di uso dati per training
- ☑ Procedure di data breach: tempi di notifica (< 48h), cooperazione, documentazione
- ☑ Diritto di audit con specificazione di durata, frequenza e costi
- ☑ Accesso ai log su richiesta e consegna a fine contratto
- ☑ Obblighi di supervisione umana in relazione alla classe di rischio
- ☑ Penali specifiche per violazione delle clausole AI-specific (non solo le penali generali)

Checklist post-contrattuale: il monitoraggio continuo

- ☑ Il fornitore è stato formalmente designato Responsabile del trattamento con atto firmato?
- ☑ La DPIA e/o FRIA sono state completate e archiviate prima del go-live?
- ☑ Il personale dell’ente coinvolto ha ricevuto formazione sull'utilizzo del sistema?
- ☑ I KPI sono monitorati e i risultati sono documentati periodicamente?
- ☑ Sono stati effettuati gli audit periodici previsti contrattualmente?
- ☑ In caso di aggiornamento sostanziale del sistema: nuova valutazione di conformità effettuata?
- ☑ Il registro dei trattamenti dell’ente è stato aggiornato con il nuovo sistema IA?

Sezione 11

Aspetti trasversali della supply chain IA responsabile

Trasparenza nella supply chain IA: obblighi verso gli utenti

- Il principio di trasparenza dell'AI Act (art. 50) obbliga i deployer a informare gli utenti quando interagiscono con un sistema IA
- Contenuto dell'informativa: tipologia di sistema IA, finalità, capacità e limiti, logica di funzionamento, diritti esercitabili
- Per sistemi che influenzano decisioni: spiegazione del peso dell'IA nella decisione finale, dati utilizzati, criteri applicati
- Contenuti artificiali: testi, immagini, video generati da IA devono essere chiaramente etichettati (art. 50 AI Act)
- Deepfake: obbligo di disclosure quando un sistema genera contenuti audiovisivi artificiali che simulano persone reali
- Il fornitore deve implementare tecnicamente le funzionalità di disclosure: il contratto deve specificare come e dove vengono mostrate le informazioni agli utenti finali

Bias e non discriminazione: una responsabilità di governance della supply chain

- I bias algoritmici possono generare discriminazioni sistematiche in decisioni istituzionali: reclutamento, accesso a servizi, valutazioni
- Tre tipologie di bias rilevanti: nei dati (dataset non rappresentativi), algoritmici (scelte di design), umani (pregiudizi nella progettazione)
- L’ente si impegna a promuovere l'utilizzo di dati di qualità elevata, affidabili, equi e rappresentativi di tutta la popolazione interessata
- Il fornitore deve documentare la provenienza legittima dei dataset di addestramento (art. 53 AI Act) e la politica di gestione del bias
- Clausola contrattuale: il fornitore si impegna a condurre test di bias periodici e a comunicare i risultati all’ente
- Misura correttiva: in caso di bias documentati, il fornitore ha l'obbligo contrattuale di adottare misure correttive entro un termine definito

Sostenibilità e impatto ambientale dell'IA: una leva emergente

- Il training e l'inferenza di modelli IA di grandi dimensioni hanno un impatto energetico e ambientale significativo
- Il Piano Triennale ICT PA 2024-2026 include l'efficienza energetica come criterio di valutazione dei sistemi IA adottati dalla PA
- Le Linee Guida dell’ente prescrivono che i sistemi IA siano utilizzati secondo un approccio sostenibile, attento alla tutela ambientale
- Criterio di selezione del fornitore: politica di sostenibilità del fornitore, utilizzo di energie rinnovabili nell'infrastruttura cloud
- Clausola contrattuale: il fornitore si impegna a fornire informazioni sul consumo energetico del sistema e ad adottare misure di efficienza progressiva
- L'integrazione del criterio di sostenibilità nelle valutazioni di fornitura IA è coerente con i principi del Green Public Procurement

