Comunicato stampa del Consiglio dei Ministri n. 177

10 Giugno 2026

Il Consiglio dei Ministri si è riunito mercoledì 10 giugno 2026, alle ore 12.20 a Palazzo Chigi, sotto la presidenza del Presidente Giorgia Meloni. Segretario, il Sottosegretario alla Presidenza Alfredo Mantovano.

.....

DISPOSIZIONI ATTUATIVE IN MATERIA DI INTELLIGENZA ARTIFICIALE

Il pacchetto attuativo in materia di intelligenza artificiale all'ordine del giorno del Consiglio dei Ministri costruisce una risposta normativa organica alla trasformazione tecnologica in corso. La scelta di fondo è promuovere l'innovazione, ma governarla dentro una cornice antropocentrica: l'IA può sostenere decisioni, servizi, formazione e competitività, ma non sostituire la responsabilità umana né comprimere i diritti fondamentali.

La linea comune delle misure è tenere insieme crescita e garanzie: competenze diffuse attraverso formazione mirata sin dalla formazione scolastica, e quindi in base agli specifici settori di appartenenza, tutela della persona nei rapporti di lavoro, accesso effettivo alla giustizia in caso di danno, presidi penali per le violazioni più gravi, autorità coordinate e investimenti capaci di far nascere un sistema nazionale competitivo e sicuro.

Dapprima con la legge n. 132/25 e oggi con I decreti attuativi, l'Italia è all'avanguardia in Europa, perché è Nazione che si dota del primo quadro normativo nazionale organico sull'intelligenza artificiale, pienamente coerente con l'AI Act europeo.

Questi schemi di decreti legislativi hanno conosciuto oggi l'esame preliminare del Consiglio dei Ministri. Poi ci sarà il vaglio delle Commissioni parlamentari; delle Conferenza delle Regioni; delle Authority competenti.

I decreti sono coerenti e conformi all'AI Act europeo (Regolamento UE 2024/1689): non introducono una disciplina alternativa rispetto al quadro europeo, ma ne assicurano l'attuazione nell'ordinamento nazionale.

Sia al momento della redazione del ddl, poi divenuto legge, sia adesso, nel lavoro riguardante i decreti attuativi, il Governo ha mantenuto un dialogo costante con la Commissione europea, a livello informale con riunioni e interlocuzioni, a livello formale, nell'ambito della procedura di notifica di alcune parti della legge IA.

L'attuazione con i decreti delegati fa tesoro di tutte le considerazioni espresse in tali interlocuzioni bilaterali, rispettando la completezza della disciplina UE in materia di definizione dei requisiti fondamentali dei sistemi di IA, senza sovrapposizioni. Dunque, la disciplina attuativa italiana non solo non contrasta col regolamento europeo, ma ne rappresenta il compimento per quelle tecniche di disciplina che rientrano nella competenza dello Stato.

Il tratto qualificante dei decreti delegati, come già era stato della legge 132/25, è l'impostazione antropocentrica. Le norme costruiscono una cornice di garanzie affinché l'innovazione tecnologica resti sempre al servizio della persona, della sua dignità e dei suoi diritti fondamentali. È una impostazione in oggettiva sintonia, pur nella diversità degli ambiti, con l'ispirazione dell'enciclica Magnifica Humanitas di Papa Leone XIV. È comune il messaggio di fondo: la tecnica non può diventare misura dell'umano, né sostituirsi alla coscienza, alla responsabilità e al discernimento dell'uomo. L'intelligenza artificiale è una risorsa solo se resta governata da una visione etica e umanistica, che coniughi innovazione, giustizia, sicurezza e bene comune.

Nel dettaglio, il Consiglio dei Ministri ha esaminato e approvato i seguenti due decreti legislativi:

A) Adeguamento della normativa nazionale alle disposizioni del Regolamento del Parlamento europeo e del Consiglio in materia di poteri delle Autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione (decreto legislativo - esame preliminare)

1. FORMAZIONE
La formazione è la condizione abilitante della strategia nazionale sull'IA: non semplice addestramento tecnico, ma alfabetizzazione critica, consapevolezza dei rischi, capacità di interpretare gli output, responsabilità nell'uso degli strumenti.

