

Focus Team Assicurazioni
Focus Team Innovazione e Trasformazione Digitale
26 Ottobre 2026

Focus Team Assicurazioni



Focus Team Leader

Stefano Micheli

stefano.micheli@belex.com

Tel. +39-02-771131

**Focus Team Innovazione
e Trasformazione Digitale**



Focus Team Leader

Tommaso Faelli

tommaso.faelli@belex.com

Tel. +39 02 771131



Autori

Francesco Faccendini

francesco.faccendini@belex.com

Tel. +39-02-771131

Giulia Tenaglia

giulia.tenaglia@belex.com

Tel. +39-02-771131

Elisa Simionato

elisa.simionato@belex.com

Tel. +39-02-771131

Matteo Furlani

matteo.furlani@belex.com

Tel. +39-02-771131

Responsabilità civile da utilizzo di sistemi di intelligenza artificiale

1. Introduzione

Il 30 settembre è entrato in vigore il D.lgs. 9 settembre 2026, n. 160 (il “Decreto”) ⁽¹⁾ di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 (“AI Act”). Il Decreto tocca diversi temi ⁽²⁾ in esecuzione delle deleghe previste dalla c.d. Legge italiana sull’intelligenza artificiale (legge 23 settembre 2025, n. 132) e disciplina gli strumenti di tutela civile connessi all’impiego illecito di sistemi di IA con l’introduzione dell’azione diretta nei confronti dell’assicurazione ⁽³⁾.

Le previsioni del Decreto sono al momento l’unica disciplina specifica in materia di IA e responsabilità civile. L’AI Act, infatti, contiene norme di regolazione del mercato e sicurezza del prodotto, la cui efficacia è garantita da un sistema di sanzioni amministrative applicate da autorità indipendenti, ma non regola un’eventuale responsabilità civile (tematica non

⁽¹⁾ Il testo del Decreto è disponibile al seguente [link](#).

⁽²⁾ Il Decreto, in particolare (oltre alla responsabilità civile e alla connessa assicurazione oggetto di questo contributo), tocca i temi di: (i) IA nell’attività di polizia; (ii) ricerca, sperimentazione e formazione; (iii) dati biometrici e identificazione remota in tempo reale; (iv) riconoscimento facciale a posteriori; (v) nuovi reati e nuove regole nel procedimento penale; (vi) responsabilità degli enti.

⁽³⁾ Si segnala inoltre che è stato recentissimamente introdotto il D.lgs. 7 ottobre 2026, n. 179 (il cui testo è disponibile al seguente [link](#)). Fra le principali novità, tale decreto ha attribuito competenze specifiche alle autorità di vigilanza individuando, oltre all’Agenzia per l’Italia Digitale (AgID) e all’Agenzia per la cybersicurezza nazionale (ACN) quali autorità nazionali per l’intelligenza artificiale, anche IVASS quale autorità competente sui sistemi di IA ad alto rischio utilizzati nell’esercizio dell’attività assicurativa o riassicurativa e di distribuzione di prodotti assicurativi, ferme le competenze attribuite al Garante per la protezione dei dati personali nei casi previsti dall’AI Act (art. 5).

Inoltre, il decreto del 7 ottobre 2026 introduce misure sanzionatorie per le violazioni dell’AI Act irrogabili dalle suddette autorità. Le sanzioni possono essere non pecuniarie e in tal caso (a) consistere nell’ordine di eliminare le infrazioni e di astenersi dal ripeterle, anche indicando le misure da adottare e il termine per attuarle; o, (b) qualora l’infrazione contestata sia cessata, consistere in una dichiarazione pubblica avente ad oggetto la violazione commessa e il soggetto responsabile (art. 22). In alternativa, le autorità possono imporre una sanzione amministrativa pecuniaria fino a 35 milioni di Euro o, se superiore, fino al 7% del fatturato mondiale totale annuo, salvo che la violazione non costituisca un reato.

specificamente disciplinata nemmeno nel c.d. Digital Omnibus ⁽⁴⁾ che aveva modificato l'AI Act).

A livello europeo, vi era stato un tentativo di regolamentare la responsabilità civile nel contesto dell'utilizzo dell'IA con la proposta di *AI Liability Directive* (COM(2022) 496), che era incentrata sull'accesso probatorio ai dati dei sistemi ad alto rischio e su una presunzione relativa di causalità. Tuttavia, il tentativo si è arrestato con il ritiro formale della proposta ⁽⁵⁾.

2. Le previsioni del Decreto in materia di responsabilità civile e di inversione dell'onere della prova

Nel contesto in esame, le novità introdotte dal Decreto si articolano lungo tre direttrici principali: l'accesso alle prove, la presunzione del nesso di causalità e l'introduzione di un'azione diretta verso l'assicuratore.

