Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile (Atto n. 418)

Commissioni riunite I Affari Costituzionali e II Giustizia

Camera dei deputati

Roma, 24 luglio 2026

assonime
L'associazione delle imprese

Assonime desidera, innanzitutto, ringraziare per la possibilità di formulare osservazioni e proposte in merito allo Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile (A.G. n. 418).

In via preliminare, intendiamo sottolineare il nostro apprezzamento per l'impegno del legislatore nel favorire la trasparenza nell'uso dei sistemi e dei modelli di IA e la correttezza dei soggetti che a vario titolo partecipano alla catena del valore, così da accrescere la fiducia di cittadini, imprese e pubbliche amministrazioni.

È apprezzabile, inoltre, l'attenzione posta dal legislatore al contemperamento tra esigenze regolatorie parimenti essenziali: da un lato, la tutela dei diritti fondamentali, della sicurezza degli utenti e dell'affidabilità dei sistemi di IA; dall'altro, la necessità di non introdurre elementi di incertezza giuridica che rischino di compromettere investimenti, innovazione e capacità competitiva delle imprese italiane.

Da questo punto di vista, si condivide la scelta di regolare l'utilizzo dei sistemi di IA per l'attività di polizia, la previsione di disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti di sistemi di intelligenza artificiale, unitamente all'introduzione di disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi. Tuttavia, è ferma convinzione di Assonime che per realizzare le suddette esigenze di certezza, chiarezza e prevedibilità delle norme che attuano la delega contenuta nell'art. 24 della legge 23 settembre 2025, n. 132, secondo i principi e i criteri direttivi enunciati ai commi 1, 2, lett. h), 3 e 5, inclusa la lettera d), sussistano taluni margini di miglioramento, relativi all'utilizzo dei sistemi di IA per attività di polizia e ai criteri di ripartizione dell'onere probatorio nelle azioni di responsabilità per danni da IA. Su questi due profili si svolgono di seguito alcune osservazioni.

1. Utilizzo dei sistemi di IA per attività di polizia

Quanto al primo aspetto, riteniamo preliminarmente importante ricordare che i sistemi di intelligenza artificiale, accanto al conseguimento di un'ampia gamma di benefici, possono costituire, indipendentemente dalle finalità del loro utilizzo, un potente strumento per pratiche dannose e contrarie alla libertà, all'uguaglianza e ai diritti fondamentali sanciti dalla Carta dell'Unione europea. Per assicurare un livello elevato di protezione contro gli effetti nocivi dei sistemi di IA, il Regolamento europeo (UE) 2024/1689 del 13 giugno 2024 – c.d. IA Act – promuove la diffusione di un'intelligenza artificiale nel rispetto del principio antropocentrico (art. 1). Come prescritto dalla Carta dei diritti fondamentali dell'UE, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di tali diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale o all'esigenza di proteggere i diritti e le libertà altrui.

L'identificazione biometrica ha un impatto diretto o indiretto su una serie di diritti e libertà fondamentali come la dignità umana, la libertà di movimento, la libertà di riunione, oltre che sulla protezione dei dati personali; pertanto, è essenziale costruire con accuratezza un sistema di regole chiare e prevedibili accompagnato da garanzie adeguate onde evitare un'ingiustificata intrusione nella vita privata delle persone. Ciò è ancor più doveroso quando i sistemi di IA sono utilizzati nel settore delle attività di contrasto dell'illegalità.

Sotto questo punto di vista, le disposizioni dell'articolo 10 relative all'utilizzo di sistemi dotati di tecnologia di riconoscimento facciale a posteriori, sollevano numerose perplessità, in quanto un loro utilizzo generalizzato, senza misure minime di tutela per i diritti e le libertà dell'individuo, potrebbe portare a scenari di sorveglianza di massa indiscriminata, manifestamente non in linea con il requisito di stretta necessità previsto dal diritto europeo.

