Legge sull'intelligenza artificiale

Dossier n° 57 -
12 novembre 2021

Tipo e numero atto	*Proposta di regolamento COM(2021)206*
Data di adozione	*21 aprile 2021*
Base giuridica	*Articolo 114 del Trattato sul funzionamento dell'Unione europea (TFUE): misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno*
Settori di intervento	*Innovazione; intelligenza artificiale; nuova tecnologia; vigilanza del mercato; protezione dei dati; autorizzazione di vendita; dati personali; marcatura CE di conformità; tecnologia digitale; biometria.*
Assegnazione	*8 giugno 2021 – Commissioni IX e X riunite*
Segnalazione del Governo	*Si*

In sintesi

Preannunciata in una serie di documenti programmatici della Commissione europea (tra i quali, il Libro Bianco sull'Intelligenza artificiale - un approccio europeo all'eccellenza e alla fiducia COM(2020)65), e pubblicata contestualmente alla comunicazione Promuovere un approccio europeo all'intelligenza artificiale COM(2021)205), la proposta di regolamento COM(2021)206 reca una serie di norme armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad **alto rischio**, così come **restrizioni** in relazione a determinati usi, tra i quali in particolare i sistemi di identificazione biometrica remota.

L'intelligenza artificiale (IA) consiste in una famiglia di tecnologie in grado di generare **output** quali contenuti, **previsioni**, raccomandazioni o **decisioni** che influenzano gli ambienti con cui interagiscono.

La nuova disciplina mira a **ridurre al minimo** i rischi per la **sicurezza** e i **diritti fondamentali** che potrebbero essere generati dai sistemi di IA prima della loro immissione sul mercato dell'UE. A tal fine, l'approccio della Commissione si basa su una "**piramide di rischio**" ascendente (che va dal **rischio basso/medio** a quello **elevato**, fino al rischio **inaccettabile**) per classificare, nell'ambito dell'IA, una serie di casi di pratiche generali e di impieghi specifici in determinati settori, cui la Commissione ricollega rispettive **misure di attenuazione**, o addirittura i **divieti** di alcune pratiche di IA.

Tali **divieti** riguardano una serie limitata di utilizzi dell'IA ritenuti **incompatibili** con i valori dell'Unione europea, in particolare quelli che si sostanziano nei diritti fondamentali contenuti nella Carta europea.

Si tratta in particolare di: divieti concernenti i sistemi di IA che **distorcono** il **comportamento** di una persona attraverso tecniche subliminali o sfruttando **vulnerabilità specifiche** in modi che causano o sono suscettibili di causare **danni fisici** o **psicologici;** divieti concernenti

l'attribuzione di un **punteggio sociale** (*social scoring*) con finalità generali mediante sistemi di IA da parte di autorità pubbliche.
Il regime specifico di divieto si estende a determinati sistemi di **identificazione biometrica remota** (ad esempio strumenti di riconoscimento facciale per controllare i passanti in spazi pubblici), salvo casi eccezionalmente autorizzati dalla legge riconducibili in linea di massima ad attività di prevenzione e contrasto del crimine, in ogni caso soggetti a garanzie specifiche.
Una seconda categoria di sistemi di IA, pur consentiti ma classificati ad **alto rischio**, deve rispettare un insieme di **requisiti** specificamente progettati, che comprendono l'utilizzo di **set** di **dati** di alta **qualità**, l'istituzione di una **documentazione** adeguata per migliorare la tracciabilità, la condivisione di **informazioni** adeguate con l'utente, la progettazione e l'attuazione di misure adeguate di **sorveglianza** umana e il conseguimento degli standard più elevati in termini di **robustezza**, sicurezza, cibersicurezza e precisione. La proposta delinea un **sistema** di **valutazione** di **conformità** dei sistemi di IA ad alto rischio a tali requisiti, attivato prima che vengano immessi sul mercato o messi in servizio.
Per integrarsi agevolmente con i quadri giuridici esistenti la proposta tiene conto, ove opportuno, delle **regole settoriali** per la sicurezza, assicurando la **coerenza** tra gli atti giuridici e la semplificazione per gli operatori economici.
Per una serie di sistemi di IA considerati a basso rischio sono previsti soltanto **requisiti minimi** di **trasparenza:** è il caso di *chatbot* (programmi in grado di simulare **conversazioni umane**), sistemi di riconoscimento delle emozioni o "*deep fake*" (foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali, riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce).
Sono previste norme per promuovere il ricorso a **spazi** di **sperimentazione normativa**, che creano un ambiente controllato per testare tecnologie innovative per un periodo limitato, e l'accesso ai **poli** dell'innovazione digitale e a **strutture** di prova e sperimentazione, con l'obiettivo di sostenere le imprese innovative, le PMI e le *start-up*.

I sistemi di intelligenza artificiale: tecnologia e impiego

Secondo la definizione impiegata in studi del Parlamento europeo l'**intelligenza artificiale** (IA) è l'abilità di una macchina di mostrare capacità umane quali il **ragionamento**, l'**apprendimento**, la **pianificazione** e la **creatività**; tali caratteristiche consentono all'IA la comprensione del proprio ambiente, l'elaborazione di ciò che viene percepito e l'individuazione di soluzioni per un obiettivo specifico. In particolare il sistema è in grado di ricevere i dati (già preparati o raccolti tramite sensori), di processarli e di indicare la risposta richiesta. Nella società e nell'economia attuali si conoscono numerose categorie di intelligenza artificiale realizzate mediante varie forme: si tratta, tra l'altro, di software come **assistenti virtuali**, strumenti di analisi di **immagini, motori di ricerca**, sistemi di **riconoscimento facciale** e **vocale;** l'IA interviene, altresì, sotto forma di sistemi incorporati in altri oggetti quali ad esempio robot, veicoli autonomi, droni, e in generale strumenti nel cosiddetto ambito dell'internet delle cose (*IoT - Internet of Things*).

L'"**internet delle cose**" è un'espressione impiegata per indicare quell'insieme di oggetti di uso quotidiano come telefoni, automobili, elettrodomestici, vestiti, etc, che sono collegati ad internet con una connessione senza fili tramite chip intelligenti e sono in grado di rilevare e comunicare dati.

Con riferimento alla **funzione** finale del prodotto, l'insieme dei sistemi di IA include, a titolo esemplificativo: motori di ricerca che apprendono da grandi serie di dati, forniti dagli utenti, per offrire i risultati di ricerca; software di **traduzione automatica**, basati su testi audio o scritti; sistemi di trasporto a **guida autonoma**; robot impiegati nella filiera agro alimentare (per esempio per la rimozione di erbe infestanti al fine della riduzione di diserbanti); sistemi di **allerta** per i disastri naturali sulla base di esperienze passate; sistemi per analizzare grandi quantità di **dati medici** e individuare relazioni e modelli per migliorare le **diagnosi** e la **prevenzione**.

La capacità conferita a tali sistemi di analizzare **grandi quantità** di **dati** corrisponde a necessità che stanno crescendo esponenzialmente in proporzione a quanto previsto in merito al volume dei dati prodotti, che secondo la Commissione europea nel mondo dovrebbe passare da 33 zettabyte nel 2018 a 175 zettabyte nel 2025 (un zettabyte equivale a mille miliardi di gigabyte).

