La prima legge sull'Intelligenza Artificiale

L'A.I. ACT

dell'Unione Europea

Enzo Casolino

Prendiamo qui in considerazione non «l'Intelligenza Artificiale» o meglio le «Intelligenze Artificiali» ma gli effetti sociali del loro impiego.

Il che ci rimanda direttamente alla **persona** - soggetto fisico o giuridico – che ne dispone l'impiego, e ai comportamenti di esso.

Gli effetti dell'I.A. sui singoli e sulla collettività tuttavia non sono al momento completamente qualificabili e quantificabili, per cui possono determinarsi situazioni di rischio relative ad «effetti imprevisti» incidenti sulla tutela dei diritti della persona e della società.

Le I.A. possono anche determinare deleteri «effetti voluti» in quanto impiegate in attività criminose (truffe online, violenza privata, violazione della «cybersecurity», attacchi alla libertà del mercato, alla difesa nazionale e alle reti di servizi civili e militari) con conseguente attentato alla fede e alla sicurezza pubblica.

D'altra parte, gli indubbi «effetti benefici» di I.A. a livello individuale e collettivo inducono a sostenere l'impiego di I.A. in svariati settori della vita pubblica (salute, ambiente, trasporti, diritto e giustizia, istruzione, ricerca scientifica, arte, svago, agricoltura, *disaster*

recovery, servizi pubblici in generale).

Questa duplice configurazione conduce alla opportunità/necessità di adottare:

- **disposizioni di carattere promozionale** per l'uso di I.A.
- **disposizioni di carattere sanzionatorio** relative all'abuso di I. A.
- **disposizioni per governare** le situazioni di incertezza/rischio determinabili da I.A.

Trattasi comunque di norme che tendano ad ottimizzare il rapporto rischio/beneficio tramite trasparenza dei dati e dei comportamenti certificazione dei prodotti e servizi vigilanza pubblica sul settore effettività delle sanzioni.

Le norne sanzionatorie consentono di:

- tutelarsi da comportamenti che ledono i diritti della persona (violazione della privacy e sicurezza personale, furto dell'immagine/profilo, discriminazione razziale, truffe a soggetti fragili, ricatti) la fede pubblica (turbative monetarie, commerciali, certificazioni false); l'esercizio delle funzioni istituzionali (turbative elettorali, attentati alla sicurezza nazionale).
- ottenere informative preventive e trasparenti sulle politiche del fornitore di I.A. relative all'impiego di essa (sulla gestione e tracciabilità dei dati; su tutela della privacy; istruzioni d'uso; esibizione di marcatura di garanzia):

ciò per consentire all'utente l'accettazione consapevole e responsabile del rischio.

Le norne sanzionatorie consentono inoltre di:

- assicurare il risarcimento dei danni generati da comportamenti impropri, sia intenzionali che non intenzionali (responsabilità penale e civile);.
- tutelare l'utente rispetto a comportamenti che ostacolano la «capacità di agire» (libertà di impresa, contrasto a monopoli (antitrust), a furti di copyright, ecc.);
- tutelare la fede pubblica tramite la vigilanza su I.A. a cura di amministrazioni pubbliche e di organismi indipendenti.

Le norne promozionali consentono di:

- favorire l'impiego di quelle I.A. che contribuiscono in generale al **miglioramento fisico e psichico della persona** e al **supporto alla coesione sociale**; tra cui:

- tutelare la libertà della ricerca scientifica e sviluppo in materia di I. A.;
- promuovere l'impiego di I.A. per ragioni di salute pubblica, sicurezza nazionale, funzionamento delle istituzioni (es. leggi elettorali, referendum, censimenti);
- favorire l'attuazione di «programmi di intervento» e di «politiche pubbliche» rivolte a diffondere I.A. all'interno delle imprese e dei servizi.

Ambito di applicazione delle norme su I.A.

