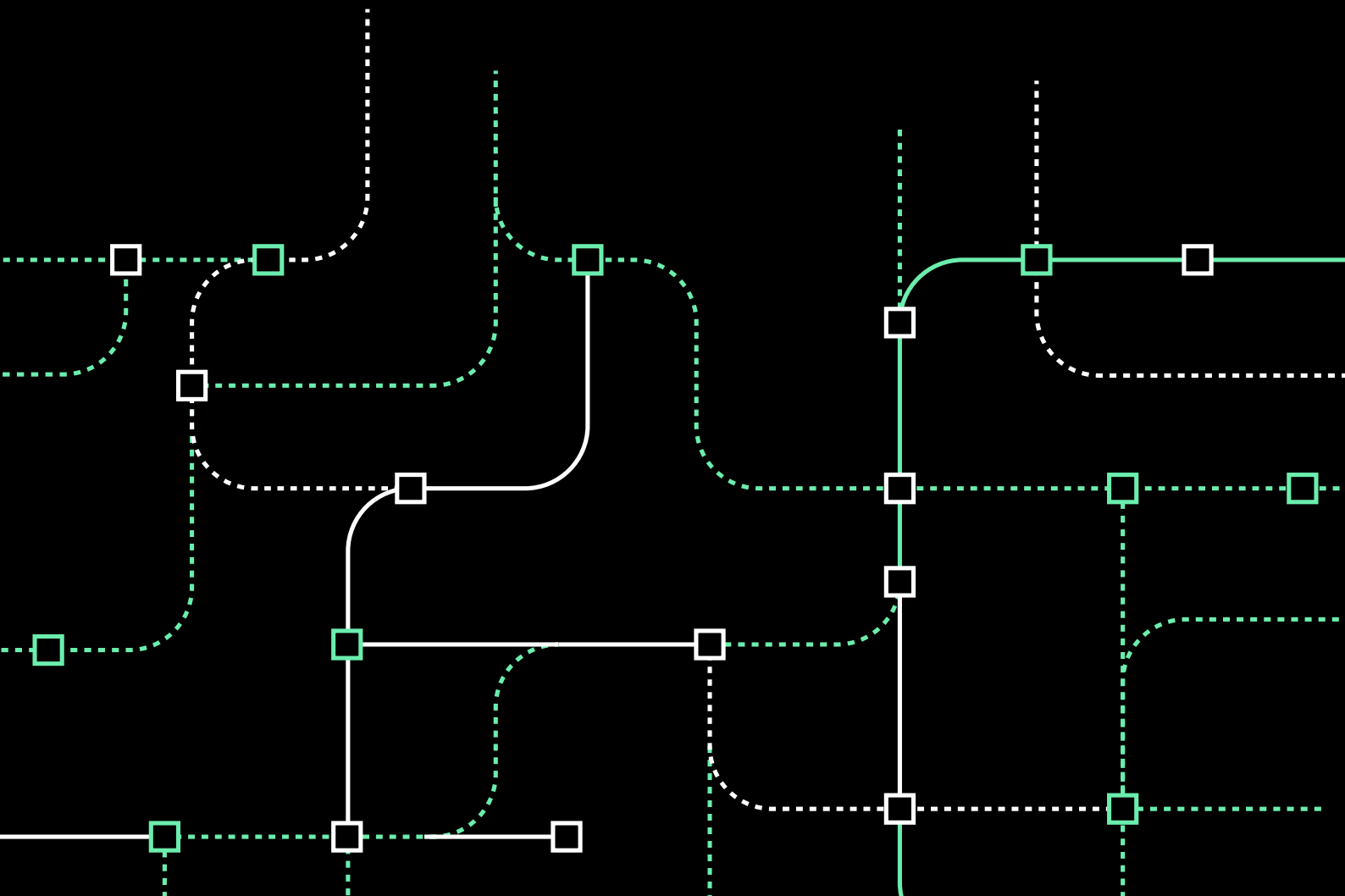
OneTrust

Report di OneTrust sulle previsioni per il 2027

Ripensare la governance dell'IA:

come orientarsi in uno scenario in continua evoluzione

Report



Indice

Introduzione: concedere l'accesso, limitare l'autorità, dimostrare la fiducia	3
Previsione 1: le garanzie sull'IA diventano un requisito commerciale.	4
Previsione 2: un agente approvato può comunque svolgere un'attività non autorizzata	7
Previsione 3: le modifiche sostanziali all'IA richiedono nuove valutazioni delle garanzie	10
Previsione 4: le interazioni con l'IA integrano le scelte sull'utilizzo dei dati nel percorso del cliente	14
Le normative sull'IA nel 2027 secondo gli esperti	17
Controprevisioni: tre scenari poco probabili nel 2027	25

Dichiarazione di non responsabilità
Nessuna parte di questo documento può essere riprodotta in alcuna forma senza il permesso scritto del proprietario del copyright. I contenuti di questo documento sono soggetti a revisione senza preavviso a causa dei continui progressi nella metodologia, nella progettazione e nella produzione. OneTrust LLC non si assume alcuna responsabilità per eventuali errori o danni di qualsiasi tipo derivanti dall'uso di questo documento. I prodotti, i contenuti e i materiali di OneTrust sono esclusivamente a scopo informativo e non hanno il fine di fornire consulenza legale. Si consiglia di rivolgersi al proprio legale per richiedere consulenza su temi specifici. I materiali OneTrust non garantiscono la conformità alle leggi e alle normative vigenti.

Copyright © 2026 OneTrust LLC. Tutti i diritti riservati. Informazioni proprietarie e riservate.

Introduzione

Concedere l'accesso, limitare l'autorità, dimostrare la fiducia



Blake Brannon
Chief Innovation Officer
OneTrust

Il dibattito sulla velocità con cui evolve l'IA di ultima generazione pone le aziende di fronte a una decisione immediata: cosa si è disposti a consentire a questi sistemi? La questione assume particolare rilevanza quando un agente può modificare un record aziendale, utilizzare informazioni sui clienti o avviare attività in un altro sistema.

Per le persone, il meccanismo è già noto: un nuovo dipendente riceve un badge, apprende quali decisioni può prendere e conquista la fiducia nel tempo. Gli agenti hanno bisogno degli stessi tre elementi, ma funzionano diversamente.

Un agente ottiene l'accesso quando viene collegato a un sistema e spesso eredita quello della persona che lo ha creato, anche oltre quanto necessario. È già una realtà: nell'indagine OneTrust 2026 sulla governance pronta per l'IA, l'87% degli intervistati afferma che la propria organizzazione incoraggia l'uso degli agenti, il 47% con governance e controlli chiari e il 40% con capacità ancora in fase di sviluppo. Incoraggiarne l'uso è la direzione giusta, purché l'accesso non venga interpretato come un'autorizzazione implicita.

Stabilire cosa un agente possa fare con il proprio accesso è una decisione distinta. L'accesso definisce ciò che un sistema può raggiungere; l'autorità, cosa può fare, per quale finalità ed entro quali limiti. Un agente con accesso al sistema degli ordini potrebbe, ad esempio, effettuare rimborsi fino a 200 dollari per ordini risalenti a meno di 30 giorni, richiedendo l'intervento umano oltre tali limiti. Questi devono essere definiti e applicati nel punto in cui avviene l'azione, perché il ruolo dell'agente può ampliarsi senza che sia evidente: nuove connessioni o informazioni possono consentirgli di agire oltre la finalità originaria, pur mantenendo la stessa approvazione. L'agente non segnalerà autonomamente il problema. Solo il 5% degli intervistati dichiara un coordinamento e responsabilità chiari lungo il ciclo di vita dell'IA. Senza questi elementi, azioni consentite possono combinarsi in un risultato non autorizzato. L'autorità deve avere limiti chiari.

