

A.I.



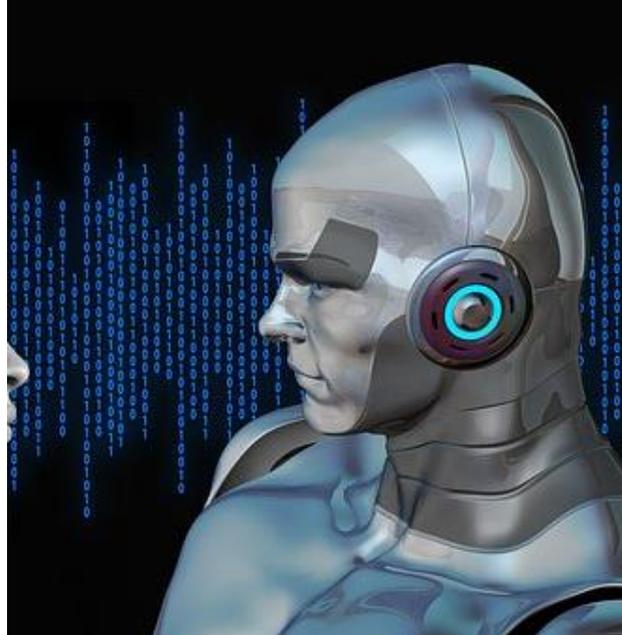
*«As soon as it works no
one calls it A.I. anymore»*

John McCarthy

(Boston 1927 – Stanford 2011)

He coined the term Artificial
Intelligence in 1956





PROPOSTA DI
REGOLAMENTO DI NORME
ARMONIZZATE PER ALCUNI
SISTEMI DI **A.I.**

Bruxelles 21.4.2021
Uno scopo e molte cautele

L'OBIETTIVO UE

l'obiettivo che si è posta ufficialmente la Commissione è quello di garantire alla UE di **promuovere** normativamente e, soprattutto, **per prima**, l'uso di alcune **tecnologie per accrescere il benessere economico generale** (c. 2) **al contempo** facendo in modo che i cittadini ne possano beneficiare **nel rispetto dei diritti fondamentali** degli stessi, così come previsti dalla Carta di Nizza (CDFUE).



Le esplicite ragioni della proposta

“L’A.I. è una **famiglia di tecnologie** in rapida evoluzione che può portare un'ampia gamma di **vantaggi economici e sociali** migliorando la **previsione, ottimizzando le operazioni** e **l'allocazione delle risorse** e **personalizzando l'erogazione dei servizi**, l'uso dell'intelligenza artificiale può supportare risultati **benefici sociali, ambientali** e fornire **vantaggi competitivi** chiave alle aziende e **all'economia** europea.

La proposta tiene conto della risoluzione del Parlamento europeo nel pieno rispetto dei principi di **proporzionalità, sussidiarietà** e del **legiferare meglio**.

La **Commissione** propone il quadro normativo in base a **4 obiettivi specifici**:

1. garantire che i sistemi di A.I. immessi sul mercato UE siano sicuri e rispettino la legislazione esistente sui diritti fondamentali e i valori dell'Unione;
2. garantire la **certezza del diritto per facilitare gli investimenti e l'innovazione** nell’A.I.;
3. migliorare la governance e l'effettiva applicazione della legislazione esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di A.I.;
4. facilitare lo **sviluppo di un mercato** unico e **prevenirne la frammentazione”**.



Un lungo percorso di studi e di consultazioni (l'etica, il mercato e la scienza)

I temi e problemi dibattuti nel corso degli ultimi anni:

- potere debordante della A.I.
- rapporto tra benefici e rischi non ben calibrato
- innovazione e utilità sociale in secondo piano rispetto al tema economico
- 2017: risoluzione del Parlamento UE sulla possibilità di attribuire personalità giuridica alla A.I. (un tema abbandonato?)
- rischi di discriminazione
- scarsa distinzione tra A.I. destinata alle cose e alle persone
- attivazione dell'A.I. poco controllabile
- A.I., lavoratori e luoghi di lavoro
- A.I., minori e persone fragili ...