L'impiego di I.A. proietta ulteriormente l'economia in un mercato globalizzato, per cui le norme nazionali in materia si rivelano inefficaci, in altri termini:

la disciplina di I.A. impone il ricorso a norme di carattere internazionale, meglio: **norme di carattere globale** (il riferimento corrispondente va alle disposizioni relative al funzionamento dei mercati, della moneta, della borsa).

Struttura delle disposizioni (A)

Norme di tutela dell'«utente» del prodotto o del servizio di I.A.

rivolte a:

- tutelare i diritti della persona; tutela da discriminazioni, frodi e furti di immagine, di identità, di dati personali;
- disciplinare la trasparenza della «responsabilità civile» del fornitore o esercente di IA. in forza di effetti imprevisti e comunque non intenzionali del suo operato;
- incentivare l'impiego di I.A. a livello personale e aziendale;
- favorire l'introduzione di I.A. riguardo all'accesso ai servizi pubblici e all'esercizio dei diritti civili (es. diritto di voto elettronico).

Struttura delle disposizioni (B)

Norme di tutela del «fornitore/esercente» di I.A:

- disposizioni di protezione del prodotto dell'ingegno (copyright) a beneficio del creatore/fornitore del prodotto o del servizio I.A.;
- regime assicurativo dei rischi derivanti da responsabilità civile.

Struttura delle disposizioni (C)

Norme di tutela delle «fede pubblica e delle pubbliche funzioni»

rivolte a.

- intercettazione dei dati relativi a reati contro la *fede pubblica*;
- trasparenza e certificazione relative a I.A. negli atti pubblici;
- vigilanza dell'Amministrazione pubblica sull'impiego fraudolento di I.A. nelle comunicazioni sociali;
- tutela della sicurezza nazionale;
- contrasto all' «hackeraggio» realizzato mediante I.A.;
- incentivazione dell'impiego di I.A. nelle imprese e amministrazioni;
- provvidenze per ridurre il «digital divide».

Tipologia delle misure di prevenzione

L'imprevedibilità degli effetti delle applicazioni di I.A. induce ad adottare norme basate non sul criterio del «controllo ispettivo» ma su quello dell' «autovalutazione e autodenuncia del rischio» associato alla vigilanza da parte di organismi pubblici.

***

Stato dell'arte riguardo alle leggi sull' I.A.

(I) Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto del Consiglio d'Europa, in vigore dal 5 settembre 2024 (Unione Europea prima firmataria):

- finalizzata a garantire, nell'impiego di sistemi di IA., la tutela dei diritti umani, il rispetto dello stato di diritto e degli standard giuridici riguardanti l'esercizio della democrazia.

(II) Linee guida ONU sulla gestione dell'intelligenza artificiale «Governing A.I. for Humanity» (dicembre 2023).

(III) Il 2° agosto 2024 è entrato in vigore il **Regolamento dell'Unione Europea sull'Intelligenza Artificiale** denominato **A. I. Act.**

A.I. Act

A.I. Act - Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale:

approvato dal Parlamento UE il 13.3.2024;

pubblicato in GUCE il 14 luglio 2024;

in vigore dal 2 agosto 2024-10;

si applica – con alcune anticipazioni (febbraio 2025) e posticipi (agosto 2027) - a partire dal 2 agosto 2026;

valido anche per i Paesi facenti parte dello Spazio Economico Europeo (SEE);

tempi di attuazione completa: 36 mesi a partire dal 2 agosto 2024

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689.

FINALITÀ DELL'ATTO

1. **migliorare** il funzionamento del mercato interno mediante un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'impiego di sistemi di **una intelligenza artificiale** (IA) **antropocentrica, affidabile, e conforme ai valori dell'Unione Europea** di cui all'art.2 del trattato sull'Unione europea – TUE (Maastricht 1992 - Lisbona 2007);
2. **garantire,** nel contempo, un livello elevato di protezione della salute, della sicurezza, dei diritti fondamentali della Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo stato di diritto e la protezione dell'ambiente;
3. **proteggere** l'Unione dagli effetti nocivi dei sistemi di IA;
4. **promuovere** l'innovazione e la sperimentazione di prodotti/servizi I.A.;
5. **garantire** la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA.