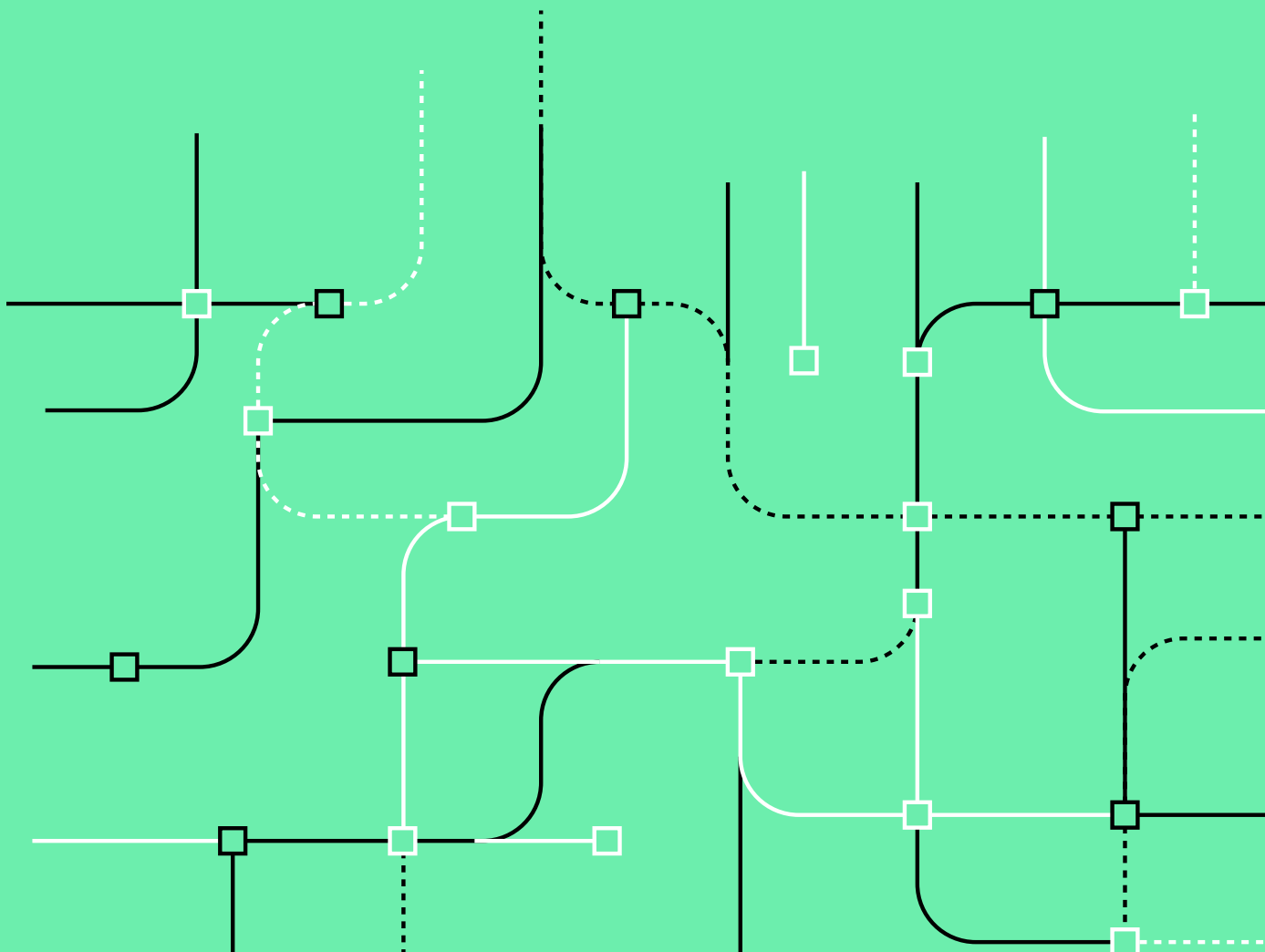
Per essere considerato affidabile, un agente deve dimostrare nel tempo di aver agito entro i limiti autorizzati e ciò deve poter essere verificato in modo indipendente. Può operare con le credenziali di una persona, ma non ne eredita l'affidabilità. L'identità si eredita, mentre la fiducia no. Inoltre, l'agente non può verificare sé stesso: le registrazioni delle sue attività devono restare al di fuori del suo controllo ed essere conservate come evidenze verificabili in modo indipendente. Solo il 28% degli intervistati dichiara di disporre di evidenze di governance e audit trail, l'attività meno diffusa nel sondaggio. La prima previsione mostra chi richiederà queste evidenze e quando. La fiducia si dimostra.