1.1 Scuola

Nella scuola l'intelligenza artificiale entra stabilmente nei percorsi educativi come contenuto da conoscere e come strumento per innovare la didattica. Si tratta non di inseguire la tecnologia, ma di rafforzare la missione educativa della scuola. Con l'attuazione della delega si interviene in tutti i settori della formazione scolastica, prevedendo misure specifiche per docenti, studenti ed adulti.

- Aggiornamento delle indicazioni nazionali ("programmi scolastici") del secondo ciclo, per integrare tecnologie avanzate e IA generativa nei percorsi di studio.
- Inserimento dell'IA nell'educazione civica, con attenzione ai profili etici e alla cittadinanza digitale.
- Rafforzamento delle competenze STEAM (scienza, tecnologia, ingegneria, arte e matematica) e dell'orientamento scolastico, per accompagnare gli studenti verso scelte formative e professionali coerenti con le trasformazioni tecnologiche.
- Formazione stabile dei docenti su funzionamento dei sistemi, rischi di errore e distorsione, tutela dei dati e uso responsabile dell'IA.

A supporto delle scuole sono previsti comitati tecnico-etici territoriali, organizzati in rete, con funzioni di indirizzo pedagogico, accompagnamento alla sperimentazione didattica, tutela dei diritti fondamentali e protezione dei dati. Essi contribuiscono anche all'aggiornamento dei regolamenti di istituto, così da rendere l'uso dell'IA sicuro e verificabile.

Importanti novità sono le misure per fronteggiare l'emergenza educativa legata all'abuso di social media, piattaforme digitali e IA. La scuola diventa presidio di prevenzione e benessere digitale: è previsto un piano di formazione dei docenti, con una dotazione di 100 milioni di euro, per rafforzare la capacità del sistema scolastico di prevenire rischi, dipendenze digitali, opacità algoritmica e forme di condizionamento dei minori. Si prevede anche il coinvolgimento delle famiglie al fine di favorire il benessere integrale della persona e dei minori nello spazio digitale.

Le misure si estendono alla formazione degli adulti, con percorsi strutturati di alfabetizzazione e formazione sull'IA, con riconoscimento delle competenze già acquisite e sostegno ai processi di aggiornamento, riqualificazione professionale e reinserimento nel mercato del lavoro.

Si promuove l'integrazione di attività formative dedicate all'Intelligenza Artificiale nei percorsi dell'istruzione superiore e negli ITS Academy per valorizzarne il ruolo

1.2 Università, AFAM, ITS Academy e ricerca

L'IA non riguarda solo i percorsi specialistici: per il suo impatto orizzontale entra, attraverso contenuti adeguati, nei diversi ambiti della formazione universitaria, AFAM e tecnico-professionale.

- Università e istituzioni AFAM integrano attività formative sull'utilizzo sicuro e consapevole dei sistemi di IA, anche con modalità laboratoriali e interdisciplinari.
- I contenuti minimi riguardano funzionamento dei sistemi, interpretazione degli output, profili giuridici, rischi di cybersicurezza e impatto sui diritti.
- I contenuti formativi minimi richiedono anche integrazioni interdisciplinari nei corsi per garantire la comprensione tecnica, l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, e la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni. Le norme introdotte consentono una visione sistemica delle competenze digitali con l'incrocio di competenze (integrazione dei profili etici e giuridici per i corsi

universitari con profilo scientifico; integrazione di profili tecnici per i corsi universitari con prevalente profilo economico o giuridico).
- L'ANVUR monitora la qualità dell'offerta formativa sulla base delle indicazioni del Ministro dell'Università e della ricerca, anche ai fini delle politiche di incentivazione.
- Le attività di divulgazione scientifica, alfabetizzazione e formazione professionale svolte da docenti e ricercatori sono valorizzate anche ai fini della valutazione e della progressione di carriera.
- Gli ITS Academy sono valorizzati come segmento strategico del sistema terziario superiore: integrano formazione, innovazione e fabbisogni produttivi e preparano figure capaci di operare in contesti ad alta intensità tecnologica.

1.3 Pubblica amministrazione: formazione del personale pubblico e raccordo con la SNA

Nella pubblica amministrazione l'intelligenza artificiale può trasformarsi più direttamente in valore pubblico: servizi più semplici, procedimenti più rapidi, migliore capacità di programmazione e decisioni amministrative più comprensibili. Per questo il ruolo del Ministero per la pubblica amministrazione è strategico: non si tratta solo di promuovere corsi sull'uso degli strumenti, ma di orientare l'intera trasformazione delle competenze pubbliche, collegando innovazione tecnologica, semplificazione amministrativa, tutela dei diritti e qualità dei servizi ai cittadini e alle imprese.