Quanto all'accesso alle prove, l'art. 17 del Decreto attribuisce al giudice, su istanza del danneggiato, il potere di ordinare l'esibizione di elementi di prova relativi al funzionamento del sistema di IA (tra cui registri, documentazione tecnica e informazioni sulla supervisione umana). In caso di inadempimento dell'ordine, il giudice può desumere argomenti di prova ai sensi dell'art. 116 c.p.c. o, in caso di mancata esibizione della documentazione richiesta, ritenere come ammessi i fatti allegati dall'istante.

L'art. 18 del Decreto introduce poi la presunzione, salvo prova contraria, del nesso causale tra la violazione di un obbligo previsto dall'AI Act e il danno subito. L'inversione dell'onere della prova sul nesso causale non si estende comunque alla colpa né alla violazione dell'obbligo, che restano oggetto di prova a carico dell'attore ⁽⁶⁾. L'art. 19 del Decreto chiarisce inoltre che la conformità del sistema di IA all'AI Act, anche se certificata, non esclude, di per sé, la responsabilità del convenuto.

A completamento della tutela, l'art. 20 del Decreto introduce l'azione diretta del danneggiato nei confronti dell'impresa di assicurazione della responsabilità civile del danneggiante (cfr. paragrafo seguente).

3. L'azione diretta nei confronti dell'impresa di assicurazione

Come anticipato nel paragrafo precedente, una delle principali novità introdotte dal Decreto è l'azione diretta nei confronti dell'impresa di assicurazione del danneggiante. L'importanza di tale meccanismo è particolarmente rilevante se si considera che, nel sistema civilistico ordinario in materia di assicurazione della responsabilità civile di cui all'art. 1917 c.c., il danneggiato non dispone di un'azione diretta contro l'assicuratore,

⁽⁴⁾ Proposta COM(2025) 836, procedura 2025/0359(COD).

⁽⁵⁾ Si veda [Withdrawal of Commission Proposal](#).

⁽⁶⁾ Come precisato dalla relazione illustrativa del Senato disponibile [qui](#).

potendo quest'ultimo essere chiamato in causa solo dall'assicurato al fine di essere manlevato in forza della polizza di assicurazione contro la responsabilità civile sottoscritta dallo stesso assicurato/danneggiante. Le uniche eccezioni a tale regola generale sono rappresentate dalla RC auto e dalla responsabilità civile sanitaria.

Sulla base della disciplina introdotta dal Decreto, chi lamenta di aver subito un danno, sia contrattuale che extracontrattuale, cagionato dall'utilizzo di un sistema di intelligenza artificiale può chiedere preventivamente al soggetto a cui ritiene che sia imputabile il danno se ha sottoscritto un contratto di assicurazione contro la responsabilità civile. Il responsabile del danno avrà quindi trenta giorni per comunicare l'eventuale esistenza di un contratto di assicurazione e, in caso di omessa o incompleta comunicazione, il giudice può desumere argomenti di prova.

Il danneggiato potrà, a questo punto, esperire azione diretta per il risarcimento del danno nei confronti dell'impresa di assicurazione del danneggiante, nei limiti del massimale previsto dal contratto di assicurazione.

Il Decreto prevede inoltre che sono opponibili al danneggiato unicamente le eccezioni derivanti dal contratto di assicurazione anteriori al sinistro (ad esempio eventuali franchigie), mentre le eccezioni derivanti da fatti successivi rispetto al sinistro potranno eventualmente essere fatte valere nel contesto dell'azione di rivalsa dell'impresa di assicurazione nei confronti dell'assicurato.

Va evidenziato che il Decreto non introduce alcun obbligo assicurativo a carico dei fornitori o degli utilizzatori di sistemi di IA. Nondimeno, poiché il danneggiato può agire direttamente nei confronti dell'assicuratore e a esso sono opponibili soltanto le eccezioni contrattuali anteriori al sinistro, le condizioni della polizza RC diventano esse stesse uno strumento di gestione del rischio IA. Tali condizioni andrebbero pertanto riesaminate alla luce dei nuovi profili di responsabilità civile delineati dal Decreto e degli obblighi di conformità imposti dall'AI Act.

4. Il coordinamento tra il Decreto, l'AI Act e il GDPR

Le norme sulla responsabilità civile si inseriscono e completano il quadro degli obblighi di trasparenza e accountability dell'AI Act e del Regolamento (UE) 2016/679 ("GDPR") a tutela degli interessati.

L'AI Act distingue i sistemi di IA a seconda del rischio intrinseco degli stessi e pone regole viepiù stringenti a seconda del livello di rischio. Da notare che fra i sistemi di IA ad alto rischio sono compresi quelli utilizzati per la valutazione del rischio creditizio e assicurativo connesso a prodotti vita e salute (Allegato III AI Act).