PRESUPPOSTI DELL'ATTO

A. l'impiego dell'I.A. apporta indubbi benefici;

B. l'impiego di I.A. può comportare rischi di varia consistenza;

C. i benefici che essa produce vengono, in generale, valutati superiori ai rischi;
D. i rischi vanno comunque ridotti mediante la ricerca, la previsione, la prevenzione, la loro mitigazione;
E. la mitigazione dei rischi va effettuata non principalmente mediante divieti, bensì mediante la cooperazione di fornitori e gestori di I.A con Amministrazioni pubbliche - UE e nazionali - vigilanti;
F. la sperimentazione di nuovi prodotti/servizi va favorita;
G. l'evoluzione della fenomenologia fa risultare essenziale:
   - la revisione dinamica della classificazione dei rischi
   - l'adozione di nuove misure e divieti rapportati al variato assetto dei fenomeni e all'entità degli eventi riscontrati.

   Per cui: L' *«A.I. Act»* introduce un sistema di «norme sperimentali» *(processo iterativo continuo*) essenziale per una «navigazione a vista» riguardo ad una fenomenologia sostanzialmente benefica ma non consolidata.

DESTINATARI DELL'ATTO

Le norme prendono a riferimento e sono rivolte:

a. al «fornitore» di modelli di I.A. destinati al mercato;
b. al «distributore» sul mercato di modelli di I.A.;
c. al «*deployer*»: il soggetto che utilizza un sistema di I.A. sotto la sua autorità;
d. ai «prestatori di servizi» in genere, comportanti impiego di sistemi di I.A., compresi i soggetti stabiliti/ubicati in un Paese terzo esterno all'Unione;
e. a tutti gli «utenti» destinatari di prodotti/servizi che impiegano I.A.

L'Atto è costituito da 113 articoli e 13 allegati.

È già in vigore perché non richiede il recepimento da parte dei singoli Stati: ciò in ragione della sua natura di Regolamento e non di Direttiva.

Non poche disposizioni devono essere integrate con successivi provvedimenti amministrativi.

STRUTTURAZIONE COMPLESSIVA DELLE NORME

Per perseguire la protezione dei cittadini europei e la promozione del settore I.A., l'Atto definisce i criteri generali di comportamento da parte di ogni soggetto che crei o

somministri o impieghi prodotti rientranti nell'ambito dell'I. A.

I previsti provvedimenti attuativi devono completarsi entro il prossimo biennio, dopo di che si procede in base al criterio della revisione dinamica dei provvedimenti: soprattutto quelli a livello di Stati.

Per creare un quadro giuridico favorevole all'innovazione (Titolo V), in particolare per le PMI e le start-up, la sperimentazione normativa viene incoraggiata anche a livello nazionale, pur associata ad un sistema di valutazione responsabile dei rischi, e di governance pubblica.

La sperimentazione dovrà avvenire nell'ambito di un ambiente controllato e autorizzato (*sandbox*), e per un periodo di tempo predefinito: il tutto sulla base di un piano di prova concordato con le autorità competenti.

IDENTIFICAZIONE DEI RISCHI

In particolare al fine di instaurare un **«ecosistema di fiducia»** l'Atto:

1. identifica le categorie di rischio:
2. stabilisce le procedure per gestirli;
3. introduce disposizioni per l'immissione sul mercato di modelli di I.A. per uso generale;
4. stabilisce il monitoraggio del mercato a cura di appositi organismi di «*governance*».

GESTIONE DEI RISCHI IN RAGIONE DELLE FASI DI VITA DEL SISTEMA/PRODOTTO E DEI DIFFERENTI IMPIEGHI DI I.A.

viene prescritto un **procedimento ciclico:**

1. identificazione dei rischi;
2. valutazione «ex ante» dei rischi;
3. classificazione dei rischi (rischio inaccettabile; rischio alto; rischio basso o minimo);
4. adozione di misure precauzionali conseguenti;
5. immissione nel mercato del sistema/prodotto;
6. valutazione «ex post»;
7. ulteriori misure correttive.