ALCUNI TEMI INGOMBRANTI POCO PRESENTI NELL'ELABORAZIONE GIURIDICA

A.I. QUALE ESPRESSIONE “MODERNA” DELLA TECNICA

- L'uomo è essenzialmente tecnico
- Oggi il genere umano vive la tecnica
- Il controllo della tecnica pretende competenze elevate
- È la tecnica che fa mondo: l'etica “implora” la tecnica
- La tecnica non è più un mezzo ma è scopo (?)
- L'incremento della marginalizzazione umana è inevitabile
- L'A.I. comprime le possibilità dei molti di ribellarsi ai pochi
- L'A.I. può incrementare il c.d. «*no making power*» (?)
- Le prove e gli errori della scienza non giungono al vero
- La scienza porta all'esatto in base a presupposti variabili

UN INEVITABILE “ERRORE” DI FONDO?

(IL SOLITO?)

L'idea di imporre il Regolamento (peraltro a livello globale) in base alla leva del mercato e della razionalità che lo governa non pare **considerare tre elementi centrali:**

1. la **forza centripeta** della **tecnica**
2. Il fatto che le **leggi della razionalità tecnica** sono superiori a quelle del mercato
3. la circostanza che la **tecnica si impone da sé** poiché quando c'è e funziona si usa





89 Considerando

85 **Articoli** suddivisi in **XII Titoli**

9 ALLEGATI:

- **I - TECNICHE E APPROCCI DI INTELLIGENZA ARTIFICIALE**
- **II - ELENCO DELLA LEGISLAZIONE DI ARMONIZZAZIONE DELL'UNIONE;**
- **III - SISTEMI AI AD ALTO RISCHIO** DI CUI ALL'ART. 6, PAR. 2;
- **IV - DOCUMENTAZIONE TECNICA** (di cui all'art. 11, par. 1);
- **V - DICHIARAZIONE DI CONFORMITÀ UE;**
- **VI - PROCEDURA DI VALUTAZIONE CONFORMITÀ BASATA SUL CONTROLLO INTERNO;**
- **VII - CONFORMITÀ BASATA SULLA VALUTAZIONE DELLA GESTIONE DELLA QUALITÀ SISTEMA E VALUTAZIONE DELLA DOCUMENTAZIONE TECNICA;**
- **VIII - INFORMAZIONI DA PRESENTARE AL MOMENTO DELLA REGISTRAZIONE DEI SISTEMI IA AD ALTO RISCHIO A NORMA DELL'ART. 51;**
- **IX - LEGISLAZIONE DELLA UE SUI SISTEMI INFORMATICI SU LARGA SCALA NEL SETTORE LIBERTÀ, SICUREZZA E GIUSTIZIA**

I sistemi A.I. ad alto rischio (art. 6)

È in generale considerato ad **alto rischio** il sistema A.I.:

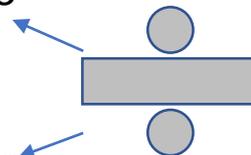
- destinato ad essere utilizzato come componente di sicurezza di prodotti soggetti a valutazione della conformità secondo la normativa di armonizzazione dell'UE elencata nell'**allegato II** (es. **componenti di sicurezza di dispositivi medici, ascensori, giocattoli**);
- previsto dall'**allegato III. (b) 1. 2** (es. i sistemi di A.I. da utilizzare per la **selezione del personale**, per valutare la **solvibilità delle persone**, i sistemi di **polizia predittiva**).



La proposta di Regolamento **cosa stabilisce in generale?**

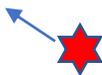
(Art. 1)

- a) **norme armonizzate** per l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA nella UE (per **tutte le AI**); **divieti** di alcune pratiche di IA;
- b) **requisiti specifici** (solo) per sistemi di **IA** ad **alto rischio** e **obblighi** per gli operatori di tali sistemi;
- c) **regole di trasparenza** armonizzate per i sistemi di **IA** destinati a **interagire** con **persone fisiche**, sistemi di **riconoscimento delle emozioni** e sistemi di **categorizzazione biometrica** e di IA utilizzati per generare o manipolare contenuti di **immagini, audio** o **video**;
- d) **norme in materia di monitoraggio** e **sorveglianza** del mercato.