La norma proposta, risultando assai ampia e non ancorata a criteri oggettivi né a procedure di controllo o autorizzative specifiche, rischia di fatto di andare in questa direzione.

1.1 Condizioni di utilizzo dei sistemi di IA per identificazione biometrica a posteriori (art. 10, commi 1 e 2)

In particolare, l'art. 10 introduce un meccanismo per cui i sistemi di videosorveglianza già autorizzati per legge, ove ricorrano esigenze di ordine e sicurezza pubblica, vengono integrati con tecnologie di riconoscimento facciale a posteriori. Il comma 2 ne consente l'attivazione, dopo la commissione di un reato, per identificare persone già indiziate sulla base di documentazione video-fotografica e sotto la responsabilità di un ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine e della sicurezza pubblica oppure dall'ufficiale di polizia giudiziaria che procede in relazione al fatto di reato.

Sul punto, va considerato anzitutto che l'identificazione biometrica in spazi accessibili al pubblico comporta una profonda ingerenza nei diritti fondamentali; pertanto, al fine di raggiungere un giusto equilibrio tra l'interesse pubblico alla repressione dei reati e l'interesse alla protezione della sfera privata dell'individuo, sarebbe opportuno circoscrivere l'utilizzo di tali strumenti al perseguimento delle fattispecie di reato più gravi. Inoltre, poiché l'attivazione delle tecnologie di riconoscimento facciale finalizzata a identificare persone già indiziate della commissione di un reato presuppone che sia stata già avviata una procedura d'indagine, l'utilizzo di tali strumenti non dovrebbe essere ammesso da parte di ufficiali di pubblica sicurezza.

Inoltre, si sottolinea come la mancata previsione di una procedura autorizzatoria, preventiva o successiva, renda la norma in contrasto con quanto disposto dall'art. 26, par. 10 del Regolamento europeo il quale stabilisce in via generale che l'uso dei sistemi di identificazione biometrica a posteriori richiede un'autorizzazione, preventiva o comunque entro 48 ore, da parte di «un'autorità giudiziaria o amministrativa, la cui decisione sia vincolante e soggetta a controllo giurisdizionale». L'unica deroga all'obbligo di

autorizzazione ammessa riguarda soltanto «l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato».

L'ipotesi considerata è dunque quella di un reato appena consumato in un luogo pubblico, ripreso da telecamere, cui il sistema di riconoscimento facciale consenta di dare un'identità all'autore nell'immediato. Si tratta di una finalità precisa e delimitata nel tempo e negli scopi.

La norma proposta dallo Schema di decreto consente invece un uso investigativo ben più ampio e il sistema di riconoscimento facciale viene utilizzato per confermare la presenza in un certo luogo di qualcuno che sia già stato individuato in precedenza come autore di un reato sulla base di documentazione video-fotografica e di altri elementi oggettivi e verificabili. Non può quindi ravvisarsi la medesima ipotesi prevista dal Regolamento europeo; ne deriva che non può essere invocata la deroga per escludere l'autorizzazione di cui sopra.

Si ritiene pertanto opportuno introdurre un'autorizzazione giudiziaria preventiva che valuti le effettive necessità, emerse nell'ambito d'indagine giudiziaria, che richiedono l'identificazione biometrica. I sistemi di riconoscimento facciale, basati su una tecnologia probabilistica - e quindi suscettibili di errore - dovrebbero essere rigorosamente finalizzati a potenziare gli strumenti a disposizione degli organi di polizia e non a sostituire le tradizionali metodologie investigative.

Una base giuridica che definisca con precisione le condizioni e i limiti entro cui le autorità di polizia possono ricorrere a sistemi di IA e individui garanzie appropriate ed effettive contro un utilizzo abusivo dei dati raccolti sono elementi imprescindibili perché le regole sull'utilizzo di dati biometrici per attività di polizia possano superare il test di proporzionalità.