Segnalazioni interne e meccanismi di reclamo nella governance IA

- L'AI Act (art. 20) richiede che i fornitori e i deployer istituiscano meccanismi per segnalare rischi relative ai sistemi IA ad alto rischio
- Strumenti minimi: canale dedicato per segnalazioni del personale, procedura di escalation interna, gestione documentata delle segnalazioni
- Collegamento con D.Lgs. 24/2023 e la Direttiva (UE) 2019/1937 (whistleblowing): le segnalazioni relative a violazioni nella gestione dei sistemi IA rientrano nell'ambito di applicazione del decreto art. 87 AI Act)
- Il contratto con il fornitore deve prevedere: obbligo di comunicare proattivamente anomalie del sistema, vulnerabilità scoperte, comportamenti imprevisti
- La gestione dei reclami degli utenti finali (es. utenti del servizio che contestano una decisione IA) è responsabilità dell’ente: il fornitore fornisce supporto tecnico
- Tracciabilità: ogni segnalazione e relativa azione correttiva deve essere documentata nel registro di governance IA

Interoperabilità e standard tecnici nella supply chain IA

- Il Codice dell'Amministrazione Digitale (art. 68, D.Lgs. 82/2005) impone alle PA l'utilizzo di standard aperti e l'adozione di formati interoperabili
- L'interoperabilità è anche una leva di governance della supply chain: sistemi proprietari chiusi aumentano il lock-in e riducono la capacità di audit
- Criteri tecnici da includere nelle specifiche di fornitura: API documentate e standardizzate, formati dati aperti (JSON, XML, CSV), documentazione del modello in formato standardizzato
- Il Piano Triennale PA 2024-2026 e le Linee Guida AGID indicano l'interoperabilità come requisito per i sistemi IA adottati dalla PA
- Clausola contrattuale: il fornitore garantisce che il sistema sia conforme agli standard di interoperabilità definiti da AGID e dal Piano Triennale
- L'interoperabilità facilita la portabilità e la sostituzione del fornitore: è quindi sia un requisito tecnico che una leva strategica della supply chain

Sezione 12

Le dieci leve per una supply chain IA responsabile

Le dieci leve per una supply chain IA responsabile

- 1. Classificare il rischio prima di ogni altra cosa: la tassonomia AI Act determina tutto il regime applicabile
- 2. Trattare la supply chain IA come un ecosistema regolato, non come una fornitura ordinaria
- 3. Contrattualizzare specificamente: clausole generali non sono sufficienti; servono clausole AI-specific e GDPR-specific
- 4. Adottare le MCC-AI come template di riferimento, modulandole in base al rischio del sistema
- 5. Esigere trasparenza tecnica: documentazione, log, metriche, test — non solo dichiarazioni
- 6. Garantire supervisione umana effettiva, non solo formale: strumenti tecnici, formazione, processi
- 7. Tutelare i dati personali per tutta la supply chain: dall'addestramento all'output, dal deploy alla dismissione
- 8. Pianificare l'exit dall'inizio: portabilità, cancellazione sicura, continuità operativa
- 9. Monitorare continuamente: KPI, audit, aggiornamenti normativi, incidenti
- 10. Documentare tutto: l'accountability non è solo compliance ma protezione istituzionale

Il ruolo strategico del DPO, RGD e del RTD nella governance IA

- Le Linee Guida dell'ente affidano la governance IA a un tandem istituzionale: RTD (Responsabile Transizione Digitale), RGD (Responsabile gestione documentale) e DPO (Responsabile Protezione Dati)
- RTD: coordina la strategia IA, monitora il Piano di integrazione, gestisce le risorse e le responsabilità per i singoli progetti
- DPO: valuta i rischi per diritti fondamentali e protezione dei dati; collabora con RTD nelle misure di contenimento; punto di contatto con il Garante
- RGD: verifica qualità, integrità e contest di dati, informazioni e documenti
- Questa governance a tre teste rispecchia la triplice natura del rischio IA: tecnico-organizzativo (RTD), giuridico-privacy (DPO), archivistico (RGD)
- Raccomandazione operativa: istituire un Comitato IA interno con RTD, DPO, responsabili degli uffici utenti, responsabile gestione documentale e consulente legale esterno
- Il Comitato IA supervisiona: due diligence fornitori, approvazione contratti, gestione incidenti, revisione periodica del portafoglio IA