Cosa intende per A.I. la bozza di Regolamento e quando si applica?

Un sistema di A.I. è definito come “**software**” di **basso, medio o elevato rischio**, «*sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I e che può, per una data serie di obiettivi definiti dall'uomo, generare risultati quali contenuti, previsioni, raccomandazioni, o decisioni che influenzano gli ambienti con cui interagiscono*» (art. 3).



Il Regolamento si applica ad alcuni di tali sistemi in sede di **progettazione** e **sviluppo**; in fase di **immissione** sul mercato; in fase di **messa in funzione**; quando **usati**; rispetto alla **conseguente** (previste o non) che possono causare (art. 2).

NB: i sistemi AI ad alto rischio sono quelli a cui il Reg. dedica la più parte delle proprie disposizioni e dei requisiti di protezione ivi previsti.

- **Approcci di apprendimento automatico**, inclusi supervisione, sistema non supervisionato e di rinforzo apprendimento che utilizza un'ampia varietà di metodi tra cui l'apprendimento profondo;
- **approcci basati sulla logica e sulla conoscenza**, compresa la rappresentazione della conoscenza, programmazione induttiva (logica), basi di conoscenza, inferenza e motori deduttivi, ragionamento (simbolico) e sistemi esperti;
- **approcci statistici**, stima bayesiana (stima di gradi di probabilità), metodi di ricerca e ottimizzazione.

Approccio basato sul rischio (piramide di Heinrich)



Rischio non accettabile: A.I. vietata (*social scoring, punteggi*)

Rischio alto: A.I. **permessa** ma soggetta a requisiti e ad una valutazione della conformità ex ante (reclutamento, dispositivi medici, infrastrutture)

Specifici rischi legati alla trasparenza: A.I. **permessa** ma soggetta a obblighi di informazione/trasparenza (*chatbot: simulazioni di conversazioni, impersonificazioni*)

Rischi minimi o assenti: A.I. **permessa** senza particolari restrizioni (*videogame*)

La Marcatura CE per A.I. ad alto rischio

La marcatura CE indica che il sistema A.I. sarebbe conforme alla normativa UE

4 Passaggi che un Produttore o un Fornitore deve compiere per apporre la marcatura CE ad un dispositivo A.I. ad alto rischio

1

Comprendere e **determinare** se il sistema di AI è classificato ad alto rischio in base al Reg. UE

2

Garantire che la progettazione, lo sviluppo e il sistema di gestione della qualità siano conformi al Reg. UE

3

Svolgere la procedura di valutazione della conformità finalizzata a garantire in concreto la conformità



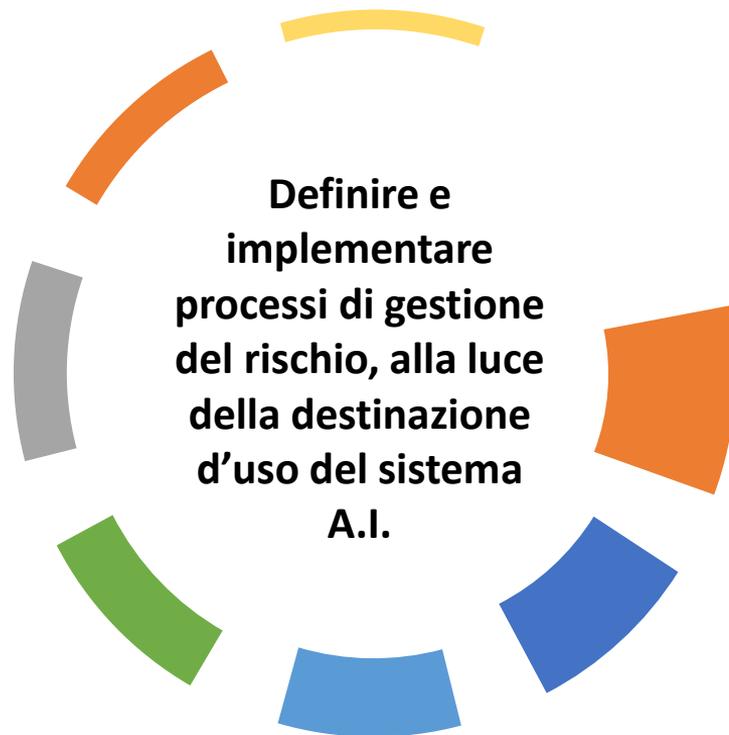
**IMMISSIONE SUL MERCATO
O
MESSA IN SERVIZIO**