Proposta

Alla luce di quanto sopra, in merito alle disposizioni contenute nel comma 2 dell'art. 10, è auspicabile:(i) circoscrivere l'utilizzo di tali strumenti al perseguimento di reati particolarmente

gravi: (ii) prevedere che l'utilizzo di tali sistemi sia riservato soltanto agi ufficiali di polizia giudiziari incaricati dell'indagine; (iii) un maggior allineamento con le norme del Regolamento europeo che richiedono l'autorizzazione da parte dell'autorità giudiziaria, preventiva o comunque entro le 48 ore, tranne quando il riconoscimento facciale sia utilizzato per «l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato».

1.2 Modalità di uso (art. 10, comma 3)

Il comma 3 dell'articolo 10 dello Schema di decreto consente l'uso di sistemi di videosorveglianza integrati con tecnologie per il riconoscimento facciale, «in caso di accesso a luoghi o ad eventi rispetto ai quali sussistono esigenze di ordine e sicurezza pubblica».

Si tratta di una norma dalla formulazione eccessivamente vaga e indeterminata, non definendo né chi dovrà valutare l'esistenza in concreto di tali esigenze né sulla base di quali criteri tali esigenze potranno essere ritenute sussistenti, né come e quando tale valutazione dovrà essere resa nota agli interessati.

Inoltre, tale previsione dispone l'acquisizione dei dati biometrici rilevati dalle immagini del volto di chiunque acceda a luoghi o eventi per i quali si presentino esigenze di ordine pubblico – come stadi, stazioni, piazze durante manifestazioni o concerti – e la loro conservazione in un archivio locale nella prospettiva di un futuro utilizzo qualora venga commesso un fatto di reato.

La raccolta di dati biometrici da utilizzare nell'eventualità che sia commesso un reato solleva dubbi di conformità con quanto previsto dall'art. 26, comma 10 del Regolamento europeo in base al quale l'uso di sistemi di IA per l'identificazione biometrica a posteriori «è limitato a quanto strettamente necessario per le indagini su uno specifico reato. In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una

determinata persona scomparsa». Peraltro, anche il considerando 95 dello stesso Regolamento espressamente esclude che i sistemi di identificazione biometrica remota a posteriori vengano utilizzati nel quadro delle attività di contrasto per condurre una sorveglianza indiscriminata.

In altre parole, mentre il Regolamento europeo ammette l'identificazione biometrica a posteriori solo per i sospettati di uno specifico reato già commesso, il comma 3 dell'art. 10 del decreto istituisce una raccolta ex ante, universale e indiscriminata, che prescinde dall'esistenza di qualsiasi reato e di qualsiasi sospettato. Quindi, l'interesse generale di repressione del reato che, a livello europeo, giustificherebbe l'utilizzo dei dati biometrici è in questo caso solo eventuale, non essendosi realizzato nel momento in cui vengono acquisite indiscriminatamente quantità di dati biometrici su vasta scala.

In aggiunta, questo scenario aumenta significativamente il rischio di possibili violazioni dei dati di alto valore, per loro natura univocamente legati all'identità della persona e immodificabili.

Il comma 3 comporta infatti la creazione di numerosi archivi di dati biometrici, per loro natura univocamente legati all'identità di una persona, appartenenti a soggetti, non sospettati di alcun reato, che accedono a luoghi o eventi caratterizzati da esigenze di ordine e sicurezza pubblica.

Va considerato che tali banche dati costituiscono un obiettivo particolarmente allettante per accessi e usi impropri e non autorizzati; con la conseguenza quindi che i soggetti cui si riferiscono i dati raccolti vengono esposti a rischi inaccettabilmente elevati solo per aver partecipato a un evento o avuto accesso in luoghi pubblici.

Peraltro, il comma 12 prevede che siano i gestori dei luoghi in cui si svolgono tali eventi a installare e manutenere i sistemi per il riconoscimento facciale. Si tratta quindi di infrastrutture appartenenti a autorità pubbliche o a soggetti privati, con differenti capacità

in termini di competenze, di risorse tecnologiche ed economiche nonché di ponderazione dei rischi rispetto a eventi di violazione di dati e conseguente perdita irreversibile dei dati biometrici.