Le disposizioni attuative prevedono che le amministrazioni introducano sistemi di IA nelle politiche di reclutamento, formazione e innovazione organizzativa, con l'obiettivo di semplificare l'azione amministrativa e accelerare i procedimenti. In questa cornice, il Ministro per la Pubblica amministrazione assume una funzione di indirizzo e coordinamento: individua fabbisogni comuni, definisce priorità formative, promuove percorsi omogenei tra amministrazioni centrali e territoriali e impedisce che l'adozione dell'IA proceda in modo frammentato o diseguale.

La formazione del personale pubblico diventa così una leva di riforma amministrativa. Deve mettere i dipendenti nelle condizioni di comprendere il funzionamento dei sistemi, interpretarne correttamente gli output, riconoscerne limiti, errori e possibili bias, proteggere dati e sicurezza, e garantire una sorveglianza umana effettiva. L'IA può assistere l'azione amministrativa, ma la responsabilità della decisione deve restare chiara, verificabile e imputabile a persone competenti.
- alfabetizzazione di base per tutti i dipendenti pubblici, per diffondere consapevolezza su opportunità, rischi, trasparenza, protezione dei dati e uso corretto degli strumenti;
- riqualificazione professionale in relazione ai percorsi specialistici nei procedimenti amministrativi, nei servizi al cittadino, nella gestione documentale, nel reclutamento e nell'analisi dei dati;
- alta formazione per dirigenti, responsabili della transizione digitale, uffici del personale e figure chiamate a governare il cambiamento organizzativo e a misurarne l'impatto sul valore pubblico;

Il raccordo con la Scuola Nazionale dell'Amministrazione consentirà di tradurre l'indirizzo del Ministero in moduli e percorsi formativi comuni, aggiornati e differenziati per funzioni e livelli di responsabilità.

1.4 Operatori sanitari

L'intelligenza artificiale assume un rilievo crescente per i medici e i professionisti sanitari, anzitutto come strumento di supporto clinico, consentendo al professionista di prendere decisioni in modo più veloce e appropriato, e di fatto inizia ad essere largamente diffusa. Proprio per questo i decreti delegati prevedono che l'uso dei sistemi deve essere accompagnato da una formazione uniforme, permanente e non limitata alle competenze tecniche.
- La formazione sull'IA è inserita obbligatoriamente, con una specifica percentuale, nel programma di Educazione Continua in Medicina (ECM).
- I contenuti riguardano l'uso operativo degli strumenti, ma anche profili deontologici, etici e giuridici, affinché il professionista mantenga piena responsabilità clinica.
- La formazione sull'IA diventa parte integrante anche della formazione manageriale rivolta ai dirigenti sanitari al fine di garantire maggiore efficienza nella gestione e nell'organizzazione dei servizi sanitari, come ad esempio nel governo delle liste d'attesa e nella razionalizzazione degli sprechi.

Il riferimento alla Piattaforma "MIA", finanziata nell'ambito del PNRR e in sperimentazione da parte di Agenas, conferma la scelta di promuovere strumenti istituzionali affidabili, sicuri e di qualità per il Servizio sanitario nazionale. L'IA può contribuire anche all'efficienza organizzativa, ad esempio nel governo delle liste d'attesa e nella riduzione degli sprechi.

1.5 Professioni

Per le professioni l'intervento introduce l'alfabetizzazione sull'IA nella formazione iniziale e continua. La responsabilità resta in capo al professionista e non si trasferisce allo strumento tecnologico.

- I percorsi formativi degli ordini coprono tre piani: tecnico (funzionamento, potenzialità e limiti dei sistemi), giuridico (regolamento europeo e norme nazionali) e deontologico. Quest'ultimo è il profilo di maggiore rilievo in quanto riguarda la responsabilità del professionista nell'uso dell'IA, gli obblighi informativi verso il cliente e il rispetto del principio antropocentrico della legge 132 del 2025.
- Gli ordini adeguano i propri regolamenti entro sei mesi, secondo le procedure di ciascuna categoria, con il coinvolgimento dell'autorità vigilante quando previsto.
- L'uso dell'IA rileva anche ai fini dell'equo compenso, attraverso parametri commisurati alla classificazione di rischio del sistema impiegato. I decreti che fissano i parametri dell'equo compenso - comprese le tariffe forensi - sono integrati entro dodici mesi. Si assicura, così, che il compenso rifletta l'effettivo apporto professionale e il livello di responsabilità connesso all'uso dell'IA, con parametri trasparenti a tutela tanto del professionista quanto del cliente.