4

Apporre la **marcatura CE** al sistema A.I. e sottoscrivere una dichiarazione di conformità

Requisiti (di *accountability*) per A.I. ad alto rischio (Titolo III, cap. 2)

- 1 Utilizzare **dati di alta qualità** per l'allenamento, la convalida e i test
- 2 Elaborare la **documentazione tecnica** e progettare **funzionalità per la registrazione** (tracciabilità e verificabilità)
- 3 Garantire un appropriato livello di **trasparenza** e **fornire informazioni** agli utilizzatori sulle capacità e **limiti** del sistema e su **come utilizzare** il sistema
- 4 Garantire la **supervisione umana** (misure integrate nel sistema e/o che devono essere implementate dagli utilizzatori)
- 5 Assicurare **robustezza, accuratezza, cybersicurezza**



Identificazione biometrica remota (IBR)

Utilizzo di sistemi **IBR** in tempo reale da parte delle forze dell'ordine (art. 5)

Le FF.OO non possono utilizzare i sistemi IBR in spazi accessibili al pubblico, tranne nel caso di:

- ricerca delle vittime di reato
- minaccia alla vita o all'integrità fisica o terrorismo
- reati gravi (mandato d'arresto UE)

Autorizzazione *ex ante* dell'autorità giudiziaria o dell'organo amministrativo indipendente

Immissione sul mercato di sistemi **IBR** (*real-time* ed *ex post*)

Valutazione *ex ante* della conformità da parte di terzi

Requisiti specifici:

- per funzionalità di registrazione
- **supervisione umana**

Ambito di applicazione (art. 2)

Il Regolamento **SI applica**:

- **ai fornitori** che immettono sul mercato o mettono in servizio sistemi di A.I. nell'UE, indipendentemente dal fatto che tali fornitori siano situati all'interno dell'UE o in un paese terzo;
- **agli utenti** di sistemi di A.I. situati all'interno dell'UE.

Il Regolamento **NON si applica**:

- ai sistemi di A.I. sviluppati o utilizzati SOLO per **scopi militari**;
- alle **autorità pubbliche** di un **paese terzo** e alle organizzazioni internazionali che rientrano nell'ambito di applicazione del Regolamento se esse utilizzano sistemi di A.I. nel quadro di accordi internazionali per l'applicazione della legge e la cooperazione giudiziaria con UE o con uno o più stati membri.

Alcune definizioni (art. 3)

Fornitore

Persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa un sistema di A.I. o che dispone di un sistema di A.I. sviluppato al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, sia a pagamento che a titolo gratuito

Utente

Un fornitore che è una micro o una piccola impresa ai sensi della raccomandazione della Commissione 2003/361 / CE 61

Immissione sul mercato

La prima messa a disposizione di un sistema di A.I. sul mercato UE

Messa a disposizione sul mercato

La fornitura di un sistema di A.I. per la distribuzione o l'uso sul mercato UE nel corso di un'attività commerciale, a titolo oneroso o gratuito

Dati biometrici

Dati personali risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o confermano l'identificazione univoca di tale persona fisica, come le immagini del viso o i dati dattiloscopici

Sistema di riconoscimento delle emozioni

Un sistema di AI allo scopo di identificare o inferire **emozioni o intenzioni** di persone fisiche **sulla base dei loro dati biometrici**