Sul punto si ricorda che il Parlamento europeo, nella risoluzione del 6 ottobre 2021, ha espresso profonda preoccupazione con riferimento all'utilizzo di database privati di riconoscimento facciale e ha esortato gli Stati membri a individuare un quadro giuridico comune per l'utilizzo dell'IA nelle attività di contrasto che rispetti appieno l'acquis europeo in materia di protezione dei dati e dei diritti umani (in particolare punto 6 e 34).

Proposta

È auspicabile una profonda revisione del comma 3 al fine di: (i) definire con accuratezza i criteri oggettivi di valutazione delle esigenze che rendano necessario l'utilizzo di sistemi di IA per il riconoscimento facciale; (ii) prevedere una maggiore conformità con il Regolamento europeo nella misura in cui è necessario un collegamento diretto tra l'acquisizione dei dati e l'obiettivo perseguito dall'autorità di contrasto; (iii) valutare la proporzionalità rispetto all'elevato rischio di perdita irreversibile dei dati derivante dalla costituzione di numerosi database privati.

2. Responsabilità per i danni da IA e criteri di ripartizione dell'onere probatorio

La legge delega introduce quale criterio direttivo per l'attuazione del Regolamento europeo quello della «previsione di strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenendo conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal Regolamento (UE) 2024/1689»[1].

[1] Al riguardo, la legge n. 132/2025 individua quale criterio direttivo cui il Governo deve attenersi nell'esercizio della delega quello della "previsione di strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal Regolamento (UE) 2024/1689".

L’articolo 18 dello Schema di decreto introduce una presunzione relativa circa l’esistenza del nesso causale: quando il danno deriva dalla violazione di uno o più obblighi previsti dal Regolamento europeo, il nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria. Ciò significa che il danneggiato non è tenuto a fornire una prova piena della causalità: è sufficiente dimostrare l'esistenza del danno e la violazione di uno degli obblighi previsti dal Regolamento. Sarà invece il convenuto a dover fornire la prova contraria, dimostrando che il danno si sarebbe verificato comunque oppure che esso è riconducibile a cause diverse dalla violazione contestata. La relazione illustrativa chiarisce che l’inversione dell’onere della prova non si estende alla colpa né alla violazione dell’obbligo, che restano oggetto di prova a carico dell’attore.

La disposizione mira ad attenuare le difficoltà che il soggetto danneggiato incontra nel dimostrare il collegamento causale tra la violazione degli obblighi normativi e il danno subito. La scelta di intervenire alleggerendo la prova del nesso causale appare giustificata dal rilievo, già valorizzato in sede europea, che i sistemi di intelligenza artificiale sono frequentemente caratterizzati da opacità, elevata complessità tecnica e difficoltà di comprensione da parte del soggetto danneggiato.

La formulazione contenuta nello Schema di decreto presenta tre distinte criticità.

(i) In primo luogo, la presunzione è collegata indistintamente alla violazione di uno o più obblighi previsti dal Regolamento (UE) 2024/1689, senza distinguere tra obblighi che gravano su soggetti diversi della catena del valore e che perseguono finalità eterogenee. Tale scelta rischia di produrre effetti irragionevoli, poiché attribuisce il medesimo rilievo processuale a violazioni profondamente diverse per natura, funzione e incidenza causale rispetto al danno.

Si pensi, ad esempio, all'obbligo di alfabetizzazione in materia di IA, imposto al deployer dall'art. 4 dell'AI Act, la cui funzione è quella di promuovere un uso consapevole dei sistemi, rispetto agli obblighi gravanti sul fornitore relativi alla governance dei dati, alla gestione del

rischio, alla documentazione tecnica o alle procedure di conformità, che incidono direttamente sulla progettazione, sulla sicurezza e sull'affidabilità del sistema. Equiparare, ai fini dell'operatività della presunzione, la violazione di tali obblighi significa prescindere dalla diversa idoneità causale che essi presentano rispetto alla produzione del danno.