Responsabilità e sanzioni: il rischio di non governance

- AI Act: sanzioni amministrative fino a € 35 milioni o il 7% del fatturato mondiale annuo (per violazioni gravi); fino a € 15 milioni o 3% per altri obblighi
- GDPR: sanzioni fino a € 20 milioni o il 4% del fatturato mondiale annuo; applicabili anche alle PA italiane tramite il Garante
- Responsabilità civile ex AI Act (direttiva sulla responsabilità IA): il deployer può essere ritenuto responsabile dei danni causati da sistemi IA che non ha adeguatamente governato
- Responsabilità dirigenziale nella PA: i dirigenti che autorizzano l'adozione di sistemi IA senza adeguata governance, ve ne ricorrano i presupposti possono rispondere di danno erariale
- Rischio reputazionale: l'uso non trasparente di IA nella PA genera diffidenza degli utenti e rischio di contenzioso amministrativo
- La non governance della supply chain IA non è una scelta neutrale: è una scelta attiva di esposizione al rischio

Responsabilità: le novità del D.Lgs. 160/2026

1. Nasce il reato di "omessa adozione di misure di sicurezza nei sistemi di IA" (art. 437-bis c.p.)

Non basta dotarsi di un sistema certificato: chi omette le misure tecniche o di sorveglianza umana necessarie a prevenire malfunzionamenti **risponde penalmente se ne deriva pericolo per la vita o l'incolumità pubblica** (reclusione da 1 a 5 anni, fino a 8 se il pericolo riguarda la sicurezza dello Stato).

La norma colpisce esplicitamente anche l'utilizzatore (deployer) professionale che omette intenzionalmente la sorveglianza umana — non solo chi progetta o immette sul mercato il sistema.

Corollario automatico: l'art. 25-vicies del D.Lgs. 231/2001 estende questa responsabilità agli enti, con sanzioni pecuniarie fino a 1.000 quote e sanzioni interdittive.

Responsabilità: le novità del D.Lgs. 160/2026

2. Inversione dell'onere della prova sul piano della responsabilità civile

L'art. 18 introduce una **presunzione del nesso di causalità**: se il **danno - contrattuale o extracontrattuale** - deriva dalla **violazione di un obbligo** previsto dall'AI Act, **il nesso di causalità tra violazione e danno si presume**, salvo prova contraria a carico del convenuto.

A questo si somma l'art. 17 (**Accesso alle prove**), che consente al danneggiato di ottenere l'esibizione giudiziale di registri di log, documentazione sul sistema di gestione dei rischi e informazioni sulla supervisione umana — un vero meccanismo di discovery mirato al funzionamento interno del sistema di IA.

Inoltre, il danneggiato gode di maggiori tutele effettive derivanti dalla possibilità di esperire un'azione diretta per il risarcimento del danno nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile al convenuto (art.20).

Responsabilità: le novità del D.Lgs. 160/2026

3. La certificazione non è uno scudo

L’art. 19 lo dice espressamente: la conformità al Regolamento IA, anche se certificata, non esclude di per sé la responsabilità. Avere la marcatura CE o la documentazione tecnica in regola è condizione necessaria, non sufficiente.

Cosa significa in pratica per un’organizzazione deployer

Il legislatore ha spostato il baricentro della responsabilità **dalla mera conformità documentale alla capacità dimostrabile di governare il sistema nel tempo**: sorveglianza umana tracciata, gestione dei rischi documentata, log immutabili e conservati, valutazioni d’impatto aggiornate.