Sistema di classificazione biometrica

Un sistema di AI con lo scopo di **assegnare persone fisiche a categorie specifiche**, come sesso, età, colore dei capelli, colore degli occhi, tatuaggi, origine etnica o orientamento sessuale o politico, sulla base dei loro dati biometrici

Sistema di identificazione biometrica a distanza

Un sistema di AI con lo scopo di identificare persone fisiche a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento e senza che l'utente del sistema di AI abbia una conoscenza preventiva se la persona sarà presente e potrà essere identificata

**Sistema IBR
in tempo reale**

Un sistema di IBR in cui l'acquisizione di dati biometrici, il confronto e l'identificazione avvengono **senza ritardi significativi**. Ciò comprende non solo l'identificazione istantanea, ma **anche brevi ritardi** limitati onde evitare l'elusione

**Sistema IBR
*ex post***

Un sistema di IBR a distanza **diverso** da un sistema IBR in tempo reale

**Spazio accessibile al
pubblico**

Qualsiasi **luogo fisico accessibile al pubblico**, indipendentemente dal fatto che si possano applicare determinate condizioni di accesso

**Autorità incaricata
dell'applicazione
della legge**

Qualsiasi **autorità pubblica competente** per la prevenzione, l'indagine, l'individuazione o perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce alla sicurezza pubblica; o qualsiasi **altro ente o organismo** incaricato dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici ai fini della prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, compresa salvaguardia/prevenzione di minacce alla PS

Forze dell'ordine

Attività svolte dalle **autorità di contrasto** per la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce alla sicurezza pubblica



Incidente grave

Qualsiasi **incidente** che direttamente o indirettamente conduce, potrebbe aver portato o potrebbe portare a uno dei seguenti eventi:

- (a) la **morte** di una persona o gravi **danni alla salute** di una persona, alla proprietà o all'ambiente,
- (b) un'**interruzione grave e irreversibile** della **gestione** e del funzionamento di **infrastruttura critica**



Gli utilizzi vietati dell'A.I. (art. 5)

L'immissione sul mercato, la messa in servizio o l'uso di un sistema di A.I. che impiega **tecniche subliminali** al di là della coscienza di una persona al fine di **distorcere** materialmente il comportamento di una persona in un modo che provoca o è probabile che causi **danni fisici o psicologici** a quella persona o ad un'altra persona.



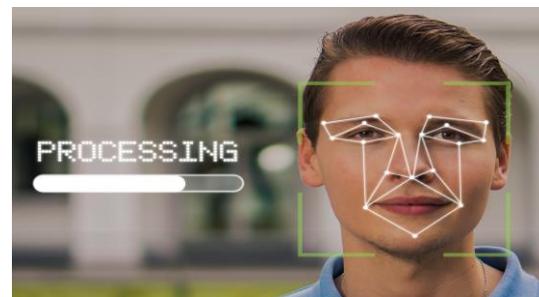
L'immissione sul mercato, la messa in servizio o l'uso di un sistema di A.I. che sfrutta una qualsiasi delle **vulnerabilità** di uno specifico gruppo di persone a causa della loro **età, disabilità fisica o mentale**, al fine di distorcere materialmente il comportamento in un modo che provochi o possa causare a quella persona o a un'altra persona **danni fisici o psicologici**.



L'immissione sul mercato, la **messaggio in servizio** o l'uso di A.I. da parte delle **autorità pubbliche**, o per loro conto, per la valutazione o la classificazione dell'affidabilità delle persone fisiche in un determinato periodo di tempo sulla base del loro comportamento sociale o della personalità nota o prevista o delle caratteristiche (c.d. sistemi di **social scoring**).



L'uso di sistemi di identificazione biometrica remota «**in tempo reale**» in **spazi accessibili al pubblico ai fini dell'applicazione della legge**. Per tale divieto sono **previste varie eccezioni** e si lascia in parte liberi gli Stati Membri di consentire e regolamentare l'uso di questo tipo di sistemi di A.I.