(ii) In secondo luogo, la disposizione rinuncia a valorizzare proprio quell'elemento sostanziale – l'opacità e la complessità tecnica dei sistemi di IA, la c.d. *black box* – che costituisce la principale giustificazione dell'alleggerimento dell'onere probatorio. La difficoltà di ricostruire il funzionamento del sistema e di dimostrare il nesso causale, infatti, è una caratteristica trasversale dell'intelligenza artificiale e non dipende dalla circostanza che il danno sia conseguenza della violazione di uno specifico obbligo previsto dall'AI Act.

Ancorare la presunzione esclusivamente alla violazione degli obblighi imposti dal Regolamento rischia, pertanto, di tradire la *ratio* stessa della disposizione. Ne consegue che potrebbero rimanere escluse dall'ambito applicativo dell'art. 18 ipotesi in cui le difficoltà probatorie sono altrettanto evidenti, se non maggiori, ma nelle quali il danno deriva dall'impiego di sistemi di IA la cui stessa immissione sul mercato o messa in servizio è vietata dal Regolamento. Si pensi ai sistemi di IA che consentono lo *scraping* indiscriminato di immagini facciali per la creazione di banche dati biometriche ovvero a quelli che impiegano tecniche subliminali o manipolative idonee ad alterare significativamente il comportamento delle persone. Tali pratiche sono vietate dall'AI Act in quanto ritenute idonee a determinare un rischio inaccettabile per i diritti fondamentali. Ciononostante, ove non sia configurabile la violazione formale di uno degli obblighi cui l'art. 18 ricollega la presunzione, il soggetto danneggiato potrebbe non beneficiare dell'alleggerimento probatorio, pur trovandosi ad affrontare le medesime difficoltà di dimostrazione del nesso causale derivanti dall'opacità del sistema.

La scelta del legislatore nazionale sembra dunque subordinare l'operatività della presunzione a un criterio formale – la violazione di specifici obblighi regolatori – anziché al

dato sostanziale che ne costituisce il fondamento, ossia l'asimmetria informativa e la peculiare difficoltà probatoria generate dall'utilizzo di sistemi di intelligenza artificiale.

(iii) In terzo luogo, la disposizione non opera alcuna distinzione in ragione del livello di rischio del sistema o modello di IA coinvolto, finendo per assoggettare alla medesima presunzione fattispecie profondamente diverse sotto il profilo della probabilità di causare un danno e dell'intensità degli obblighi normativi applicabili.

La scelta di prescindere dalla classificazione per livelli di rischio introdotta dall'AI Act determina un evidente disallineamento rispetto all'impostazione del legislatore europeo, il quale costruisce l'intera disciplina dell'intelligenza artificiale secondo un approccio *risk-based*, graduando obblighi e controlli in funzione della pericolosità dei sistemi. Tale impostazione appare inoltre poco coerente con i principi che informano il diritto italiano della responsabilità civile. Anche nel nostro ordinamento, infatti, il legislatore tende a modulare gli strumenti di agevolazione probatoria e i regimi di responsabilità in funzione della particolare pericolosità dell'attività svolta o delle caratteristiche del prodotto. Ne sono espressione, seppur in ambiti diversi, la responsabilità per l'esercizio di attività pericolose di cui all'art. 2050 c.c., che giustifica un'inversione dell'onere della prova in ragione del rischio intrinseco dell'attività, e la disciplina della responsabilità per danno da prodotti difettosi, che fonda la tutela sulla difettosità del prodotto e sul conseguente rischio per la sicurezza.

In questa prospettiva, una presunzione di causalità costruita senza alcun riferimento alla rischiosità del sistema di IA o alla sua capacità di incidere sui diritti e sulla sicurezza delle persone può risultare eccessivamente indifferenziata, alterando quel principio di proporzionalità che caratterizza tanto l'AI Act quanto il sistema nazionale della responsabilità civile.