La disciplina evita che l'automazione svaluti il lavoro intellettuale. Al contrario, riconduce l'IA a criteri trasparenti e oggettivi, tutelando tanto il professionista quanto il cliente e applicando il principio antropocentrico alla dimensione professionale.

2. TUTELA DEI LAVORATORI

Nei rapporti di lavoro l'IA può supportare analisi e organizzazione, ma non può sostituire il decisore umano nelle scelte che incidono sui diritti fondamentali della persona.

Con il decreto delegato in materia di Lavoro si afferma un principio essenziale: le decisioni concernenti la costituzione, la modifica o la risoluzione del rapporto di lavoro, compresi provvedimenti disciplinari e licenziamenti, non possono essere adottate unicamente sulla base di un trattamento automatizzato. La decisione finale è riservata a una persona fisica dotata di poteri decisionali.

Con le misure introdotte coi decreti delegate si bilancia innovazione tecnologica e tutela sociale, prevenendo opacità, automatizzazione incontrollata e discriminazioni. L'uso dei sistemi di IA deve avvenire nel rispetto della dignità, della riservatezza e del principio di non discriminazione in conformità con l'AI ACT e le norme della legge italiana sull'intelligenza artificiale.

- Prima dell'avvio del trattamento, il datore di lavoro deve adempiere agli obblighi informativi previsti dalla normativa vigente.
- Il lavoratore ha diritto, su richiesta e con l'intervento di una persona fisica, a una motivazione intelligibile della decisione che lo riguarda.
- La motivazione deve indicare l'eventuale incidenza del sistema di IA sul processo decisionale e i principali parametri considerati.
- Restano fermi il diritto di accesso ai dati.
- Il licenziamento intimato in violazione del divieto di decisione esclusivamente automatizzata è nullo.

La norma non frena l'innovazione nei processi aziendali; ne definisce il perimetro costituzionalmente compatibile. L'IA può essere uno strumento di efficienza e supporto, ma le scelte che incidono sulla vita lavorativa delle persone devono rimanere comprensibili, verificabili e imputabili a un decisore umano.

3. GIUSTIZIA: FORMAZIONE DEI MAGISTRATI

Nel settore giustizia la formazione sull'IA è una condizione di affidabilità fondamentale per assicurare che la decisione sia del magistrato e non della macchina: garantisce che gli strumenti tecnologici restino supporti all'attività umana e non sostituiscano il giudizio del magistrato.

La disciplina prevista dal decreto delegato raccorda la formazione del personale dell'amministrazione di giustizia con gli obblighi europei di alfabetizzazione sull'intelligenza artificiale.

I percorsi formativi si articolano su tre piani: tecnico, per conoscere funzionamento, potenzialità, limiti, tecniche di interrogazione e cybersicurezza; giuridico, per comprendere il Regolamento europeo, la normativa nazionale e i principi della legge n. 132 del 2025; organizzativo e valoriale, per valutare l'impatto sull'amministrazione della giustizia, sul lavoro degli uffici e sui diritti fondamentali.

La formazione è differenziata per funzione e per livello di rischio dei sistemi, aggiornata periodicamente e finalizzata in particolare alla sorveglianza umana sui sistemi ad alto rischio (la giustizia è attività di alto rischio secondo l'AI ACT).

Le nuove norme attribuiscono alla Scuola Superiore della Magistratura il compito di formare i magistrati nell'uso dell'IA, in conformità a linee programmatiche predisposte dal Ministero della Giustizia e a quelle del CSM già previste in generale dalla legge. L'uso dell'IA lascerà naturalmente e doverosamente intatta la discrezionalità del magistrato nell'interpretazione e applicazione della legge, come già previsto dalle norme europee e dalla legge del 2025. Il Comitato direttivo della Scuola in carica sta già svolgendo numerosi corsi formativi sull'IA. Il punto qualificante dei corsi di formazione è che l'IA non sostituisce lo ius dicere: può migliorare organizzazione, ricerca e strumenti di supporto, ma la decisione deve restare presidiata dalla competenza, dall'indipendenza e dalla responsabilità della persona.