Tra gli obblighi più importanti previsti dall'AI Act vi sono le previsioni sulla trasparenza imposte ai produttori (c.d. *provider*) di sistemi ad alto rischio, i quali devono progettare e sviluppare tali sistemi in modo da garantire un livello sufficiente di trasparenza del loro funzionamento, corredandoli di istruzioni per l'uso che ne illustrino la destinazione, le caratteristiche, le capacità e le limitazioni prestazionali (art. 13 AI Act).

Tale obbligo di trasparenza deve essere letto insieme all'art. 17 del Decreto: il giudice, infatti, ordina l'esibizione degli elementi di prova relativi al funzionamento del sistema di IA *"all'altra parte o al terzo che ne dispone"*, potendo dunque l'ordine riguardare tanto il produttore quanto l'utilizzatore a prescindere da quale è il soggetto chiamato in causa ⁽⁷⁾.

Peraltro, tali doveri di trasparenza implicano il sorgere di una dialettica particolare tra produttori e utilizzatori, in cui i primi, per evitare sanzioni e limitare la propria responsabilità nei confronti dei secondi, dovranno essere quanto più chiari ed esaustivi nel definire i possibili utilizzi impropri, i limiti e le istruzioni di utilizzo del sistema, fermo sempre che la stessa documentazione potrà essere prodotta in giudizio su ordine del giudice.

Il mancato rispetto dei doveri di trasparenza è sottoposto a sanzione amministrativa (art. 99 AI Act). Oltre ai produttori, anche gli utilizzatori ⁽⁸⁾ hanno specifici doveri di documentazione e trasparenza, in particolare la tenuta di registri di log, la sorveglianza umana e l'utilizzo del sistema conformemente alle istruzioni del fornitore (art. 26 AI Act). Questi obblighi hanno diretto impatto sulle previsioni introdotte dal Decreto: come detto, la documentazione relativa al sistema di IA e alla sua gestione potrà essere esaminata in giudizio in base a quanto previsto dall'art. 17 del Decreto, e tale diritto di accesso comprende, tra l'altro, i log di sistema, la documentazione relativa alla valutazione e gestione dei rischi, la documentazione tecnica e le informazioni concernenti i meccanismi di sorveglianza umana. L'inottemperanza ingiustificata all'ordine di esibizione, come detto, può

⁽⁷⁾ A riguardo la relazione illustrativa del Senato, disponibile [qui](#), precisa: *"L'articolo 17 disciplina lo strumento centrale di superamento dell'asimmetria informativa tra danneggiato e soggetto cui è imputato il danno, modellato in larga parte sull'archetipo dell'ordine di esibizione previsto dalla disciplina antitrust di derivazione eurounitaria, nonché sulle indicazioni provenienti dalla proposta, ancorché ritirata, di direttiva sulla responsabilità da intelligenza artificiale. Il comma 1 attribuisce al giudice il potere di ordinare, su istanza della parte che allega di avere subito il danno, all'altra parte o al terzo che ne dispone, l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema di intelligenza artificiale. L'ordine è subordinato alla presentazione, da parte dell'istante, di fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema e il danno lamentato. Lo standard probatorio prescelto è quello della verosimiglianza, coerente con la funzione strumentale dell'esibizione, che presuppone per definizione una situazione di asimmetria informativa non superabile con i mezzi ordinari di acquisizione probatoria. (...) Il comma 3 codifica i principi di necessità e proporzionalità dell'ordine di esibizione, imponendo al giudice di tenere conto degli interessi di tutte le parti, con particolare riguardo alla tutela dei segreti commerciali e delle informazioni riservate."*

⁽⁸⁾ Cioè i c.d. *deployer* nel testo in inglese, vale a dire coloro che utilizzano il sistema di IA nel loro business (art. 3, par. 1, n. 4 AI Act). Tipicamente un'impresa di assicurazione sarà *deployer* nel caso di acquisto di un sistema dall'esterno, ma potrebbe anche avere gli obblighi del produttore qualora il sistema sia immesso sul mercato con il marchio dell'assicurazione.

comportare conseguenze significative per la parte inadempiente.

Va considerato, tuttavia, che le previsioni del Decreto si scontrano con il calendario di entrata in vigore scaglionato dell'AI Act. Infatti, molti degli obblighi previsti dall'AI Act entreranno in vigore in un momento futuro rispetto al Decreto (in particolare, alla fine del 2027 e nel 2028) e dunque almeno in una prima fase il Decreto offrirà una tutela solo parziale e di fatto non armonizzata ⁽⁹⁾.