Ulteriori impieghi possono apportare vantaggi in termini di **sicurezza** sul lavoro, grazie a robot dedicati alle attività più pericolose. Secondo le citate ricerche l'intelligenza artificiale può consentire inoltre lo sviluppo di nuovi prodotti e servizi, anche in settori in cui le aziende europee sono già in una posizione di forza come l'economia circolare, la **moda** e il **turismo**, ottimizzando **percorsi** di **vendita**, migliorando la **manutenzione** dei macchinari, o **risparmiando** energia.
La Commissione europea ha anche stimato **l'impatto economico** dell'automazione del lavoro, della conoscenza, e dei robot e dei veicoli autonomi entro il 2025 nel contesto della transizione verde e digitale, valutando la possibilità di un aumento di **60 milioni** di posti di lavoro nell'UE entro lo stesso anno.
Inoltre, grazie all'impiego dell'IA si prevede un aumento della **produttività del lavoro** tra l'11 e il 37 per cento entro il 2035; si ritiene inoltre che l'applicazione nell'ambito dei servizi pubblici consentirebbe una riduzione dei costi in settori quali il **trasporto pubblico**, **l'istruzione**, la gestione **dell'energia** e dei **rifiuti**, la sostenibilità dei prodotti, risultando preziosa per il raggiungimento degli obiettivi del *Green Deal.*
Da ultimo, non appare secondario l'uso dell'intelligenza artificiale nelle attività di prevenzione e contrasto del **crimine**, o come ausilio nella **giustizia penale**, tramite le capacità di rapida elaborazione di significativi volumi di dati, per esempio per la previsione e prevenzione di **attacchi terroristici**, o in campi già sperimentati come la ricerca di **pratiche illegali** *online*.
Anche il campo militare registra l'uso crescente di intelligenza artificiale, tra l'altro nel caso di attacchi informatici, o ad esempio nel settore dei droni.
Attualmente, secondo la Commissione europea, oltre il 50 per cento delle grandi imprese europee impiega sistemi di intelligenza artificiale, mentre **un quarto** dei robot ad uso **industriale** e **professionale** è prodotto in Europa; inoltre, negli ultimi tre anni i finanziamenti dell'UE per la ricerca sull'IA e l'innovazione hanno raggiunto la soglia del **miliardo e mezzo** di **euro**, registrando un aumento del **70 per cento** rispetto al triennio precedente. La Commissione europea ha stabilito l'obiettivo di sviluppare più di **venti miliardi** di investimenti all'anno (provenienti dal bilancio UE, dalle risorse nazionali, e dagli sforzi prodotti dalle imprese).
La questione attiene peraltro alla sfida relativa alla concorrenza nel settore con i grandi competitor. Più nel dettaglio, secondo le stime della Commissione europea nel 2016 il volume di investimenti nell'**UE** nell'intelligenza artificiale si è attestato **tra 2,4 e 3,2 miliardi** a fronte di un impegno nell'**America settentrionale** stimato tra i **12 e 18,6 miliardi di euro**, e a investimenti in **Asia** tra i **6,5 e i 9,7 miliardi di euro**.
La crescente rilevanza dell'adozione dell'IA può essere ulteriormente apprezzata dall'aumento di nuovi brevetti relativi a tale famiglia di tecnologie, che - secondo la Commissione europea - nell'ultimo decennio si sarebbe attestato al 400 per cento. In particolare, dal 1960 al 2018 sono 1.863 le richieste di brevetto depositate negli Stati Uniti, 1.085 in Cina, mentre sono 1.074 nell'UE. Anche in tale ambito emergono differenze con i competitor dell'UE, atteso che le aziende statunitensi risultano leader nel deposito di brevetti in 12 settori su 20 nel quali si applica l'IA.
Per un inquadramento generale dell'intelligenza artificiale nelle sue componenti essenziali e per una ricostruzione delle iniziative assunte ai vari livelli istituzionali si rinvia al Dossier di documentazione del Servizio Studi n.164 Intelligenza artificiale, dati e big data: profili tecnici e sviluppi normativi.

Questioni e criticità correlate all'uso dell'IA

La Commissione europea ha indicato una serie di **rischi** specifici potenzialmente **elevati** per la

sicurezza e i diritti fondamentali posti dall'impiego dell'IA, di fronte ai quali il diritto vigente dell'UE è considerato inadeguato, se non del tutto inapplicabile.
Tra le criticità dedotte dalla Commissione europea, il fatto che spesso non sia possibile stabilire il motivo per cui un sistema di IA è giunto a un risultato specifico (**opacità** del processo che porta dall'elaborazione dell'input dei dati all'output), determinando una serie di difficoltà nel valutare e dimostrare se qualcuno è stato ingiustamente svantaggiato dall'uso di sistemi di IA, ad esempio nel contesto di una decisione di **assunzione** o di **promozione** oppure di una domanda di **prestazioni pubbliche**. Particolare attenzione è stata prestata ai sistemi di **riconoscimento facciale** negli spazi pubblici, i quali, in assenza di una disciplina adeguata, possono dispiegare effetti intrusivi sulla vita privata; ulteriori questioni problematiche discendono dai casi in cui si registra uno scarso addestramento o una cattiva progettazione del sistema di IA, con ciò causando errori significativi in grado di discriminare le persone o comprometterne la tutela della vita privata. La distorsione da progettazione o da bassa qualità dei dati può avere effetti **discriminanti** in particolare nei processi applicati alle dinamiche del mercato del lavoro, al settore del credito, financo ai procedimenti penali, causando ineguaglianze ad esempio sul piano dell'etnia, del genere, e dell'età.
Ad esempio, la Commissione europea ha sottolineato come la **sottorappresentazione** di alcuni **gruppi sociali** nel processo di immissione dei dati in un sistema di IA possa generare discriminazioni sugli **studi clinici** (se caratterizzati dall'inclusione di un numero maggiore di dati provenienti da uomini), con l'effetto di generare conclusioni errate e conseguenze negative in ordine al **trattamento** del **sesso femminile**. Nello stesso senso, un esempio frequentemente citato dalle Istituzioni europee, quello concernente sistemi di intelligenza artificiale utilizzati nella gestione delle **risorse umane** nel mondo del lavoro che, in base a dati contenenti distorsioni storiche impiegati per adottare una decisione, hanno finito per favorire **assunzioni** o **promozioni maschili** rispetto a quelle femminili.
Da ultimo, si ricorda il tema dei rischi per l'ordinato svolgimento del **dibattito pubblico** determinati dall'uso dell'intelligenza artificiale nel contesto dell'**informazione**; è il caso per esempio dell'IA in grado di creare *bolle in rete* in cui i contenuti sono **presentati** in base ai dati con cui l'utente ha **interagito in passato**, con l'effetto di impedire la tutela di un **ambiente aperto** a un **dibattito pluralistico**, inclusivo e accessibile. L'IA può essere infine usata per creare immagini, video e audio falsi ma estremamente realistici, noti come *deepfake*, in grado di truffare, pregiudicare la **reputazione** e mettere in dubbio la fiducia nei processi decisionali, con il rischio che in definitiva si crei un processo di **polarizzazione** del dibattito pubblico e di manipolazione delle elezioni.