Tutto questo non significa rallentare. Limiti chiari evitano ritardi inutili, mentre la governance consente di prendere le decisioni più complesse con la rapidità necessaria e di stabilire chi è responsabile dei rischi residui.

Le quattro previsioni che seguono analizzano come accesso, autorità ed evidenze influenzeranno l'adozione e i risultati aziendali nel 2027, dalle garanzie commerciali ai limiti delle attività delegate, fino all'evoluzione dell'ecosistema di IA e all'utilizzo dei dati dei clienti. Prima di ampliare l'autorità di un agente, puoi definirne la finalità, bloccare un'azione non autorizzata e ricostruire cosa è accaduto? È questa la sfida a cui il report invita a prepararsi.

Previsione 1

Le garanzie sull’IA diventano un requisito commerciale



Previsione 1

Le garanzie sull'IA diventano un requisito commerciale

Nel 2027, chi acquista servizi basati sull'IA ad alto impatto richiederà sempre più spesso evidenze aggiornate e pertinenti all'implementazione prima di attivarli o ampliarne l'utilizzo. Le garanzie richieste dipenderanno dal livello di autonomia della funzionalità, dall'impatto sul business e dai potenziali danni. Questa pressione potrebbe estendersi anche alle decisioni relative a contratti, rinnovi e budget.

Un fornitore introduce una nuova funzionalità di IA, pronta per essere attivata. Il cliente, però, attende: le garanzie esistenti coprono anche ciò che il servizio può fare ora?

La preparazione tecnica non garantisce l'adozione da parte del cliente. Il valore commerciale della nuova funzionalità dipende anche dalla capacità di risolvere i rischi che ne ostacolano l'attivazione.

Nel 2027, questo legame diventerà più evidente. Gli acquirenti verificheranno se le garanzie esistenti coprono funzionalità, connessioni ai dati e implementazione. Evidenze mancanti o non aggiornate potrebbero ritardare l'attivazione o limitarne l'utilizzo e l'espansione.

La ricerca OneTrust mostra una base di evidenze ancora disomogenea: solo il 28% dispone di evidenze di governance e audit trail, mentre il 38% considera prioritario prepararsi a normative, standard o audit nei prossimi 12 mesi.

> "I clienti hanno bisogno di garanzie adeguate alla funzionalità proposta. Quando questa cambia, le verifiche precedenti potrebbero non essere più sufficienti. Evidenze pertinenti aiutano a valutare l'esposizione e a decidere se attivarla."

Tim Mullen
Chief Information Officer
OneTrust



Le evidenze devono supportare una decisione. Un test di penetrazione individua le vulnerabilità; una valutazione dei controlli verifica il rispetto dei limiti stabiliti. Resta essenziale sapere cosa è stato esaminato, quali misure restano efficaci e chi può accettare il rischio residuo.

Secondo una recente ricerca di Gartner, la governance dell'IA sta emergendo come criterio di acquisto, con richieste di evidenze su tracciabilità, monitoraggio e meccanismi di intervento. Informazioni incomplete possono allungare la due diligence e creare vincoli assicurativi, pur senza dimostrare quanto questi requisiti incidano già sui risultati commerciali.

L'attenzione si estende anche alla dirigenza. Secondo Gartner, i leader devono sapere quali decisioni aziendali sono influenzate dall'IA e chi ne è responsabile. Questa maggiore attenzione renderà le evidenze sempre più importanti per decidere se attivare una funzionalità o ampliarne l'autorità.