VALUTAZIONE DEI RISCHI

La **valutazione ex ante** comprende (Titolo III) una prima attività a cura dello stesso sviluppatore/fornitore dei sistemi di I.A (art.11) o a cura di un Organismo notificato (soggetto terzo rispetto al fornitore: art.43 e all.VII), al fine di riscontrarne la coerenza di essi con i criteri della normativa nonché la loro accuratezza, robustezza e cybersicurezza durante l'intero ciclo di vita (art.15).

Successivamente all'immissione nel mercato, la prescritta ulteriore **valutazione «ex post»** viene effettuata ai sensi dell'art.9:

trattasi di processo iterativo in modo da rilevare eventuali ulteriori rischi e prevenirne le conseguenze nocive.

Per tutto questo i fornitori dovranno redigere e aggiornare i documenti di valutazione dei rischi (art.11).

I fornitori - non appena ne vengano a conoscenza – sono tenuti a informare le autorità nazionali competenti riguardo a incidenti gravi, malfunzionamenti, usi distorti e lesioni dei diritti fondamentali che si siano verificati anche all'esterno del proprio ambito.

CATEGORIE DEI RISCHI (art.9 AI Act).

Rischio inaccettabile: viene prescritto il divieto assoluto di impiego di quei sistemi o prodotti di I.A. che, ad esempio, permettono l'attribuzione di un «punteggio sociale» da parte di governi o imprese, e che determinano una sostanziale minaccia per i diritti fondamentali della persona**;**

Rischio alto: viene prescritto il divieto di impiego dei sistemi/prodotti/servizi I.A. elencati (art.6, all.III), salvo di quelli specificamente autorizzati: esempio, quelli utilizzati per la selezione e l'assunzione di personale devono rispettare requisiti rigorosi, tra cui le misure per l'elevata qualità e trasparenza dei dati e delle informazioni a beneficio degli utenti, la sorveglianza umana, l'attenuazione dei pericoli, ecc.;

Rischio basso o minimo: è consentito il libero impiego: es: i sistemi di I.A impiegati per i filtri spam e i videogiochi non sono soggetti ad alcun divieto, ma il distributore deve registrarli (art.49) ed è invitato ad adottare codici di condotta aggiuntivi.

In generale, indipendentemente dalla categoria del rischio, **vige l'obbligo della trasparenza:** per cui, sistemi - quali i chatbot - devono informare gli utenti che essi non stanno interagendo con un essere umano, mentre alcuni contenuti generati da I.A. devono essere riconoscibili dall'utente e quindi esplicitamente etichettati come tali.

SISTEMI I.A. AD ALTO RISCHIO (art.6, all. III).

In via generale, **si presume ad alto rischio** il sistema I.A. impiegato in:

- **identificazione biometrica remota;**
- **infrastrutture digitali critiche (sistemi di servizi pubblici:** es. gestione traffico, erogazione elettricità, acqua, gas, ecc.);
- **istruzione e formazione professionale;**
- **lavoro e occupazione;**
- **accesso del soggetto a servizi pubblici essenziali;**
- **attività di contrasto alla criminalità;**
- **migrazione, asilo e gestione del controllo delle frontiere;**
- **amministrazione della giustizia e processi democratici** (elezioni, referendum);
- **mercato dell'Unione:** se l'impatto è significativo si configura come "sistema ad **alto rischio sistemico**".

GESTIONE DEI RISCHI

Ai fini dell'immissione nel mercato, risultano di particolare rilievo le prescrizioni relative alla sorveglianza umana (art.1), per cui i sistemi ad alto rischio dovranno essere progettati e sviluppati anche con **strumenti adeguati di interfaccia uomo-macchina**, in modo tale da poter essere supervisionati da persone fisiche durante il periodo in cui sono in uso. La sorveglianza umana deve mirare a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali.