Coerentemente con le considerazioni che precedono, si ritiene auspicabile che la disciplina della responsabilità civile per i danni cagionati da sistemi di intelligenza artificiale venga ricondotta nell’alveo delle categorie già conosciute dall'ordinamento, graduando

l'operatività della presunzione in relazione al livello di rischio del sistema o, quantomeno, alla natura degli obblighi violati e alla loro effettiva incidenza sulla produzione del danno.

In particolare, l'attività di sviluppo, immissione sul mercato, distribuzione e impiego di sistemi e modelli di IA ad alto rischio dovrebbe essere ricondotta nell'ambito dell'art. 2050 c.c., relativo alla responsabilità per l'esercizio di attività pericolose. Tale qualificazione trova fondamento nella peculiare attitudine di tali sistemi a incidere sui diritti fondamentali della persona, circostanza che costituisce il presupposto stesso della loro classificazione come *high-risk* da parte dell'AI Act. Per l'effetto, il produttore, distributore, o utilizzatore commerciale di un sistema ad alto rischio[2] sarà tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno. Tale prova liberatoria dovrebbe comprendere non soltanto il rispetto degli obblighi imposti dall'AI Act, ma anche l'adozione di ogni ulteriore cautela suggerita dallo stato dell'arte, dalle conoscenze tecnico-scientifiche e dalle circostanze del caso concreto, purché concretamente esigibile.

Ove invece non ricorra il presupposto dell'alto rischio, i principi europei e nazionali in materia di responsabilità da prodotto difettoso dovrebbero costituire il parametro di riferimento per il legislatore, essendo pacifico che ogni modello o sistema di IA, a prescindere dalla

[2] Paragrafo 21 della sentenza Cass. civ., Sez. III, 7 novembre 2019, n. 28626: "A tale diversificazione di fasi e di disponibilità del prodotto pericoloso, almeno finché il ciclo della sua trasformazione non è esaurito, non può che corrispondere una conseguente diversificazione della responsabilità dei diversi soggetti che quelle fasi gestiscono in autonomia gli uni dagli altri, ciascuno assumendo una quota ben determinata e ben prevedibile del relativo rischio di impresa connesso alla produzione di beni mediante impiego di materiali pericolosi."
Paragrafo 22 della sentenza Cass. civ., Sez. III, 7 novembre 2019, n. 28626: "In particolare, tali diverse fasi debbono essere considerate, di norma (e con l'eccezione che subito si vedrà) ed ai fini della responsabilità da attività pericolosa tra i diversi soggetti coinvolti professionalmente nel medesimo processo produttivo, l'una indipendente dall'altra ed ognuna caratterizzata da oneri di precauzione incombenti a ciascun soggetto titolare del potere di impresa di volta in volta esercitato, parametrati allo stato di avanzamento della lavorazione ed almeno tendenzialmente idonei a scongiurare i rischi propri di quella fase: diversamente, si tratterebbe di estendere incongruamente la nozione di attività pericolosa e la relativa severa responsabilità sostanzialmente oggettiva anche alla circolazione del bene pericoloso e senza alcuna limitazione, con insostenibile equiparazione alla responsabilità da prodotto difettoso o da vizi della cosa venduta, che hanno però presupposti molto meno gravosi per il produttore e per il distributore rispetto alla presunzione di cui all'art. 2050 c.c.".

pericolosità ed indipendentemente dalla violazione di obblighi di legge, possa cagionare un danno risarcibile[3].

Sotto questo profilo, la disciplina del prodotto difettoso offre un paradigma maggiormente coerente rispetto alla presunzione generalizzata prevista dall'art. 18 dello schema di decreto. Pur presentando limiti applicativi – in particolare con riguardo alle categorie di danno risarcibili e ai soggetti legittimati ad agire – essa appare strutturalmente più adatta a disciplinare i danni derivanti dall'impiego di sistemi di IA, in quanto per un verso già oggi si estendono all'intera catena del valore[4] e per altro verso introducono criteri di valutazione della difettosità fortemente sintonizzati sulle caratteristiche dell'IA[5].