4. AUTORITÀ NAZIONALI IA

La governance nazionale dell'IA deve essere chiara, cooperativa e proporzionata: regole certe per tutelare i diritti, senza frenare ricerca, sperimentazione e sviluppo industriale.

Il decreto definisce l'assetto nazionale delle autorità coinvolte nell'attuazione dell'AI Act. Il fulcro della governance è costituito da AgID, quale autorità di notifica, e da ACN, quale autorità di vigilanza del mercato e punto di contatto unico con le istituzioni dell'Unione europea. A queste competenze si affiancano quelle di altre autorità settoriali, in ragione degli ambiti di rischio e delle attività interessate.

- Banca d'Italia, CONSOB e IVASS esercitano funzioni di vigilanza sui sistemi di IA ad alto rischio utilizzati dagli intermediari finanziari e direttamente collegati alla fornitura di servizi finanziari.
- Il Garante per la protezione dei dati personali interviene, per i profili di competenza, sui sistemi di IA ad alto rischio utilizzati in attività di contrasto, gestione delle frontiere, giustizia e democrazia.
- Sono previsti strumenti di cooperazione informativa e operativa tra le autorità, per mettere a fattor comune competenze tecniche e regolatorie.

Il quadro sanzionatorio è graduato e proporzionato. Il decreto si avvale della facoltà prevista dall'AI Act di introdurre limiti massimi inferiori rispetto a quelli europei, calibrando le sanzioni sul grado di responsabilità dei soggetti coinvolti lungo la catena di approvvigionamento dei sistemi di IA.

Anche nei settori più sensibili, come sicurezza pubblica, contrasto dei reati, frontiere e giustizia, il criterio resta quello del controllo qualificato: l'IA può fornire analisi, previsioni e supporto, ma non può fondare decisioni giuridicamente pregiudizievoli in modo automatico né dar luogo a forme di sorveglianza massiva o indiscriminata. Le autorità competenti devono garantire proporzionalità, protezione dei dati e sorveglianza umana effettiva.

Le autorità nazionali trasmettono una relazione annuale, per il tramite del Comitato di coordinamento presso il Dipartimento per la trasformazione digitale, alla Presidenza del Consiglio dei Ministri, anche al fine di valutare eventuali interventi di revisione normativa.

B) Adeguamento della normativa nazionale alle disposizioni del Regolamento del Parlamento europeo e del Consiglio in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale (decreto legislativo - esame preliminare)

5. ATTIVITÀ DI POLIZIA

L'IA può rafforzare prevenzione e contrasto dei fenomeni criminosi, ma solo entro un perimetro rigoroso: uso mirato e proporzionato, divieto di sorveglianza massiva, autorizzazione giudiziaria per l'identificazione biometrica in tempo reale e decisioni sempre presidiate da operatori formati all'uso corretto. Non introducono una sorveglianza biometrica generalizzata, ma si disciplinano due utilizzi mirati, eccezionali e presidiati da garanzie: l'identificazione biometrica remota in tempo reale per finalità tassative di prevenzione di ordine pubblico e sicurezza e ricerca di persone; il riconoscimento facciale a posteriori solo dopo la commissione di un reato e sulla base di elementi oggettivi e verificabili. La decisione resta umana e l'uso è circoscritto da limiti di finalità, tempo, luogo, tracciabilità, protezione dei dati, controllo dell'autorità.

In conformità all'articolo 5 del regolamento europeo, l'articolo 8 consente l'uso in tempo reale soltanto per prevenire minacce specifiche e gravi alla sicurezza e all'ordine pubblico, nonché per la ricerca di persone scomparse o di vittime di sequestro, tratta o sfruttamento sessuale. L'impiego deve servire esclusivamente a confermare l'identità di persone oggetto di interesse; il confronto avviene con banche dati adeguate e costituite lecitamente, mentre è vietato l'uso di banche dati alimentate mediante scraping non mirato. La richiesta all'autorità giudiziaria deve indicare finalità, durata, area, persone interessate, banche dati e tecnologie impiegate; l'autorizzazione è temporaneamente e territorialmente delimitata, riferita a persone specifiche e non può superare quindici giorni, salvo proroga motivata. Nei casi di urgenza è previsto un regime accelerato, ma l'uso deve essere interrotto, con cancellazione dei dati e inutilizzabilità dei risultati, se mancano i presupposti o l'autorizzazione.