Contenuti

Ambito di applicazione e definizioni

Il titolo I definisce l'**oggetto** del regolamento e l'**ambito** di applicazione del nuovo regime, concernente l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA, nonché una serie di **definizioni** impiegate ai fini del nuovo regime.
L'**articolo** 3 definisce **sistema** di **intelligenza artificiale** un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I del regolamento, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali **contenuti**, **previsioni**, **raccomandazioni** o **decisioni** che influenzano gli ambienti con cui interagiscono.
La definizione di **sistema di IA** è concepita, nelle intenzioni della Commissione, in maniera il più possibile neutrale dal punto di vista tecnologico, al fine di stare al passo degli sviluppi della tecnica e del mercato. Il titolo è integrato dall'allegato I, recante un elenco di **approcci** e **tecniche** per lo sviluppo dell'IA che la Commissione può **aggiornare** mediante **atti delegati**. L'allegato riporta tre tipologie di approcci e tecniche: approcci di **apprendimento automatico**; approcci basati sulla **logica** e approcci basati sulla **conoscenza**; approcci **statistici**, metodi di

ricerca e ottimizzazione.
La proposta definisce i partecipanti all'intera catena del valore dell'IA, quali i **fornitori** e gli **utenti** di sistemi di IA, considerando tanto gli operatori pubblici quanto quelli privati in maniera da assicurare parità di condizioni.
Al riguardo, si ricorda che nella relazione trasmessa al Parlamento ai sensi dell'art. 6, comma 4, della legge n. 234 del 2012, il Governo, nell'ambito delle prospettive negoziali e delle eventuali modifiche ritenute necessarie od opportune, sottolinea in via generale l'elasticità del perimetro di applicazione del nuovo regime (in quanto modificabile attraverso atti delegati), e la necessità di valutare il rischio di incertezza giuridica e di "delega in bianco" alla Commissione.
Circa l'ambito di applicazione dal punto di vista **soggettivo**, l'**articolo 2** prevede, tra l'altro, che la nuova disciplina si applichi:
a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, **indipendentemente** dal fatto che siano stabiliti nell'Unione o in un Paese terzo;
b) agli **utenti** dei sistemi di IA situati nell'Unione;
c) ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, laddove l'*output* prodotto dal sistema sia utilizzato nell'Unione.
Il regolamento si applica anche alle autorità pubbliche, mentre sono esclusi dal nuovo regime i sistemi di IA sviluppati o usati per scopi esclusivamente militari. Sono altresì esclusi dall'ambito di applicazione le **autorità pubbliche** di **Paesi terzi** e le **organizzazioni internazionali**.

Pratiche di intelligenza artificiale vietate

Il titolo II stabilisce un elenco di **pratiche** di IA **vietate**. Nello specifico, l'**articolo 5** vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che:

- utilizzano **tecniche subliminali** che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un **danno fisico** o **psicologico**;
- sfruttano le **vulnerabilità** di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di **distorcere materialmente** il **comportamento** di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un **danno fisico** o **psicologico.**

Ai sensi della medesima disposizione, sono altresì vietati

- l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'**affidabilità delle persone fisiche** per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il **punteggio sociale** così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:
  - un **trattamento pregiudizievole** o **sfavorevole** di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che **non** sono **collegati** ai contesti in cui i dati sono stati originariamente generati o raccolti;
  - un **trattamento pregiudizievole** o **sfavorevole** di determinate persone fisiche o di interi gruppi di persone fisiche che sia **ingiustificato** o **sproporzionato** rispetto al loro comportamento sociale o alla sua gravità;
- l'uso di sistemi di **identificazione biometrica** remota "in **tempo reale**" in **spazi accessibili al pubblico** a fini di attività di contrasto, **a meno che** e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:
  - la ricerca mirata di potenziali **vittime** specifiche di reato, compresi i minori scomparsi;
  - la **prevenzione** di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
  - il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un **autore** o un **sospettato** di un **reato** contemplato dal regime in materia di **mandato**

d'arresto europeo, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

Sono inclusi in tale categoria di reati, tra l'altro: la partecipazione a un'**organizzazione criminale**, il **terrorismo**, la **frode** e il **riciclaggio**, il traffico di **droga** e di armi, la **corruzione** e la criminalità informatica.

La proposta precisa inoltre che l'uso di sistemi di identificazione biometrica remota in **tempo reale** in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi citati debba tener conto:

- della natura della **situazione** che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del **danno causato** dal mancato uso del sistema;
- delle conseguenze dell'uso del sistema per i **diritti** e le **libertà** di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

Tale impiego deve altresì rispettare le tutele e le condizioni necessarie e **proporzionate** in relazione all'uso, in particolare per quanto riguarda le **limitazioni temporali**, **geografiche** e **personali**; inoltre ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto deve essere subordinato a un'**autorizzazione preventiva** rilasciata da un'**autorità giudiziaria** o da un'**autorità amministrativa indipendente** dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale.

Tuttavia, in una situazione di **urgenza debitamente giustificata**, **è possibile** iniziare a **usare** il sistema **senza autorizzazione** e richiedere l'autorizzazione **solo durante o dopo l'uso**. L'autorità giudiziaria o amministrativa competente, tenendo conto di una serie di elementi, rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è **necessario** e **proporzionato**.

Infine, uno Stato membro può decidere di prevedere la possibilità **di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni sopra descritte.** Tale Stato membro stabilisce nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni, nonché per le attività di controllo ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati, compresi i reati per i quali si impiega la tecnica di rilevazione biometrica, le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

Sistemi di IA ad alto rischio

Il titolo III è dedicato alla disciplina concernente una serie di sistemi di IA in grado di creare un **rischio alto** per la **salute** e la **sicurezza** o per i **diritti fondamentali** delle persone fisiche. In sostanza, tali sistemi sono consentiti purché rispettino una serie di **requisiti** e siano oggetto di una **valutazione di conformità ex ante**.

In particolare, la proposta individua due principali categorie di sistemi di IA ad alto rischio: sistemi di IA destinati ad essere utilizzati come **componenti** di **sicurezza** di prodotti soggetti a **valutazione della conformità ex ante** da parte di terzi; **altri sistemi** di IA indipendenti (elencati nell'allegato III) che presentano principalmente implicazioni rispetto ai diritti fondamentali.

Tra le tecnologie di IA ritenute ad alto rischio si annoverano gli impieghi nei seguenti settori.

- **infrastrutture critiche** (ad es. i trasporti) che potrebbero mettere a rischio la vita e la salute dei cittadini;
- istruzione o formazione professionale, che può condizionare l'accesso all'istruzione e alla vita professionale di una persona (ad es. punteggio degli esami);
- componenti di **sicurezza** dei prodotti (ad es. applicazione dell'IA nella chirurgia robotica);
- **occupazione**, gestione dei lavoratori e accesso al lavoro autonomo (ad es. software di selezione dei CV per le procedure di assunzione);
- **servizi pubblici e privati essenziali** (ad es. sistemi di credito sociale che negano ai cittadini l'opportunità di ottenere un prestito);
- gestione della **migrazione**, dell'**asilo** e del controllo delle **frontiere** (ad es. verifica dell'autenticità dei documenti di viaggio);
- amministrazione della **giustizia** e processi democratici (ad es. applicazione della legge a una serie concreta di fatti);
- **identificazione** e **categorizzazione biometrica** delle persone;
- attività di **contrasto** che possono interferire con i diritti fondamentali delle persone (ad es. valutazione dell'affidabilità delle prove).

L'**articolo 7** tuttavia consente alla Commissione europea di **ampliare** l'**elenco** dei sistemi di IA ad alto

rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.

Il capo 2 include le disposizioni volte a stabilire i **requisiti giuridici** dei sistemi ad alto rischio.
In particolare, **l'articolo 9** prevede l'obbligo di istituire, attuare, documentare e mantenere un **sistema di gestione dei rischi** per tali tecnologie.