1. Identificazione biometrica e classificazione delle persone fisiche: a) sistemi di A.I. (SAI) destinati ad essere utilizzati per **riconoscimento biometrico da remoto "in tempo reale"** e "**post**" identificazione delle persone fisiche.

2. Gestione delle infrastrutture critiche: a) SAI destinati ad essere utilizzati come componenti di sicurezza nella gestione del **traffico stradale** e fornitura di **acqua, gas, riscaldamento** ed elettricità.

3. Istruzione e formazione professionale: a) SAI destinati ad essere utilizzati per determinare l'**accesso** o **assegnazione** di persone a **istituti di istruzione** e formazione professionale; **b)** destinati ad essere utilizzati allo scopo di **valutare gli studenti** in istituti di istruzione e formazione professionale o per **test** richiesti per l'**ammissione** agli istituti scolastici.

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: **a)** destinati ad essere utilizzati per il **reclutamento/selezione di persone**, in particolare, per posti vacanti, lo screening o le domande o la valutazione candidati nel corso di interviste o test; **b)** per **prendere decisioni** sulla **promozione e la cessazione di rapporti** connessi al lavoro, per l'assegnazione dei compiti e per il monitoraggio e valutare le prestazioni e il comportamento delle persone in tali relazioni.

5. L'accesso e il godimento dei servizi privati essenziali e dei servizi pubblici e benefici: **a)** sistemi destinati ad essere utilizzati **dalle autorità pubbliche** o per conto di autorità incaricate di valutare **l'ammissibilità delle persone fisiche all'assistenza pubblica o a vantaggi e servizi**, nonché per concedere, ridurre, revocare o recuperare tali vantaggi e servizi; **b)** destinati ad essere utilizzati per valutare **l'affidabilità creditizia** di persone o stabilire il loro punteggio di credito, con l'eccezione dei sistemi AI messi in servizio da parte di piccoli fornitori per il proprio uso; **c)** per la spedizione o per stabilire la priorità nell'invio di **servizi di pronto intervento di emergenza**, anche da parte dei vigili del fuoco e assistenza medica.

destinati ad essere utilizzati dalle **FFOO o autorità preposte**:

- a) all'applicazione della legge per valutazione individuale del rischio e al fine di valutare se una **persona fisica possa offendere** o rioffendere o il rischio per potenziali **vittime di reati**;
- b) all'applicazione della legge che, con poligrafi e strumenti simili, rilevino **lo stato emotivo di una persona** fisica;
- c) per rilevare falsi di cui all'art. 52, par. 3);
- d) per la valutazione **dell'affidabilità delle prove nel corso di indagini o procedimenti giudiziari per reati**;
- e) per **la previsione il verificarsi o il ripetersi di un reato effettivo o potenziale** sulla base della **profilazione delle persone** di cui all'art. 3, par. 4, della dir. 2016/680 o **valutazione dei tratti e delle caratteristiche della personalità o del passato comportamento criminale di persone fisiche o gruppi**;
- f) per la **profilazione di persone** fisiche di cui all'art. 3, par. 4, dir. 2016/680 nel corso di individuazione, indagine o perseguimento di reati;
- g) per **l'analisi della criminalità relativa alle persone fisiche**, consentire alle autorità preposte **di effettuare ricerche complesse correlate e non correlate a grandi insiemi di dati disponibili** in diverse origini dati o in diversi formati di dati in per identificare modelli sconosciuti o scoprire relazioni nascoste nei dati.

7. Gestione della migrazione, dell'asilo e del controllo delle frontiere: **a)** utilizzati dalle autorità pubbliche competenti, come poligrafi e strumenti simili, o per rilevare lo **stato emotivo di una persona fisica**; **b)** utilizzati dalle autorità pubbliche per **valutare un rischio**, compreso **un rischio per la sicurezza**, un **rischio di immigrazione irregolare** o un rischio per la salute di una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro; **c)** utilizzati dalle autorità pubbliche per la verifica **dell'autenticità dei documenti di viaggio** e supporto per verificare la documentazione delle persone fisiche e rilevare i documenti non autentici; **d)** destinati ad assistere le autorità pubbliche per l'esame di domande di asilo, **visti e permessi di soggiorno** e relativi reclami relativi all'ammissibilità delle persone fisiche che chiedono **asilo**.