La **Commissione può ampliare l'elenco dei sistemi di I.A. ad alto rischio utilizzati all'interno di alcuni settori predefiniti.** A distanza di cinque anni dalla data di applicazione dell'Atto, la Commissione pubblicherà una Relazione di Valutazione e di Riesame della disciplina relativa all'impiego di I.A. all'interno dell'Unione.

DIVIETI SPECIFICI

Tra le applicazioni rischiose vietate e classificate come reati (art.5 e All. II dell'Atto) troviamo quelle che impiegano **sistemi che**:

sfruttano **tecnologie subliminali o che incidono sulla vulnerabilità** delle persone, o rivolte alla classificazione di esse, o al riconoscimento facciale e rilevamento delle emozioni, o alla categorizzazione o identificazione biometrica o che generano e distribuiscono contenuti falsi (deep fake);

comportano abuso di persone vulnerabili e fragili;

praticano la categorizzazione biometrica facente riferimento a dati personali sensibili;

includono la pesca a strascico (social *scraping*) **di volti** rilevati tramite rete;

operano il riconoscimento delle emozioni negli ambienti lavorativi e scolastici;

vengono impiegati a scopo di criminalità predittiva in base all'analisi della persona, ceto sociale, etnia, ecc.

consentono di attribuire **punteggio automatico a comportamenti della persona**.

ECCEZIONI PREVIA NOTIFICA E/O AUTORIZZAZIONE

Non è vietato il riconoscimento facciale e biometrico in tempo reale impiegato:

a scopo di ricerca di vittime di reati e di persone scomparse, o di antiterrorismo;

in caso di minacce certe alla vita o alla sicurezza fisica delle persone o di attacco terroristico;

a scopo di localizzazione e identificazione dei presunti autori di una lista di 16 reati.

Il divieto di categorizzazione biometrica non riguarda l'etichettatura o il filtro di *dataset* biometrici, legalmente acquisiti, per **scopi di pubblica sicurezza o di difesa nazionale.**

Inoltre, i divieti **non si applicano agli impieghi di sistemi I.A, anche di quelli definibili ad alto rischio, per motivi di ricerca scientifica e di sviluppo**, qualora non ledano fattualmente la sfera della persona e della collettività.

I GARANTI NAZIONALI DEI DATI PERSONALI E DEL MERCATO I.A.

devono inviare ogni anno alla Commissione UE un rapporto sull'uso dei sistemi di riconoscimento biometrico in tempo reale, così come i casi di verificati impieghi proibiti.

OBBLIGHI A FINI DI TUTELA E GARANZIA NELLA GESTIONE DEI RISCHI

L'immissione sul mercato, la messa in servizio o l'uso di un sistema che utilizzi tecniche subliminali consentite, devono tutti assicurare che comunque l'utente ne sia consapevole e che non comporti per esso un danno fisico o psicologico (art.16 dell'Atto);

Il **criterio della trasparenza determina l'obbligo**:

- per tutti i soggetti (fornitore di modelli> fornitore di sistemi> fornitore di servizi> datore di lavoro> dipendente/utente): di informare che si sta interagendo con un'attività comportante rischio (art.53);
- per tutti i soggetti fornitori: di esporre la marcatura di conformità CE (art. 24);
- per i fornitori di modelli/servizi: di registrare il sistema (art.49) nella banca dati UE (art.71);

In particolare, per i sistemi ad **alto rischio**:

- obbligo di fornire garanzia all'utente di accuratezza, robustezza e cibersicurezza durante tutto il relativo ciclo di vita;

I sistemi di I.A. definiti a **rischio minimo** (Titolo IX) possono essere sviluppati e utilizzati nell'UE senza obblighi specifici; tuttavia, gli sviluppatori – fornitori -distributori sono tenuti a registrarli (art.49) e invitati ad adottare confacenti codici di condotta volontari.

SANZIONI

Fino a 35 milioni di euro e fino al 7% del fatturato mondiale dell'azienda (art.99 dell'Atto).