I sistemi di gestione dei rischi devono comprendere le seguenti fasi:

a. **identificazione** e analisi dei rischi noti e prevedibili associati a ciascun sistema di IA ad alto rischio;
b. stima e **valutazione** dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile;
c. valutazione di **altri eventuali rischi** derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato;
d. adozione di adeguate misure di **gestione** dei rischi.

L'obiettivo del sistema di gestione è che qualsiasi rischio residuo associato a ciascun pericolo nonché il **rischio residuo complessivo** dei sistemi di IA siano considerati accettabili, in caso di uso **conforme** alla sua finalità prevista, o **uso improprio ragionevolmente prevedibile**. I rischi residui devono essere **comunicati** all'utente.

In sostanza, le misure di gestione dei rischi devono garantire:

a. un'**adeguata progettazione** e **fabbricazione**;
b. **misure di attenuazione** e di **controllo** in relazione ai rischi che non possono essere eliminati;
c. la fornitura di **informazioni adeguate** e, ove opportuno, la **formazione** degli utenti.

L'articolo 10 stabilisce i requisiti in materia di **dati** e di *governance* dei dati.

Al riguardo si ricordano le **definizioni** di dati contenute nell'articolo 3:

- i "dati di **addestramento**" sono dati utilizzati per **addestrare** un sistema di IA adattandone i parametri che può apprendere, compresi i pesi di una rete neurale;
- i "dati di **convalida**" sono quelli utilizzati per fornire una **valutazione** del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine di evitare l'eccessivo adattamento ai dati di addestramento (*overfitting*), considerando che il set di dati di convalida può essere un set di dati distinto o essere costituito da una partizione fissa o variabile del set di dati di addestramento;
- i "dati di **prova**" sono quelli utilizzati per fornire una **valutazione indipendente** del sistema di IA addestrato e convalidato al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio.

I dati di addestramento, convalida e prova devono essere **pertinenti**, **rappresentativi**, esenti da **errori** e **completi**, e devono possedere le **proprietà statistiche appropriate**, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato; devono infine tener conto delle **caratteristiche** o degli **elementi particolari** dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

L'articolo 11 regola l'obbligo di redigere la **documentazione tecnica** di un sistema di IA ad alto rischio prima dell'immissione sul mercato o della messa in servizio di tale sistema.
L'articolo 12 prevede che i sistemi di IA ad alto rischio siano progettati e sviluppati con capacità che consentano la **registrazione automatica** degli eventi ("*log*") durante il loro funzionamento, secondo standard stabiliti in norme riconosciute o specifiche comuni.

Infine, i sistemi di IA ad alto rischio devono sottostare a **valutazioni di conformità** (articolo 19) finalizzate a individuare le misure di gestione dei rischi più appropriate (*vedi infra*); tali prove devono garantire che i sistemi di IA ad alto rischio funzionino in modo coerente per la finalità prevista e che siano conformi ai requisiti stabiliti dal regolamento.
Successivamente occorre **registrare** i sistemi di IA autonomi in una banca dati dell'UE, e firmare una dichiarazione di conformità; il sistema di IA dovrebbe recare la **marcatura** CE (articolo 19).
L'articolo 20 disciplina il regime dei *log* (le **registrazioni automatiche** degli eventi da parte dei sistemi di IA):i fornitori di sistemi di IA ad alto rischio conservano i **log generati**

automaticamente (per un periodo limitato in ragione di una serie di parametri) dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il **loro controllo** in virtù di un accordo contrattuale con l'utente o in forza di legge.

Il regolamento prevede altresì che i fornitori di sistemi di IA ad alto rischio che ritengano o abbiano motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio **non sia conforme** adottino immediatamente le misure correttive necessarie per rendere **conforme** al nuovo regime tale dispositivo, **ritirarlo** o **richiamarlo**, a seconda dei casi. In tal caso i fornitori devono informare i **distributori** del sistema di IA ad alto rischio in questione e, ove applicabile, il **rappresentante** autorizzato e gli **importatori** (articolo 21).
Devono essere inoltre informate immediatamente **le autorità nazionali competenti** degli Stati membri in cui è stato immesso il sistema e, ove applicabile, l'**organismo notificato** che ha rilasciato un **certificato** per il sistema di IA ad alto rischio, in particolare in merito alla non conformità e alle eventuali misure correttive adottate (articolo 22); ulteriori obblighi di cooperazione con le **autorità competenti** sono previsti dall'articolo 23.
Infine l'articolo 24 stabilisce che qualora un sistema di IA ad alto rischio collegato a prodotti ai quali si applicano le discipline di settore in materia di sicurezza (elencate nell'allegato II, sezione A), sia immesso sul mercato o messo in servizio insieme al prodotto fabbricato conformemente a tali atti giuridici e **con il nome** del **fabbricante del prodotto**, quest'ultimo **si assume la responsabilità** della conformità del sistema di IA al regolamento in esame e ha, per quanto riguarda il sistema di IA, gli **stessi obblighi** imposti al fornitore di tale sistema.
Sono altresì previsti obblighi specifici per i **rappresentanti autorizzati** (articolo 25), gli **importatori** (articolo 26), e i **distributori** dei sistemi di IA (articolo 27).
Infine l'articolo 28 **assimila** distributori, importatori, utenti o ulteriori soggetti **ai fornitori** per quanto riguarda gli obblighi a loro carico:

a. se immettono sul mercato o mettono in servizio un sistema di IA ad alto rischio con il **loro nome** o **marchio**;
b. se **modificano** la **finalità** prevista di un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio;
c. se apportano una **modifica sostanziale** al sistema di IA ad alto rischio.

Nelle ipotesi b) o c) il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA ad alto rischio non è più considerato tale ai fini del regolamento.

L'articolo 29 stabilisce gli **obblighi** degli **utenti** dei sistemi di IA ad alto rischio. Essi devono, tra l'altro:

- usare tali sistemi conformemente alle **istruzioni per l'uso** che accompagnano i sistemi;
- nella misura in cui esercitano il **controllo** sui **dati di input**, garantire che tali dati di input siano pertinenti alla luce della finalità prevista del sistema di IA ad alto rischio;
- **monitorare il funzionamento** del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso; se hanno motivo di ritenere che l'uso in conformità alle istruzioni per l'uso possa far sì che il sistema di IA presenti un rischio devono **informare** il fornitore o il distributore e **sospendere** l'uso del sistema; essi devono altresì informare il fornitore o il distributore qualora abbiano individuato un **incidente grave** o un **malfunzionamento** e **interrompere** l'uso del sistema di IA;
- **conservare** i **log** generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log siano sotto il loro controllo, e per un periodo adeguato alle finalità del sistema di IA ad alto rischio e agli obblighi giuridici applicabili a norma del diritto dell'Unione o nazionale.

Relativamente al ciclo di testing*, marcatura, immissione sul mercato e vigilanza dei sistemi di IA, nella citata relazione del Governo si precisa che sarà necessaria un'attenta valutazione di quali e quante strutture/procedure di verifica della conformità e sorveglianza nel mercato interno*

interverranno nel processo.

Autorità di notifica e organismi notificati; norme, valutazione della conformità, certificati, registrazione

Le disposizioni contenute nel Capo 4 (**articoli da 30 a 39**) disciplinano:

- le **autorità di notifica,** enti responsabili della predisposizione e dell'esecuzione delle **procedure** necessarie per la **valutazione**, la designazione e la notifica degli **organismi di valutazione** della conformità e per il loro monitoraggio;
- gli **organismi notificati**, soggetti che effettuano la valutazione di conformità dei sistemi di IA ad alto rischio nelle ipotesi in cui il regolamento richiede per tale procedura l'intervento di un soggetto terzo.