8. Amministrazione della giustizia e processi democratici: **a)** sistemi di IA destinati ad **assistere un'autorità giudiziaria nella ricerca e interpretazione dei fatti e della legge e applicazione della legge a un insieme concreto di fatti**.

Requisiti (by design) per sistemi A.I. ad alto rischio

- deve essere stabilito, attuato, documentato e mantenuto un **sistema di gestione del rischio**, ovvero un processo iterativo continuo, che richiede un aggiornamento sistematico (art. 9);
- vi è l'obbligo di assicurarsi che i sistemi vengano sviluppati seguendo **specifici criteri qualitativi** per quanto riguarda i dati ed i modelli utilizzati (art. 10);
- la **documentazione tecnica** deve essere redatta **prima** che il sistema sia immesso sul mercato o messo in servizio, deve essere tenuta aggiornata e deve dimostrare che il sistema sia conforme ai requisiti previsti dal Regolamento (art. 11);
- i sistemi devono essere progettati e sviluppati con capacità che consentono la **registrazione automatica** degli **eventi** (art. 12);
- i sistemi devono essere progettati e sviluppati in modo tale da garantire che il loro **funzionamento** sia sufficientemente **trasparente** da consentire agli utenti di interpretare l'output del sistema e utilizzarlo in modo appropriato (art. 13);

- i sistemi devono essere **progettati e sviluppati**, anche con **strumenti di interfaccia uomo-macchina** appropriati, in modo da poter essere **efficacemente controllati dalle persone** fisiche durante il periodo in cui il sistema di A.I. è in uso (art. 14);
- i sistemi devono essere progettati e sviluppati in modo tale da raggiungere, alla luce dello scopo previsto, un **livello di accuratezza adeguato, robustezza e sicurezza informatica** e prestazioni costanti sotto questi aspetti per tutto il loro ciclo di vita (art. 15).

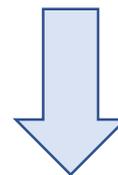


La verifica del rispetto dei requisiti avverrà attraverso
«**procedure di valutazione della conformità**»



Valutazione della conformità? (art. 19)

- **I fornitori di sistemi di A.I. ad alto rischio garantiscono che i loro sistemi siano sottoposti alla pertinente **procedura di valutazione della conformità**, prima della loro immissione sul mercato o messa in servizio;**
- per i sistemi di A.I. ad **alto rischio** di cui al punto 5, let. b), dell'allegato III (*credit scoring*) che sono immessi sul mercato o messi in servizio da fornitori che sono **enti creditizi disciplinati dalla direttiva 2013/36/UE**, la valutazione della conformità è effettuata come parte della procedura di cui agli articoli da 97 a 101 di tale direttiva (viene coinvolto un **organismo esterno di valutazione della conformità**).



Una volta effettuata con successo la valutazione della conformità, i sistemi di A.I. dovranno essere **marcati CE**. **Alcuni sistemi** dovranno inoltre essere registrati in un **apposito database accessibile al pubblico**. Solo a questo punto, potranno essere immessi sul mercato.

La **marcatura CE** e la **registrazione nel suddetto database** saranno quindi i **principali strumenti** che consentiranno di **valutare facilmente**, almeno in **prima battuta**, quali sono quei **prodotti e tecnologie** che rispondono alla **normativa UE**.



Obblighi di trasparenza

Il Regolamento prevede specifici **obblighi informativi** applicabili anche ad alcuni sistemi di A.I. non considerati di per sé ad “alto rischio” ma destinati ad **interagire con persone fisiche**, a **riconoscere le emozioni** (es. alcuni apparati promozionali del tipo “**digital signage**”) e usati per la **manipolazione di video e immagini di persone fisiche** (es. c.d. “**deep fake**”).