Una simile ricostruzione consentirebbe di mantenere la disciplina nazionale all'interno delle categorie consolidate della responsabilità civile, evitando l'introduzione di una presunzione di causalità uniforme e svincolata dal livello di rischio del sistema. Al contempo, essa garantirebbe una maggiore coerenza sia con l'impostazione *risk-based* dell'AI Act sia con la logica sottesa al nuovo quadro europeo della responsabilità da prodotto difettoso, nel quale la tutela risarcitoria viene modulata in funzione della concreta pericolosità dell'attività o delle caratteristiche del prodotto.

---

[3] La Direttiva (UE) 2024/2853 del 23 ottobre 2024, che abroga la Direttiva 85/374/CEE in materia di danni da prodotti difettosi, infatti, già si applica ai software e per questa via ai modelli e sistemi di intelligenza artificiale (considerando 3), sia che operino come moduli a sé stanti, sia che siano integrati come componenti in altri dispositivi o reti (considerando 6).

[4] Cassazione civile sez. III, 9/04/2026, n. 9001.

[5] In particolare, l'articolo 7 della Direttiva del 2024 in via di recepimento in Italia stabilisce che, nel valutare se un prodotto offra la sicurezza che ci si può legittimamente attendere, rilevano circostanze specifiche, quali: i) la capacità di "continuare a imparare o acquisire nuove funzionalità dopo la sua immissione sul mercato o messa in servizio"; ii) specifiche presunzioni relative (iuris tantum) di difettosità e di causalità a favore del danneggiato. In particolare, il comma 2 prevede che il carattere difettoso del prodotto si presume qualora il convenuto ometta di divulgare i pertinenti elementi di prova ordinati dal giudice, oppure qualora l'attore dimostri la violazione di requisiti obbligatori di sicurezza o un malfunzionamento evidente del prodotto in condizioni d'uso ordinarie o prevedibili. Il comma 3 prevede che il legame eziologico si presume per il solo fatto che il prodotto sia difettoso e che la natura del danno sia compatibile con tale difetto. In base al comma 4, il giudice presume la difettosità, il nesso causale, o entrambi, qualora il danneggiato incontri difficoltà eccessive – dovute in particolare alla complessità tecnica o scientifica – nel fornirne la prova, a condizione che dimostri la mera probabilità del difetto o del nesso di causalità.

Così ricalibrati gli assi della responsabilità civile, l'art. 19 dello Schema di decreto assumerebbe la funzione che gli è propria di norma di chiusura del sistema. La disposizione prevede infatti che la conformità del sistema di IA agli obblighi stabiliti dal Regolamento (UE) 2024/1689, ancorché attestata mediante le procedure di valutazione della conformità previste dallo stesso Regolamento, non esclude di per sé la responsabilità del convenuto.

In tale prospettiva, la norma ribadisce un principio consolidato nel diritto della responsabilità civile: il rispetto degli standard normativi e delle prescrizioni amministrative costituisce certamente un elemento rilevante nella valutazione della condotta del convenuto, ma non è sufficiente, di per sé, a escludere la responsabilità risarcitoria. La conformità all'AI Act rappresenta tuttavia un importante indice dell'adozione delle cautele richieste dal legislatore europeo e della condotta diligente, pur non traducendosi in una forma di *safe harbour* o di immunità civilistica automatica.

L'accertamento della responsabilità dovrà pertanto essere condotto secondo le ordinarie regole del diritto civile, verificando, a seconda dei casi, la sussistenza dei presupposti dell'art. 2050 c.c. ovvero della disciplina sulla responsabilità da prodotto difettoso. In tale contesto, la conformità agli obblighi dell'AI Act potrà assumere rilievo quale elemento di prova dell'adozione delle misure diligenti richieste al produttore, al distributore o al *deployer*, senza tuttavia precludere al giudice di accertare l'esistenza di ulteriori cautele esigibili o di un difetto di sicurezza del sistema.