In particolare, ciascuno Stato membro designa o istituisce un'**autorità di notifica**, la quale deve essere organizzata e gestita in modo tale che non sorgano **conflitti di interesse** con gli organismi di valutazione della conformità e che siano salvaguardate **l'obiettività** e **l'imparzialità** della sua attività (**articolo 30**).
Il regolamento prevede i requisiti necessari per gli **organismi notificati**, in particolare per quanto riguarda **l'indipendenza** e la **competenza** (articolo 33).
Ove necessario, la Commissione indaga su tutti i casi in cui vi siano motivi di **dubitare** della conformità di un organismo notificato ai requisiti richiesti dal regolamento (**articolo 37**).
Il regime in materia di valutazione della conformità, di certificazione e di registrazione dei sistemi di IA è contenuto nel Capo 5.
In sintesi, a seconda del tipo di sistema il fornitore segue la procedura di valutazione della conformità basata sul **controllo interno**, ovvero quella basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica, con il **coinvolgimento di un organismo notificato**.

In particolare, i sistemi di IA destinati a essere utilizzati come **componenti** di **sicurezza** di **prodotti** disciplinati conformemente al diritto UE (ad esempio macchine, giocattoli, dispositivi medici, ecc.) sono soggetti agli **stessi meccanismi** di conformità e applicazione ex ante ed ex post dei prodotti di cui sono un componente (fermo restando che tali meccanismi devono assicurare la conformità non soltanto ai requisiti stabiliti dalla normativa settoriale, ma anche a quelli testé indicati in materia di IA).

Per quanto riguarda i sistemi di IA ad alto rischio indipendenti di cui all'allegato III, la proposta prevede espressamente che la maggior parte dei sistemi sia soggetta a una valutazione di conformità basata sul **controllo interno** (articolo 43, paragrafo 2).

Secondo quanto precisato dalla Commissione europea nella relazione introduttiva, farebbero eccezione i **sistemi di identificazione e categorizzazione biometrica** delle persone fisiche, in quanto soggetti a una valutazione di conformità da parte di terzi.

Tuttavia si segnala che l'articolo 43, paragrafo 1, prevede per queste ultime tecnologie la possibilità di **optare** tra il processo valutativo da parte di un **organismo notificato** o la valutazione di conformità basata sul **controllo interno** nei casi in cui il fornitore abbia impiegato **standard armonizzati** o – se applicabili - **specifiche comuni**.

Al riguardo, si segnala l'opportunità di acquisire elementi di chiarimento sul perimetro dei sistemi di IA soggetti a valutazione di conformità che richiedono l'intervento di un organismo notificato e su quello dei sistemi relativi a tecnologie in regime di autocontrollo.
La questione è peraltro oggetto di dibattito, atteso che nel parere adottato il 22 settembre 2021 il Comitato economico e sociale europeo ha sottolineato che "la complessità dei requisiti e degli obblighi di informazione, in aggiunta all'autovalutazione, rischia di banalizzare questo processo, riducendolo a una lista di controllo dove un semplice "sì" o "no" potrebbe essere sufficiente per soddisfare i requisiti". Ciò premesso, "il CESE raccomanda di rendere ***obbligatorie le valutazioni da parte di terzi per tutta l'IA ad alto rischio****".*
L'articolo 48 prevede, tra l'altro, che il fornitore compili una **dichiarazione scritta di conformità UE** (ai requisiti previsti dal regolamento) per ciascun sistema di IA e la tenga a disposizione delle autorità nazionali competenti per **dieci anni** dalla data in cui il sistema di IA è stato

immesso sul mercato, a seguito della quale il fornitore si assume la **responsabilità** della conformità a tali requisiti. Infine l'articolo 49 prevede la **marcatura** CE del prodotto di IA, in conformità con la disciplina già prevista in altri atti dell'UE, come il regolamento (CE) n. 765/2008, che pone norme in materia di **accreditamento** e **vigilanza** del mercato per quanto riguarda la commercializzazione dei **prodotti**, o la direttiva 2009/48/CE sulla **sicurezza** dei **giocattoli**.

Obblighi di trasparenza per determinati sistemi di IA

Il titolo IV, costituito dal solo **articolo 52**, riguarda alcuni sistemi di IA considerati a rischio limitato. Si prevede, in particolare, che i fornitori garantiscono che i sistemi di IA destinati a **interagire** con le **persone fisiche** (al di fuori di quelli utilizzati ai fini di attività di prevenzione e contrasto dei reati) siano progettati e sviluppati in modo tale che le persone fisiche siano **informate** del fatto di stare interagendo con un sistema di IA, a meno che ciò **non risulti evidente** dalle circostanze e dal contesto di utilizzo.
Simile obbligo di **trasparenza** è previsto dalla norma anche per quanto riguarda i *deepfake* (sistemi di IA che generano o manipolano immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona) i quali sono tenuti a rendere noto che il contenuto è stato **generato** o **manipolato artificialmente**.

Misure a sostegno dell'innovazione

Le disposizioni contenute nel titolo V, tra l'altro, incoraggiano le autorità nazionali competenti a creare spazi di **sperimentazione normativa** per l'IA volti a creare un ambiente controllato per sottoporre a prova tecnologie innovative per un periodo di tempo limitato sulla base di un piano di prova concordato con le autorità competenti. Sono altresì previste misure per ridurre gli oneri normativi per le PMI e le *start-up*.

In particolare, l'**articolo 55** obbliga gli Stati membri a:

- fornire ai fornitori di **piccole dimensioni** e alle *start-up* un **accesso prioritario** agli spazi di sperimentazione normativa per l'IA nella misura in cui essi soddisfano le condizioni di ammissibilità;
- organizzare specifiche attività di **sensibilizzazione** sull'applicazione del regolamento adattate alle esigenze dei fornitori di **piccole dimensioni** e degli utenti;
- ove opportuno, istituire un canale dedicato per la **comunicazione** con i fornitori di **piccole dimensioni**, gli utenti e altri innovatori, al fine di fornire orientamenti e rispondere alle domande sull'attuazione del regolamento.

Inoltre nel fissare le tariffe per la valutazione della conformità la proposta prevede che si debba tener conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni, **riducendo** tali **tariffe** proporzionalmente alle loro **dimensioni** e alle dimensioni del loro mercato.

Governance e attuazione

Il titolo VI istituisce un sistema di *governance* articolato a livello di Unione e nazionale. In particolare, si istituisce un **comitato europeo** per l'intelligenza artificiale, con il compito di facilitare l'attuazione del regolamento e sostenere la cooperazione tra le **autorità nazionali** di **controllo** e la Commissione, nonché di fornire consulenza e competenze alla Commissione e di consentire la condivisione delle migliori pratiche tra gli Stati membri (**articoli da 56 a 58**).
L'**articolo 59** prevede inoltre che ciascuno Stato membro istituisca o designi **autorità nazionali competenti** al fine di garantire l'**applicazione** e l'**attuazione** del regolamento; tali organismi sono organizzati e gestiti in modo che sia salvaguardata l'**obiettività** e l'**imparzialità** dei loro compiti e attività. Ciascuno Stato membro deve designare un'autorità nazionale di **controllo** tra le autorità nazionali competenti.
L'autorità nazionale di controllo agisce in qualità di **autorità di notifica** e di **autorità di vigilanza del mercato**, a meno che uno Stato membro non abbia motivi organizzativi e amministrativi per designare **più di un'autorità**. In tal caso gli Stati devono comunicare i motivi

che giustificano la designazione di più autorità

Le autorità nazionali competenti devono disporre di **risorse finanziarie** e **umane** adeguate per svolgere i loro compiti (in particolare, sufficiente personale permanentemente disponibile, dotato di competenza in materia di **tecnologie**, **dati** e **calcolo**, diritti fondamentali, rischi per la salute e la sicurezza, etc.).