In conformità con l'articolo 26, paragrafo 10, dell'Ai ACT, l'articolo 10 disciplina il riconoscimento facciale a posteriori nei sistemi di videosorveglianza già installati in base alla legge. La tecnologia può essere attivata solo dopo la commissione di un reato, anche tentato, per identificare persone indiziate sulla base di documentazione video-fotografica e di elementi oggettivi e verificabili. Il titolare del trattamento è il Ministero dell'interno - Dipartimento della pubblica sicurezza; sono previste valutazione d'impatto e consultazione del Garante, conservazione locale dei dati per sette giorni, log non modificabili per cinque anni, divieto di decisioni pregiudizievoli fondate solo sull'output e divieto assoluto di uso non mirato o generalizzato.

Le disposizioni costruiscono un equilibrio effettivo tra sicurezza e diritti: mettono a disposizione delle Forze di polizia strumenti tecnologicamente avanzati, ma solo come supporto mirato all'azione umana e mai come controllo generalizzato della popolazione.

La conformità dell'articolo 8 discende dal puntuale raccordo con l'articolo 5 dell'AI Act: il regolamento vieta in via generale l'identificazione biometrica remota in tempo reale per finalità di contrasto, ma ammette eccezioni tassative per la ricerca di vittime o persone scomparse, la prevenzione di minacce gravi e specifiche e l'identificazione/localizzazione di soggetti collegati a reati gravi. Lo schema nazionale recepisce questa logica e la rafforza con autorizzazione dell'autorità giudiziaria, delimitazione temporale, geografica e personale, valutazione d'impatto sui diritti fondamentali, log e notifica al Garante.

La conformità dell'articolo 10 si fonda sull'articolo 26, paragrafo 10, dell'AI Act, che disciplina il post-remote biometric identification per finalità di contrasto. La norma nazionale ne riproduce la ratio: uso ex post, mirato, collegato a un reato specifico, fondato su elementi oggettivi e mai utilizzabile in modo indiscriminato.

Inoltre, la previsione che nessuna decisione negativa possa basarsi unicamente sul risultato dell'applicazione dà attuazione al principio europeo di sorveglianza umana e impedisce la delega decisionale all'algoritmo.
Si vieta la costituzione di banche dati biometriche tramite forme di raccolta indiscriminata di informazioni dal web. I punti chiave del decreto delegato in materia di attività di polizia possono così riassumersi:

- IA come supporto alle forze di polizia: le decisioni restano dell'uomo e gli algoritmi forniscono solo indicazioni, previsioni, contenuti e analisi di supporto.

- Regole stringenti per l'identificazione biometrica in tempo reale, ammessa solo in casi eccezionali, con autorizzazione dell'Autorità giudiziaria e per periodi limitati.
- Nessun 'Grande Fratello': sono vietate le banche dati biometriche create con raccolta massiva e non mirata di dati dal web, nonché forme di identificazione biometrica indiscriminata.
- Formazione specifica per gli operatori di polizia.

6. LA TUTELA DEL DANNEGGIATO E LA RESPONSABILITÀ CIVILE

La tutela civile mira a riequilibrare la posizione di chi subisce un danno da un sistema di IA, superando opacità tecnologica e asimmetrie informative senza introdurre nuovi obblighi sostanziali a carico delle imprese.
Il decreto rafforza l'accesso alla giustizia per il danneggiato in una materia tecnicamente complessa, nella quale la ricostruzione del funzionamento del sistema e del nesso causale può risultare particolarmente difficile. L'intervento si concentra sugli strumenti processuali necessari a rendere effettiva la tutela della persona danneggiata.

- Accesso alla documentazione tecnica del sistema, per consentire al danneggiato di comprendere le caratteristiche rilevanti dell'IA utilizzata.
- Presunzione del nesso di causalità, che alleggerisce l'onere probatorio senza eliminarlo integralmente.
- Foro alternativo prossimo alla residenza del danneggiato persona fisica, per rendere meno gravoso l'accesso alla tutela giudiziaria.
- Azione diretta nei confronti dell'assicurazione, quale ulteriore strumento di effettività della tutela risarcitoria.

Il valore dell'intervento è duplice. Da un lato si evita un vuoto di tutela, anche a fronte del ritiro della proposta europea sulla responsabilità da IA; dall'altro mantiene ferma la distinzione tra rafforzamento processuale della posizione della vittima e imposizione di nuovi oneri sostanziali agli operatori. Restano infatti ferme le tutele già previste in materia di protezione dei dati e responsabilità da prodotto.