DOCUMENTAZIONE OBBLIGATORIA RELATIVA ALLA GESTIONE DEI SISTEMI I.A.

Il responsabile di attività I.A. produce, conserva ed esibisce a richiesta la documentazione (avente carattere di autocertificazione) relativa:

a) all'analisi dei rischi;
b) alla formazione degli addetti;
c) al funzionamento del servizio di sorveglianza umana (art.14);

d) alle linee guida prodotte e ai servizi di assistenza all'utente, ecc.;
e) all'autodenuncia di effetti dannosi o impropri riscontrati in fase di applicazione del sistema I.A.;
f) ai codici di buone pratiche (art.50) adottati, tra cui i «**codici di condotta**» i cui modelli saranno predisposti a cura della Commissione UE (ex art.69).

MISURE RIVOLTE ALLA PROMOZIONE DI I. A.

L'Atto contiene svariate disposizioni intese a promuovere l'impiego di I.A.

Tra esse particolare rilievo assume quella rivolta a favorire la «**sperimentazione**»: la quale consente l'esposizione con cautele anche ad un rischio elevato: «esposizione controllata». Per questo, viene prevista e favorita la sperimentazione tecnica e normativa di nuove applicazioni in ambienti controllati: le *sandbox* (spazi di sperimentazione normativa, art.57). Queste *sandbox* sono costituite da un ambiente fisico o virtuale in cui l'operatore può sperimentare, anche derogando alle norme ordinarie, in quanto gli è consentito – previo accordo con l'Autorità - di sottoporre a prova, per un periodo limitato, tecnologie innovative potenzialmente rischiose sotto la supervisione delle autorità competenti e sulla base di un piano concordato.

Viene prevista anche la «sperimentazione di sistemi ad alto rischio in condizioni reali al di fuori degli spazi della sperimentazione normativa I.A. (art.60) tramite atti di esecuzione emessi direttamente dall'Ufficio I.A. della Commissione.

L'Atto contiene anche altre disposizioni promozionali relative ad esoneri per sostenere l'innovazione, ridurne gli oneri normativi e sostenere le piccole e medie imprese (PMI) e le start-up.

«GOVERNANCE»

ORGANI DEPUTATI ALLA VIGILANZA E CONTROLLO DEL MERCATO I.A.

Ufficio per l'I.A. (art.64) della Commissione EU;

Gruppo di esperti scientifici (art.68);

Comitato europeo per l'intelligenza artificiale (art.56);

Consiglio europeo per l'I.A. (art.65), organo consultivo;

Forum consultivo (art.67), organismo a composizione multilaterale;

Organismo di valutazione notificato (art.31);

Autorità di notifica (art.28);

Banca dati dell'UE per i sistemi di IA ad alto rischio (art.71), relativa ai sistemi obbligatoriamente registrati (art.49);

Garante europeo della protezione dei dati (art. 57 e 100);

Autorità nazionale di vigilanza del mercato I.A.(art. 70); Struttura deputata al rilascio della **istituenda marcatura digitale CE** sui sistemi I.A. (art.48).

SPECIFICHE SUL SISTEMA DI «GOVERNANCE»:

1) Ufficio per l'I.A. (art.64): è l'organismo operativo con cui la Commissione governa vigila e provvede nel merito;

2) il **Gruppo di esperti scientifici (art.68), è l'**organismo consultivo di supporto alla Commissione;

3) il **Comitato europeo per l'intelligenza artificiale (art.56):** è costituito da esperti competenti provenienti dai Paesi UE; esso esamina la fattibilità di nuovi programmi, valuta le strategie nazionali, promuove l'impiego etico e sicuro di I.A., raccoglie e pubblicizza - tra gli Stati membri - le migliori pratiche poste in atto;

4) il **Consiglio europeo per l'I.A. (art.65):** è costituito dai rappresentanti degli Stati: esso esercita funzioni consultive e di indirizzo;