In caso di contenzioso, sarà fondamentale per le organizzazioni dimostrare di aver costruito un solido sistema di governance della compliance in tema di AI, capace di produrre le prove della propria accountability.

Principio delle Linee Guida Camera di Commercio MI, 2026

> ***La trasparenza e la responsabilità sono fondamentali nella gestione pubblica dell'intelligenza artificiale: esse costituiscono le condizioni di legittimità dell'azione amministrativa.***

La supply chain è il luogo dove questi principi si traducono in obblighi concreti e verificabili.

Sezione 13

Roadmap di implementazione

Roadmap di implementazione: le priorità immediate

- **Fase 1— Inventario e classificazione**

  Mappare tutti i sistemi IA adottati o in fase di adozione; classificare il rischio; identificare i fornitori della supply chain

- **Fase 2 — Valutazioni d'impatto**

  Condurre DPIA e FRIA per i sistemi ad alto rischio; documentare i risultati; adottare misure correttive

- **Fase 3 — Governance contrattuale**

  Aggiornare i contratti esistenti con clausole AI-specific; predisporre template contrattuali per nuove forniture; aggiornare il modello di nomina ex art. 28 GDPR

- **Fase 4— Formazione e KPI**

  Formare il personale; implementare sistema di monitoraggio KPI; istituire il Comitato IA interno; effettuare il primo ciclo di audit

Schema: dalla norma alla clausola contrattuale

- **AI Act, art. 9 → Gestione del rischio**
  Clausola: il fornitore implementa e mantiene un sistema di gestione del rischio; fornisce supporto per la classificazione
- **GDPR, art. 28 → Responsabile del trattamento**
  Clausola: atto di nomina con obblighi specifici; divieto uso dati per finalità proprie o addestramento
- **AI Act, art. 12 → Logging**
  Clausola: registrazione automatica eventi; accesso su richiesta; consegna a fine contratto
- **AI Act, art. 14 → Supervisione umana**
  Clausola: strumenti tecnici di supervisione graduati per classe di rischio; formazione personale
- **AI Act, art. 15 + GDPR art. 32 → Sicurezza**
  Clausola: misure di sicurezza dettagliate; SLA; business continuity; audit periodici
- **AI Act, art. 27 → FRIA**
  Clausola: il fornitore collabora e fornisce documentazione tecnica per la FRIA pre-deploy

Obblighi contrattuali per classe di rischio: sintesi operativa

- **TUTTI i sistemi IA**

  Nomina Responsabile ex art. 28 GDPR · Divieto uso dati per addestramento · Clausola di cybersicurezza · Divieto sistemi vietati ex art. 5 AI Act

- **Rischio LIMITATO (aggiuntivi)**

  Disclosure automatizzata verso utenti · Marcatura contenuti generativi (art. 50 AI Act) · Facoltà di supervisione e override

- **Rischio ALTO (aggiuntivi)**

  FRIA obbligatoria pre-deploy · Gestione del rischio ex NIST AI RMF · Logging automatico completo · Supervisione strutturata · Metriche accuratezza/robustezza · Supporto rafforzato fornitore

- **GPAI – Modelli uso generale (aggiuntivi)**

  Documentazione dataset addestramento (art. 53) · Registrazione database UE · Policy uso accettabile

CONCLUSIONI

Una supply chain AI necessita di governance integrata

DIGEAT FESTIVAL

ARCHIVI DIGITALI
PROTEZIONE DATI
IA E REGOLE DEL FUTURO





io, umano

giorni di un futuro pass

5/8 NOVEMBRE 2026

LECCE/GALLIPOLI

DIGITALAW



I misteri dell'orizzonte (*Les mystères de l'horizon*)
René Magritte (1955)

GRAZIE PER
L'ATTENZIONE

andrealisi@studiolegalelisi.it

Una volta che sei diventato maestro in una cosa, diventa subito allievo in un'altra

(G.Hauptmann)

PROCEDAMUS©
PRISMA