7. LA RESPONSABILITÀ PENALE (ALTERAZIONE E OMISSIONI DI MISURE DI SICUREZZA)

La risposta penale è circoscritta alle violazioni più gravi: non colpisce la tecnologia in sé, ma le condotte e le omissioni umane che, nei sistemi ad alto rischio, mettono concretamente in pericolo beni primari.

Il decreto introduce un nuovo articolo nel codice penale, il 437-bis, che sanziona l'omessa adozione delle misure di sicurezza nei sistemi di IA ad alto rischio e la loro alterazione quando ne derivi un pericolo concreto per la vita, l'incolumità pubblica o la sicurezza dello Stato.

La previsione risponde a una logica di effettività: nei segmenti in cui l'IA incide su beni di rango primario, la sicurezza non può restare affidata a obblighi solo formali. La responsabilità può estendersi anche all'ente, in base al decreto legislativo n. 231/2001, in modo che il presidio non gravi soltanto sulle persone fisiche ma riguardi anche l'organizzazione che trae vantaggio dall'impiego del sistema.

La punibilità è ancorata al pericolo concreto e, per la forma colposa, alla colpa grave: si evita così di criminalizzare ogni scostamento tecnico o ogni errore operativo, concentrando l'intervento penale sulle violazioni realmente idonee a mettere a rischio vita, incolumità pubblica o sicurezza dello Stato.

Il messaggio è chiaro: l'innovazione è sostenuta, ma chi sviluppa, mette in servizio o utilizza sistemi ad alto rischio deve presidiare seriamente le misure di sicurezza. La responsabilità resta umana e organizzativa, lungo l'intero ciclo di vita del sistema.

Conclusioni:

La regolazione dell'IA è accompagnata da una scelta industriale: rafforzare l'ecosistema nazionale, sostenere start-up e tecnologie strategiche, attrarre capitale privato e consolidare la sovranità digitale italiana ed europea.

L'articolo 23 della legge n. 132/2025 destina una quota delle risorse del Fondo di sostegno al venture capital, fino a un ammontare complessivo di 1 miliardo di euro, allo sviluppo dell'ecosistema nazionale dell'IA. L'obiettivo è promuovere imprese innovative, filiere tecnologiche prioritarie e capacità industriale nei settori strategici.

I dati disponibili mostrano un trend già significativo: il mercato italiano dell'IA ha raggiunto nel 2025 1,8 miliardi di euro, con una crescita del 50% rispetto all'anno precedente; CDP Venture Capital ha già allocato oltre 300 milioni di euro a favore di iniziative IA, sostenendo più di 150 start-up e coinvolgendo circa 20 fondi gestiti da SGR terze, anche attraverso strumenti dedicati come il "Fondo Artificial Intelligence".

Voce	**Dato essenziale**
Risorse programmate	Fino a 1 miliardo di euro dal Fondo di sostegno al venture capital
Risorse già allocate	Oltre 300 milioni di euro; 313 milioni nel dettaglio degli allegati
Imprese sostenute	Oltre 150 start-up e circa 20 fondi gestiti da SGR terze
Capitale umano	Oltre 1.000 occupati altamente qualificati nelle imprese sostenute
Nuovi investimenti	Oltre 500 milioni di euro previsti nel prossimo triennio
Polo SophIA	Circa 30 milioni di euro dal 2026 per IA e cybersicurezza

Gli investimenti stanno abilitando filiere prioritarie come robotica umanoide, guida autonoma, quantum, fotonica per l'high-performance computing e IA verticale. Tra le iniziative già realizzate figurano Generative Bionics, Niulinx, Algorithmiq, CamGraPhIC/2D Photonics, ALLSIDES e Smartness, con capacità di attrarre capitali nazionali e internazionali e creare nuove posizioni altamente specializzate.
A partire dal 2026 si affianca il Polo nazionale di trasferimento tecnologico dedicato all'IA e alla cybersicurezza, "Polo SophIA", come ulteriore leva per sostenere start-up deep tech e trasformare i risultati della ricerca in imprese innovative. La strategia complessiva mira a fare dell'IA non solo un oggetto di regolazione, ma un asse di crescita, competitività e posizionamento internazionale del Paese.
⋆⋆⋆⋆⋆

Il Consiglio dei Ministri è terminato alle ore 13.29.