Il ruolo delle autorità nazionali include la prestazione di **orientamenti** e **consulenza** sull'attuazione del regolamento, anche ai fornitori di piccole dimensioni, eventualmente consultando autorità con competenze diverse laddove sia richiesta l'attuazione di altre norme di settore. Gli Stati membri possono inoltre istituire un **punto di contatto centrale** per la comunicazione con gli operatori.

Nella relazione citata, il Governo sottolinea la complessità del meccanismo di governance, il quale sposterebbe sulle autorità nazionali una serie di responsabilità e competenze al momento difficilmente rilevabili negli Stati membri. A tal proposito secondo il Governo l'adeguamento potrebbe prevedere ingenti oneri amministrativi e tempi lunghi di attuazione.

Il Garante europeo della protezione dei dati svolge il ruolo di autorità competente per la vigilanza delle istituzioni, delle agenzie e degli organismi dell'Unione nei casi in cui essi rientrano nell'ambito di applicazione del regolamento (**articolo 59, paragrafo 8**).

Il titolo VII prevede la creazione di una **banca dati** a livello dell'UE per i sistemi di IA ad alto rischio indipendenti che presentano particolari implicazioni in relazione ai diritti fondamentali, gestita dalla Commissione e alimentata con i dati messi a disposizione dai fornitori dei sistemi di IA, tenuti a registrare i propri sistemi prima di immetterli sul mercato o altrimenti metterli in servizio (**articolo 60**).

Il titolo VIII stabilisce gli obblighi in materia di **monitoraggio** e **segnalazione** per i fornitori di sistemi di IA per quanto riguarda il monitoraggio successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito.

In particolare, ai sensi dell'**articolo 62**, i fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi **incidente grave** o **malfunzionamento** di tali sistemi che costituisca una violazione degli **obblighi** previsti dal diritto dell'Unione intesi a tutelare i **diritti fondamentali** alle **autorità di vigilanza del mercato** degli Stati membri in cui tali incidenti o violazioni si sono verificati.

Tale notifica è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente o il malfunzionamento o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, **non oltre 15 giorni** dopo che è venuto a conoscenza dell'incidente grave o del malfunzionamento.

Le autorità di vigilanza del mercato, oltre ai poteri già definiti dalla disciplina generale sulla conformità dei prodotti, hanno il potere di indagare in merito al rispetto degli **obblighi** e dei **requisiti** per tutti i sistemi di IA ad alto rischio già immessi sul mercato.

In particolare, ai sensi dell'**articolo 67**, se, dopo aver effettuato una valutazione l'autorità di vigilanza del mercato di uno Stato membro ritiene che, sebbene **conforme** al regolamento, il sistema di IA presenti un **rischio** per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore pertinente di adottare **tutte le misure adeguate** a far sì che il sistema di IA, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio o che sia, a seconda dei casi, **ritirato** dal mercato o **richiamato** entro un termine ragionevole, proporzionato alla natura del rischio.

Il sistema di sanzioni delineato dall'**articolo 71** prevede per le violazioni più gravi del regolamento (ad esempio, inosservanza del divieto delle pratiche di intelligenza artificiale indicate all'articolo 5) sanzioni amministrative pecuniarie fino a **30 milioni di euro** o, se l'autore del reato è una società, fino al **6 per cento** del **fatturato mondiale** totale annuo dell'esercizio precedente, se superiore. Per inosservanze ritenute meno gravi le soglie scendono a **20 milioni** di euro o al 4 per cento del fatturato. La fornitura di **informazioni inesatte**, **incomplete** o **fuorvianti** agli organismi notificati e alle autorità nazionali competenti è soggetta a sanzioni amministrative pecuniarie fino a **10 milioni** o, se l'autore del reato è una società, fino al **2 per cento** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Relazione con altri atti UE

La proposta di regolamento sull'IA è uno degli atti della Commissione europea volti a dare seguito alle **opzioni strategiche** indicate nel citato **Libro bianco** del 19 febbraio 2020, ritenute idonee a realizzare un ecosistema in materia di IA contraddistinto da **eccellenza** e **fiducia**. In particolare, nella relazione allegata al Libro bianco la Commissione europea aveva approfondito il tema delle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica per quanto riguarda i profili di sicurezza e responsabilità. A tal proposito la Commissione aveva annunciato, tra l'altro, l'intenzione di valutare possibili modifiche alla direttiva sulla **responsabilità** per **danno** da prodotti difettosi e di ulteriori possibili interventi mirati di armonizzazione delle norme nazionali in materia di **responsabilità.** In particolare, la Commissione aveva iniziato a considerare se e in quale misura fosse necessario mitigare le conseguenze della complessità del funzionamento dei sistemi di IA adeguando l'**onere della prova** richiesto dalle norme nazionali in materia di responsabilità in relazione ai danni provocati dal funzionamento delle applicazioni di IA.
Sul Libro bianco citato, il 19 maggio 2021, la Commissione IX (Trasporti) della Camera dei deputati ha approvato un documento finale.

Si ricorda altresì che contestualmente alla presentazione del regime in esame, la Commissione europea ha avviato l'iter legislativo di una proposta di regolamento che sostituirebbe l'attuale direttiva sui prodotti macchina (direttiva 2006/42/CE). Il regolamento stabilisce i **requisiti** per la **progettazione** e la **costruzione** di prodotti macchina al fine di consentire la messa a disposizione sul mercato o la messa in servizio di prodotti macchina e stabilisce norme concernenti la **libera circolazione** di prodotti macchina nell'Unione.

Il nuovo regolamento è volto a garantire l'**integrazione sicura** dei sistemi di IA nelle macchine nel loro complesso, tra l'altro chiedendo alle imprese di effettuare un'**unica dichiarazione** della conformità. Esso inoltre mira a **semplificare** gli **oneri** amministrativi e i **costi** per le imprese consentendo formati digitali per la documentazione e adeguando le spese di valutazione della conformità per le PMI.

Il Parlamento europeo è intervenuto nel dibattito in materia di IA, tra l'altro, approvando una serie di **raccomandazioni** su ciò che le norme europee sull'IA dovrebbero ricomprendere, tra l'altro, in materia di **etica**, **responsabilità** e diritti di **proprietà intellettuale**.
In particolare il 20 ottobre 2020 il Parlamento ha adottato le seguenti risoluzioni:

- raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti **etici** dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL));
  Secondo il Parlamento le norme devono essere incentrate sulla **persona**. Le raccomandazioni indicano in che modo si possano assicurare **sicurezza**, **trasparenza** e presa di responsabilità, come evitare la creazione di **pregiudizi** e di **discriminazioni**, stimolare la responsabilità sociale e ambientale e come assicurare il rispetto dei diritti fondamentali.
- raccomandazioni alla Commissione su un regime di **responsabilità civile** per l'intelligenza artificiale (2020/2014(INL));
  Secondo il Parlamento europeo tali regole dovrebbero essere applicate alle attività di IA **fisiche** o **virtuali** che danneggiano o influiscono sulla vita, la salute, l'integrità fisica, il patrimonio, o che causano un rilevante danno immateriale che si traduce in una "perdita economica verificabile". Sebbene le tecnologie di IA ad alto rischio siano ancora rare, la risoluzione stabilisce che gli operatori dovrebbero avere un'assicurazione simile a quella per i veicoli a motore.
- risoluzione sui diritti di **proprietà intellettuale** per lo sviluppo di tecnologie di intelligenza artificiale (2020/2015(INI)).
  Il Parlamento europeo sottolinea l'importanza di distinguere tra le **creazioni umane** ottenute con l'assistenza dell'IA e quelle generate **autonomamente** dall'IA. Secondo la risoluzione l'IA non dovrebbe avere **personalità giuridica**; la proprietà dei diritti di proprietà intellettuale dovrebbe essere quindi concessa **solo agli esseri umani**. Inoltre, nel testo si approfondisce ulteriormente il tema del diritto d'autore, della raccolta di dati, dei segreti commerciali, dell'uso di algoritmi e del *deepfake*.