Resta ferma poi, in senso più ampio, ogni tutela dal punto di vista della normativa privacy: l'art. 16, co. 3 del Decreto fa salve le previsioni dell'art. 82 GDPR, che prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR abbia il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Sul piano della prova liberatoria, l'art. 82, par. 3, GDPR consente al titolare o al responsabile di sottrarsi alla responsabilità solo dimostrando che *“l'evento dannoso non gli è in alcun modo imputabile”*, ossia provando l'insussistenza del nesso causale tra la violazione e il danno. In Italia, la responsabilità per trattamento illecito di dati personali è ricondotta pacificamente al modello dell'art. 2050 c.c., con la conseguenza che il titolare del trattamento deve dimostrare di aver adottato tutte le misure idonee a evitare il danno. In futuro, dunque l'art. 18 del Decreto (approfondito nel precedente paragrafo 2) andrà coordinato con le previsioni del GDPR in tutti i casi in cui i sistemi di IA trattino dati personali ⁽¹⁰⁾.

5. Conclusioni

Il Decreto rappresenta un passo avanti significativo nella regolazione dell'IA a livello nazionale, introducendo un quadro normativo che disciplina sia la responsabilità civile sia l'accesso alle tutele assicurative/risarcitorie per i danni derivanti dall'utilizzo di sistemi di intelligenza artificiale.

In particolare, sul fronte assicurativo, il Decreto, pur non imponendo un obbligo di copertura assicurativa (a differenza di quanto previsto in materia di RC auto e coperture catastrofali), introduce il meccanismo dell'azione diretta nei confronti dell'impresa di assicurazione, rendendo così meno complesso e più celere l'ottenimento di un risarcimento in caso di danno causato da sistemi di IA. Un'ulteriore tutela per il danneggiato è data dalla possibilità per l'assicuratore di opporre esclusivamente le eccezioni anteriori al sinistro.

⁽⁹⁾ Per approfondimento si veda A. Bertolino, *“AI Act dopo il Digital Omnibus: l'obbligo slitta, ma la responsabilità anticipa la prova”*, in Diritto e Giustizia, 25 agosto 2026.

⁽¹⁰⁾ Lo stesso Garante per la protezione dei dati personali già in passato ha sottolineato la stretta correlazione fra le due normative: si veda il comunicato stampa del Garante, *“Intelligenza artificiale: il Garante privacy scrive a Parlamento e Governo. Necessario individuare Autorità di vigilanza indipendenti e imparziali”*, 25 marzo 2024, doc. web [9996508](#).

Per le imprese di assicurazione e gli intermediari, il Decreto impone una revisione delle coperture RC alla luce dei rischi specifici connessi ai sistemi di IA, con particolare attenzione alla definizione del rischio assicurato, all'ambito di operatività della garanzia e alle relative esclusioni e limitazioni. Il coordinamento tra AI Act, GDPR e Decreto richiede inoltre un approccio integrato alla compliance che tenga conto delle intersezioni tra disciplina dell'intelligenza artificiale e protezione dei dati personali.

Infine, particolare attenzione dovrà essere posta sugli strumenti interni alle compagnie per la gestione dei contenziosi che, proprio alla luce della possibilità di avvalersi dell'azione diretta verso la compagnia, saranno destinati a crescere nel numero.



Focus Team Assicurazioni

Il *Focus Team* è una costellazione di competenze in diversi ambiti di attività con *focus* sulle assicurazioni.

Stefano Micheli

Societario

Massimiliano Danusso

Bancario & Finanziario

Vittorio Allavena

Litigation & Dispute Resolution

Alessandro De Nicola

Compliance & Investigations

Francesco Anglani

Competition & Antitrust

Tommaso Faelli

Proprietà Intellettuale

Angelo Bonetta

Litigation & Dispute Resolution

Andrea La Mattina

Diritto Marittimo e Societario

Raffaele Cassano

Amministrativo

Francesca Marchetti

Bancario & Finanziario



Focus Team Innovazione e Trasformazione Digitale

Il *Focus Team* è una costellazione di competenze in diversi ambiti di attività con focus su innovazione e trasformazione digitale.

Tommaso Faelli

IP-IT-Privacy

Alessandro De Nicola

Legal Risk, Compliance & Investigations

Marco Adda

Fiscale

Maurizio Pappalardo

Antitrust

Giulia Bianchi Frangipane

Societario

Luca Perfetti

Amministrativo

Enrico Chieppa

Litigation & Dispute Resolution

Vittorio Pomarici

Lavoro

Gianpaolo Ciervo

Bancario

Giulia Tenaglia

IP-IT-Privacy

Fabrizio Colonna

Financial Regulatory

Matteo Viani

Fiscale

Luca Guerrini

Dispute Resolution

Anna La Mura

Privacy & Data Protection