Nel 2027, l'IA potrebbe essere utilizzata anche nella valutazione preliminare dei fornitori, sulla base di policy pubbliche e materiali relativi alle garanzie. Resta da capire quanto questo inciderà sulla selezione dei fornitori.

Per i CFO e i responsabili degli investimenti, occorre valutare se una funzionalità generi valore sufficiente a giustificarne costi ed esposizione. Questi fattori, insieme alle garanzie, avranno un peso crescente nelle decisioni su ulteriori investimenti. Rispettare i limiti approvati non basta a giustificare l'espansione.

Per i fornitori, risolvere le questioni relative alle garanzie diventa essenziale per favorire l'adozione di una funzionalità di IA. I team commerciali devono individuare le evidenze mancanti e chi può decidere. Gli acquirenti devono invece scegliere se attivarla, imporre condizioni o attendere.

Cosa potrebbe cambiare questo scenario

Gli acquirenti potrebbero continuare ad affidarsi a questionari e verifiche periodiche consolidati. Le esclusioni assicurative potrebbero modificare l'esposizione senza incentivare investimenti nella governance. La previsione sarebbe meno solida se nuove evidenze incidessero raramente su attivazione, condizioni o ampliamento dell'utilizzo.



Probabilità: moderata.

Impatto sul settore

Elevato quando le garanzie incidono sull'adozione o sull'espansione, influenzando prodotti, condizioni commerciali e decisioni di investimento.

Priorità per i responsabili della governance

- Sicurezza e prodotto: allineare le garanzie alla funzionalità e alla versione offerte.
- Team commerciali: monitorare le richieste che ritardano l'adozione o modificano l'ambito di implementazione.
- Rischio e ufficio legale: individuare gli aspetti rilevanti relativi a contratti, copertura assicurativa e obblighi di informativa.
- Finanza e responsabili aziendali: definire il valore atteso, i costi operativi e le evidenze necessarie prima di ulteriori investimenti o di un'espansione.