Si ricorda inoltre che, il 20 gennaio 2021, il Parlamento ha proposto delle linee guida per l'uso dell'intelligenza artificiale in campo **militare e civile**. In particolare, gli eurodeputati hanno sottolineato la necessità di un **controllo umano** sui sistemi di intelligenza artificiale e hanno reiterato la richiesta del Parlamento di **vietare** le **armi letali autonome** abilitate da intelligenza artificiale.
Il 19 maggio 2021, il Parlamento ha approvato la risoluzione sull'uso dell'IA nell'istruzione, nella cultura e nel settore audiovisivo, sottolineando, tra l'altro, che le tecnologie dell'IA devono essere progettate in maniera tale da evitare qualsiasi **pregiudizio** di genere, sociale o culturale e proteggendo al tempo stesso la **diversità**.
Infine, il 6 ottobre 2021, con la risoluzione sull'intelligenza artificiale nel **diritto penale** e il suo utilizzo da parte delle autorità di **polizia** e **giudiziarie** in ambito penale (2020/2016(INI)), il Parlamento europeo ha chiesto forti salvaguardie per i casi in cui vengano utilizzati strumenti di intelligenza artificiale dalle forze dell'ordine, tra cui un divieto permanente di riconoscimento automatizzato delle persone negli spazi pubblici e, per combattere la discriminazione, la trasparenza degli algoritmi.

Si ricorda, da ultimo, che il 18 giugno 2021 il Parlamento europeo ha istituito la **Commissione speciale sul digitale e l'intelligenza artificiale**, che secondo la decisione istitutiva è stata investita delle seguenti attribuzioni:

- analizzare il futuro **impatto** dell'**intelligenza artificiale** nell'era digitale sull'economia dell'UE, in particolare in termini di competenze, occupazione, tecnologia finanziaria, istruzione, salute, trasporti, turismo, agricoltura, ambiente, difesa, industria, energia ed *e-government*;
- esaminare ulteriormente la sfida rappresentata dalla diffusione dell'intelligenza artificiale e il suo contributo al **valore** delle **imprese** e alla **crescita** economica;
- analizzare l'approccio dei **Paesi terzi** e il loro contributo all'integrazione delle azioni dell'UE;
- presentare alle pertinenti Commissioni permanenti del Parlamento una valutazione che definisca gli **obiettivi** comuni dell'UE a medio e lungo termine e includa le fasi principali necessarie per conseguirli, utilizzando come punto di partenza le seguenti comunicazioni della Commissione pubblicate il 19 febbraio 2020: Plasmare il futuro digitale dell'Europa (COM(2020)0067); Una strategia europea per i dati (COM(2020)0066); Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia (COM(2020)0065), Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità (COM(2020)0064).

La Commissione ha organizzato una riunione interparlamentare sui temi dell'intelligenza artificiale e del decennio digitale, svoltasi l'8 novembre 2021 presso la sede di Bruxelles del Parlamento europeo.

Esame presso le Istituzioni dell'UE

Il **Consiglio europeo** del 21-22 ottobre 2021 ha, tra l'altro, sottolineato "l'importanza di compiere **rapidi progressi** circa l'istituzione di un **quadro normativo** favorevole all'innovazione per l'**intelligenza artificiale** al fine di accelerare l'adozione di tale tecnologia da parte del settore pubblico e privato garantendo nel contempo la **sicurezza** e il pieno rispetto dei **diritti fondamentali**".
A tal proposito si ricorda che al **Parlamento europeo**, la proposta di regolamento sull'IA è stata **provvisoriamente assegnata** alla Commissione per il mercato interno e la protezione dei consumatori (IMCO) mentre l'europarlamentare Brando Benifei (S&D, Italia) è stato nominato relatore nel giugno 2021. Tuttavia altre Commissioni hanno rivendicato la competenza sulla disciplina, generando un **conflitto** di **attribuzione**, tuttora in attesa di risoluzione.
Per quanto riguarda il negoziato in corso al **Consiglio dell'UE**, sebbene gli Stati membri abbiano espresso il loro **sostegno** agli **obiettivi generali** della proposta, in tale sede sarebbe

sorta una serie di **interrogativi** in merito alla **definizione** del sistema di IA, all'ambito di **applicazione** del progetto di regolamento e ai **requisiti** per i sistemi di IA ad **alto rischio**.
In particolare, i Ministri delle telecomunicazioni dell'UE hanno tenuto un primo dibattito politico approfondito sulla proposta di legge sull'IA nell'ottobre 2021, accogliendo con favore l'**approccio** della proposta basato sul **rischio**, ma anche sottolineando la necessità di discutere ulteriormente molte questioni, in particolare per quanto riguarda l'ambito di **applicazione** della legge e la definizione dei **termini chiave**.
La Presidenza slovena mira a presentare una **proposta di compromesso** nel corso del mese di **novembre 2021**.
Da ultimo si ricorda che sulla proposta, il 22 settembre 2021, il Comitato economico e sociale europeo ha adottato un parere, con il quale valuta favorevolmente il fatto che il nuovo regime ponga al centro la salute, la sicurezza e i diritti fondamentali e che abbia una portata globale.
Tuttavia il CESE individua aree di miglioramento, tra l'altro, per quanto riguarda:

- l'ambito, la **definizione** e la **chiarezza** delle pratiche di IA vietate;
- le implicazioni delle scelte delle **categorie** effettuate in relazione alla "piramide del rischio";
- l'effetto di **attenuazione** del rischio dei requisiti per l'IA ad alto rischio;
- il **rapporto** con la normativa esistente e altre recenti proposte normative.

Inoltre, con il citato parere il CESE:

- raccomanda di **chiarire** i divieti relativi alle "**tecniche subliminali**" e allo "**sfruttamento delle vulnerabilità**";
- accoglie con favore il **divieto di *social scoring*** e raccomanda che il divieto si estenda alle organizzazioni private e alle autorità semipubbliche;
- chiede sia previsto il **divieto** dell'uso dell'IA per il riconoscimento biometrico automatizzato in spazi accessibili al pubblico e al privato, salvi casi molto specifici;
- accoglie con favore l'allineamento dei requisiti per l'IA ad alto rischio con gli elementi degli **orientamenti etici** per un'IA affidabile e raccomanda di includere **tutti i requisiti** di tali orientamenti;
- raccomanda di rendere obbligatorie le **valutazioni di conformità** di **terze parti** per tutte le IA ad alto rischio e di includere un **meccanismo di reclamo** e **ricorso** per le **organizzazioni** e i **cittadini** che hanno subito **danni** da qualsiasi sistema di IA;
- in linea con il suo approccio all'intelligenza artificiale a lungo auspicato, raccomanda che il nuovo regime preveda che determinate decisioni restino **prerogativa** degli **esseri umani**.