L'art. 19 viene a svolgere così una funzione di raccordo tra la disciplina pubblicistica dell'AI Act e il diritto comune della responsabilità civile, evitando che il superamento delle procedure di conformità previste dal Regolamento europeo si traduca automaticamente nell'esclusione dell'obbligo risarcitorio, pur rappresentando un parametro della diligenza della condotta per i soggetti della catena.

Alla luce di quanto sopra, è auspicabile che la disciplina all’esame venga orientata verso un modello di responsabilità civile coerente con la logica del Regolamento (UE) 2024/1689 e con le categorie consolidate del diritto civile. Un tale assetto consentirebbe di coniugare un

elevato livello di tutela dei soggetti danneggiati con l'esigenza di assicurare agli operatori un quadro regolatorio prevedibile, evitando che la stratificazione delle discipline applicabili all'intelligenza artificiale determini incertezze interpretative e un aggravio ingiustificato del rischio giuridico per le imprese.

Proposta

Si formulano le seguenti proposte di modifica dello Schema di decreto:

(i) *Ricalibrare l'ambito applicativo dell'art. 18 alla luce dell'approccio* risk-based *dell'AI Act e delle categorie della responsabilità civile nazionale**.*** *In particolare, l'art. 18 dovrebbe escludere dal proprio ambito di applicazione i sistemi e i modelli qualificati come ad alto rischio ai sensi del Regolamento (UE) 2024/1689, per i quali troverebbe invece applicazione il regime di cui all'art. 2050 c.c., in ragione della loro intrinseca attitudine a incidere sui diritti fondamentali e della conseguente qualificazione dell'attività come pericolosa. Per i sistemi che non ricadono nella categoria dell'alto rischio, la disciplina potrebbe essere modellata sulla nuova direttiva europea in materia di responsabilità da prodotto difettoso (direttiva (UE) 2024/2853 del 23 ottobre 2024[6]), adattandone tuttavia l'ambito soggettivo alle peculiarità dell'intelligenza artificiale. In questa prospettiva, la tutela non dovrebbe essere limitata ai consumatori, ma estesa anche agli operatori economici che subiscano un danno, mentre la nozione di produttore dovrebbe comprendere, in conformità all'evoluzione della giurisprudenza e alla struttura della filiera dell'IA, tutti i soggetti che, assumendo obblighi di progettazione, controllo o precauzione, esercitano un'effettiva influenza sulla sicurezza del sistema.*

(ii) Attribuire rilievo esimente alla governance dell'intelligenza artificiale effettivamente implementata in conformità con la regolazione della materia. La disciplina dovrebbe valorizzare, nella valutazione della responsabilità, non il mero rispetto formale degli obblighi

[6] Questa direttiva dovrà essere attuata entro il 9 dicembre 2026. La delega al recepimento è contenuta nella legge 17 marzo 2026, n. 36 (Legge di delegazione europea 2025), senza principi e criteri direttivi specifici.

previsti dall'AI Act, bensì l'effettiva adozione, attuazione e documentazione di un sistema interno di governance dell'intelligenza artificiale conforme, in particolare, agli articoli 4 e 26 del Regolamento. In tale prospettiva, una compliance sostanziale, dimostrabile attraverso adeguate procedure di gestione del rischio, formazione del personale, monitoraggio continuo e tracciabilità delle decisioni, dovrebbe assumere rilievo sia ai fini del superamento delle presunzioni probatorie sia quale elemento idoneo a dimostrare l'adozione di tutte le misure concretamente esigibili per prevenire il danno[7].

[7] Per una conferma indiretta e a contrario, cfr. art. 17, comma 5 dello Schema di decreto, in base al quale il giudice può desumere argomenti di prova dall'inottemperanza all'ordine di disclosure in giudizio.