«**Regulatory sandboxes**»

- Introduzione della possibilità di creare “*regulatory sandboxes*” (**ambienti di prova**, peraltro già esistenti in diversi Stati europei, ad es. in Norvegia);
- definizione delle **condizioni per creare** “sandboxes” anche per progetti paneuropei;
- previsione di **regole specifiche per il riutilizzo di dati personali**, raccolti per altre finalità, all’interno di una “sandbox” (art. 10 par. 5);
- previsione di un **accesso preferenziale** alle “sandboxes” per le **startup**, mirando a stimolare la creazione di tecnologie innovative in Europa.

Comitato europeo per l'A.I.

Viene istituito un **Comitato europeo per l'A.I.** (composto da rappresentanti degli Stati membri e della Commissione), a cui vengono attribuite diverse funzioni, tra cui:

- facilitare un'attuazione agevole, efficace e **armonizzata** del Regolamento;
- contribuire all'efficace **cooperazione** delle autorità nazionali e della Commissione;
- fornire **consulenza** e competenza alla Commissione;
- raccogliere e condividere anche le **migliori pratiche** tra gli Stati membri.

A livello nazionale, gli Stati membri dovranno designare **una o più autorità nazionali** competenti e, tra queste, **l'autorità di controllo nazionale**, allo scopo di controllare l'applicazione e l'attuazione del regolamento.

Il **Garante europeo della protezione dei dati** fungerà da autorità competente per il controllo delle istituzioni, delle agenzie e degli organi dell'Unione quando rientrano nell'ambito di applicazione del presente regolamento.

Monitoraggio successivo all'immissione in commercio



I fornitori di sistemi di A.I devono:

- implementare i sistemi volti a **monitorare** l'uso dei sistemi di A.I. che immettono sul mercato, **per verificare se gli stessi rimangono conformi al Regolamento** nel corso del proprio ciclo di vita;
- **segnalare** alle autorità competenti eventuali **malfunzionamenti ed incidenti** che dovessero riscontrare attraverso tale attività di monitoraggio.



Elenco dei sistemi di AI ad alto rischio aggiornabile. Gli operatori devono considerare **tre fasi**: **A)** investigativa della finalità dell'AI; **B)** valutativa del rischio; **C)** di individuazione dei requisiti e metodi per mitigarlo.

- **Rischio:** **1)** salute; **2)** sicurezza; **3)** diritti e libertà fondamentali degli individui
- **Procedure** di costante **valutazione e monitoraggio** del rischio (in relazione al c.d. *machine* e *deep learning*)
- **Data Governance:** attività che porti ad un output desiderato (*accuracy*, resilienza, *cybersecurity by design*)
- **Dataset e Fine Tuning:** pertinenza e qualità dei dati, impostazione AI che eviti discriminazioni (dati sempre rappresentativi del contesto ed esatti)
- **Accountability e logging:** responsabilità, documentabilità e registrazione delle operazione
- **Trasparenza:** comprensibilità della logica AI da spiegare con linguaggio chiaro ed esplicativo dei rischi
- **Supervisione Umana by design:** da prevedere *ab initio* con la possibilità di appellarsi ad una decisione umana
- **Formazione:** competenza del personale preposto alla supervisione e intervento

Le sanzioni

In caso di violazioni del Regolamento, le autorità competenti, individuate da ciascuno Stato Membro, possono erogare sanzioni **fino a euro 30.000.000** o, se l'autore dell'illecito è un'azienda, **fino al 6% del suo fatturato annuo** totale a livello mondiale dell'esercizio finanziario precedente, a seconda di quale sia maggiore.

Le sanzioni applicabili sono, quindi, maggiori di quelle previste dal GDPR, ma in linea con quelle previste dal *Digital Services Act*.





Che cos'è l'intelligenza?

**Esiste una intelligenza
collettiva?**

**L'intelligenza è artificiale
o solo naturale?**

**Oggi si può parlare di
co-intelligenza?**

Studio Legale

Tamos & Partners

avvocatinteam.com

Approfondimenti

Avv. Lorenzo Tamos
www.avvocatinteam.it