5) il **Forum consultivo (art.67):** è costituito da rappresentanti di settori: industria, start-up, PMI, società civile, mondo accademico;

6) l'**Organismo di valutazione notificato (art.31):** valuta i rischi, deve accreditarsi presso l'Autorità di notifica;

7) l'**Autorità di notifica (art.28):** provvede ad accreditare e vigilare sull'operato degli Organismi di valutazione;

8) la **Banca dati UE dei sistemi I.A. ad alto rischio (art.71),** provvede alla «registrazione» (art.49) dei dati relativi;

9) il **Garante europeo della protezione dei dati agisce in qualità di autorità vigilante (art.57) e sanzionatoria (art.100) sulle istituzioni, agenzie e organismi dell'Unione (art.57) in relazione alle fattispecie contemplate dell'Atto;**

10) le **Autorità nazionali di vigilanza del mercato I.A. (art. 70):** gli Stati membri,

entro due anni, istituiscono una o più Autorità competente, tra cui l'Autorità nazionale di controllo, al fine di verificare il livello di applicazione della Legge. Tutto ciò impiegando al massimo strutture già esistenti, in particolare quelle relative alla cibersicurezza. In sostanza, tutto il sistema di vigilanza prefigurato dall' A.I Act va gestito - ai livelli UE e degli Stati – anche in raccordo con l'ordinamento relativo alla cibersicurezza e alla tutela del mercato (Digital Markets Act/2023), come pure con i preesistenti Organismi preposti alla vigilanza sulla Digitalizzazione e sulla Comunicazione;

11) le **Autorità di vigilanza del mercato CE:** ai due livelli (Unione/Stati) esse mantengono tutte le loro competenze riguardo **all'andamento complessivo del mercato,** ivi comprese quelle relative agli obblighi e requisiti di tutti i sistemi di IA ad alto rischio già immessi sul mercato. Come pure conservano tutti i poteri e le risorse per intervenire nel caso in cui i sistemi di I.A. generino rischi imprevisti per i quali è richiesto un intervento di emergenza.

La «governance» a livello italiano

Il monitoraggio e controllo del settore I.A. verrà esercitato anche in Italia tramite l'«**Autorità nazionale di controllo del mercato I.A**.» (art.70). Essa, ovviamente, non ha poteri normativi ma provvederà essenzialmente tramite disposizioni di carattere amministrativo. Da segnalare che in Italia opera anche l' «**Agenzia per l'Italia Digitale** "(AgID)" che provvede alla promozione anche dell'IA. mediante la collaborazione con il settore privato.

Inoltre: presso la Camera dei Deputati opera un apposito **Comitato per l'I.A**. che, tramite audizioni di esperti, monitora gli andamenti e potenzialità dell'I.A.

RIEPILOGANDO

La disciplina giuridica dell'Unione Europea considera l'Intelligenza Artificiale (I.A.) come risorsa pubblica e non una minaccia per i cittadini europei. Le norme servono per consolidare il rapporto di fiducia con i sistemi I.A., per cui **le prescrizioni UE servono a monitorare e governarne l'impiego, anche quello rischioso, e non ad impedirlo:** esse sono **rivolte a garantire la tutela della salute e della sicurezza degli utenti/consumatori e il rispetto dei diritti fondamentali dei cittadini;** tuttavia **consentono anche una**

limitata lesione dei diritti della persona quando l'impiego di I.A. è strumentale all'esercizio legittimo di pubbliche funzioni (es. sicurezza sociale, ricerca di vittime di reati e di persone scomparse; antiterrorismo; identificazione di autori di particolari reati) comunque le norme **non vietano la produzione e messa in servizio di sistemi I.A. a scopi di ricerca scientifica e sviluppo** (art.2).

***

Complessivamente: la normativa è sperimentale e ***in itinere***, infatti la Commissione EU è delegata (per 5 anni) a modificare - con atti delegati - svariate disposizioni della Legge in base all'andamento del mercato I.A. (artt. 6 e 97).