Esame presso altri Parlamenti nazionali

Sulla base dei dati forniti dal sito IPEX, l'esame dell'atto risulta concluso da parte del **Consiglio federale austriaco**, del **Parlamento croato**, del **Senato** e della **Camera dei deputati** della **Repubblica ceca**, del **Senato francese**, delle **Cortes Generales** di Spagna, e del **Senato italiano**.

In particolare, il 28 luglio 2021 la Commissione 14° (Politiche dell'Unione Europea) del Senato ha accertato la corretta individuazione della base giuridica e il rispetto della **sussidiarietà** e della proporzionalità.

Intelligenza Artificiale: La Disciplina e la situazione in Italia (a cura del Servizio Studi della Camera dei deputati)

In Italia, gli ultimi tre anni hanno visto una vasta produzione di documenti provenienti da più direzioni, che hanno cercato di definire tecnicamente che cosa sia l'intelligenza artificiale e si sono proposti di attribuirle una cornice utile a un inquadramento giuridico. Gli atti a tal proposito più significativi sono i seguenti:

1. "**Libro Bianco dell'IA a servizio del cittadino**", pubblicato da **AGID** del 2018, il quale offre una prima panoramica del possibile impiego dell'IA in relazione ai servizi e alla pubblica amministrazione;
2. il Documento "***AI for Future Italy***", che si rivolge alle esigenze di ricerca scientifica ed industriale, alle problematiche di educazione, progettualità e attività congiunta tra istituzioni ed industria, redatto approvato nel maggio 2020 dal **Lab CINI AIIS** (Laboratorio Nazionale di *Artificial Intelligence and Intelligent Systems* del Consorzio interuniversitario nazionale per

l'informatica);

3. il **Programma Nazionale per la Ricerca 2021-2027** del **Ministero dell'Università e della Ricerca,** che prevede diversi grandi domini di azione e, per la prima volta, un ambito specifico "Intelligenza Artificiale" in stretto coordinamento con altri settori, quali la trasformazione digitale, i Big Data, la robotica e la *Cibersicurezza*;
4. il documento "Proposte per una Strategia Italiana per l'intelligenza artificiale" redatto dal "Gruppo di 20 Esperti di Alto Livello" selezionati dal MISE nel dicembre 2018 e presentato per consultazione nel maggio 2019. Il documento finale è stato completato e reso pubblico nel giugno 2020 ed è quindi stata adottata, nel settembre 2020, una bozza di "**Strategia Nazionale per l'intelligenza artificiale**", che è stata sottoposta a consultazione pubblica da parte del **MISE** dal 2 al 31 ottobre 2020.

In particolare, la "**Strategia Nazionale per l'intelligenza artificiale**" individua sei priorità:

1. **l'IA** per **imprese** più competitive;
2. **l'IA** per una **pubblica amministrazione** più moderna;
3. **l'IA** per **cittadini** consapevoli e rafforzati;
4. creazione di **professionisti competenti** in tutti i campi;
5. **regolamentare** al meglio **l'impiego dei dati;**
6. formulare un **programma per l'investimento di risorse e per la *governance***.

Per ciascuna di queste, la strategia individua obiettivi e iniziative. Dalla lettura complessiva della strategia, emerge come gli obiettivi e le iniziative da attuare nei diversi settori siano spesso **interconnessi**. Soltanto un avanzamento coordinato dei vari elementi può permettere un pieno sfruttamento delle potenzialità tecniche di tali tecnologie.

Di seguito si elencano le principali iniziative da attuare:

- accelerazione del cambiamento digitale;
- riorganizzazione degli apparati delle PMI e della PA;
- utilizzo più intelligente dei dati;
- creazione di *data trust* per la sostenibilità;
- partenariato pubblico – privato;
- forte investimento pubblico;
- aggiornamento delle competenze del cittadino;
- piano IA per i consumatori;
- revisione dei corsi di laurea;
- creazione di una cabina di regia per una supervisione dell'avanzamento tecnologico e normativo nel nostro Paese.

Nel mese di **luglio 2021** il Ministero dell'università e della ricerca, il Ministero dello sviluppo economico e il Ministro per l'innovazione tecnologica e la transizione digitale hanno **istituito** un gruppo di lavoro (composto da cinque esperte e quattro esperti) con il compito di sostenere i Ministeri nelle attività di **aggiornamento** della strategia nazionale sull'Intelligenza Artificiale in particolare per renderla **coerente** al **Piano Nazionale di Ripresa e Resilienza** e agli sviluppi recenti a livello Unione Europea.

Nella riunione dell'**11 ottobre 2021** del **Comitato Interministeriale** per la **transizione digitale** (CiTD) presieduto dal Ministro per l'innovazione tecnologica e la transizione digitale, Vittorio Colao, è stato **presentato** il **Programma Strategico Nazionale per l'Intelligenza Artificiale**, realizzato dal Ministero dell'Università e della Ricerca, dal Ministero dello Sviluppo Economico e dal Ministro per l'innovazione tecnologica e la transizione digitale, con il supporto del citato gruppo di esperti in materia.

Si segnala che, in occasione delle comunicazioni in vista della riunione del Consiglio europeo del 21 e 22 ottobre 2021, svoltesi nella seduta dell'Assemblea della Camera e del Senato del 20 ottobre 2021, il Presidente del Consiglio, Mario Draghi, ha sottolineato che "la Strategia nazionale sull'intelligenza artificiale, adottata dal Comitato interministeriale per la transizione digitale costituisce il **quadro** per **migliorare** il **posizionamento competitivo** del Paese".

A livello normativo, la **legge di Bilancio per il 2019** (legge n. 145 del 2018, articolo 1, comma 226), ha previsto l'istituzione di un **Fondo** per favorire lo sviluppo delle tecnologie e delle applicazioni di Intelligenza Artificiale, *blockchain* e *Internet of Things*, con una dotazione di 15 milioni di euro per ciascuno degli anni 2019, 2020 e 2021, per finanziare progetti di ricerca e sfide competitive in questi campi.

In particolare il nuovo Fondo è destinato a finanziare:

a. progetti di ricerca e innovazione da realizzare in Italia ad opera di soggetti pubblici e privati, anche esteri, nelle aree strategiche per lo sviluppo dell'Intelligenza Artificiale, della *blockchain* e dell'*Internet of Things*, funzionali alla competitività del Paese;
b. sfide competitive per il raggiungimento di specifici obiettivi tecnologici e applicativi;
c. il supporto operativo ed amministrativo alla realizzazione di quanto previsto, al fine di valorizzarne i risultati e favorire il loro trasferimento verso il sistema economico produttivo, con particolare attenzione alle piccole e medie imprese.

Per quanto riguarda le **iniziative per la digitalizzazione del Paese** il **Ministro dell'innovazione** ha presentato, a dicembre 2019, il **Piano Italia 2025**, una **strategia complessiva** che indica tre sfide: **società digitale**, **obiettivo innovazione e sviluppo sostenibile e inclusivo**. Per affrontarle, sono delineate 20 azioni di innovazione in diversi ambiti: dall'identità digitale, alla progettazione e sperimentazione di soluzioni di intelligenza artificiale applicata ai procedimenti amministrativi e alla giustizia, in coerenza con i principi europei, all'utilizzo dei *big data* che vengono prodotti ma che sono scarsamente utilizzati dai fornitori di pubblici servizi, alle modalità di trasferimento alla produzione delle capacità innovative della ricerca.