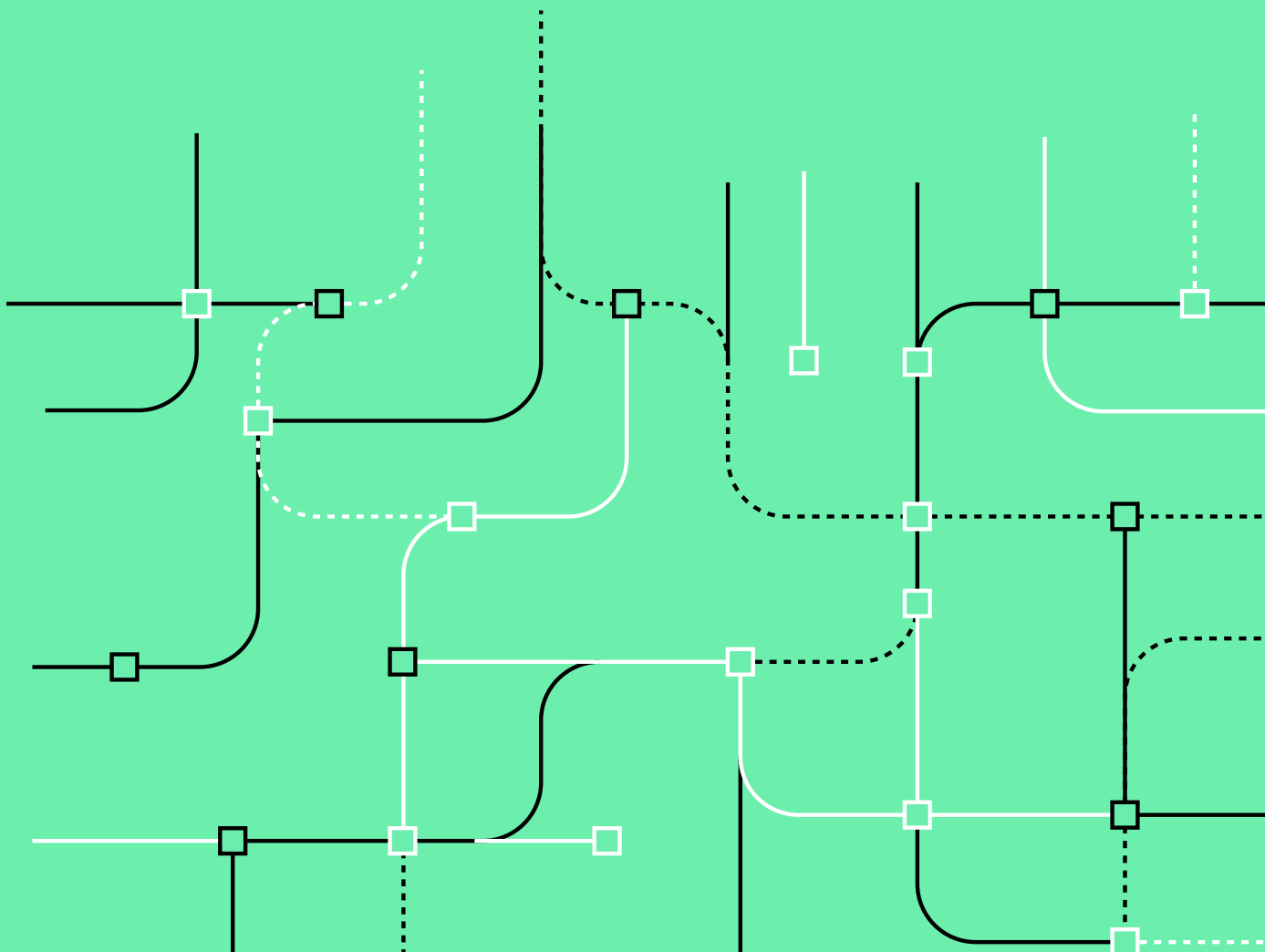
Tendenze da monitorare nel 2027

- Acquirenti che rinviano l'attivazione o l'espansione in attesa di evidenze aggiornate.
- Clausole contrattuali che richiedono nuove garanzie dopo modifiche sostanziali all'IA.
- Valutazioni assicurative specifiche per l'IA legate a condizioni di copertura o esclusioni.
- Decisioni di finanziamento ed espansione che considerano esplicitamente il valore generato e i costi operativi insieme alle evidenze sui controlli.

[1] *When AI Governance Fails, Revenue and Executives Take the Hit, Gartner, 2026*

Previsione 2

Un agente approvato può comunque svolgere un’attività non autorizzata



Previsione 2

Un agente approvato può comunque svolgere un'attività non autorizzata

Nel 2027, i programmi più avanzati per agenti di IA ad alto impatto adotteranno criteri più rigorosi su autorità, intervento e registrazioni protette. Le prime iniziative valuteranno anche l'esito combinato di azioni singolarmente consentite.

> **Agli agenti vengono affidate sempre più attività: accedere a Internet, operare su Salesforce, avviare flussi di lavoro e contattare colleghi. Ma possono ereditare l'accesso di chi li ha creati, non la sua capacità di giudizio. Se l'autorità aumenta, si tratta ancora dello stesso agente approvato?**

DV Lamba
Chief Technology and Product Officer
OneTrust

Un agente deve ridurre la spesa per i servizi cloud senza compromettere le scadenze di elaborazione degli ordini. Riduce la capacità inutilizzata e rinvia i processi batch, due operazioni tecnicamente autorizzate.

I costi diminuiscono, ma l'elaborazione notturna degli ordini non rispetta la scadenza. Le singole azioni erano consentite, ma il loro effetto complessivo ha violato un limite dell'attività autorizzata.

La sfida è definire ciò che un agente è autorizzato a fare e quali conseguenze sono inaccettabili. L'autorizzazione tecnica a una singola azione non giustifica qualsiasi compromesso che ne possa derivare. I limiti devono essere applicabili e consentire di intervenire quando necessario.

Il ruolo di un agente può ampliarsi dopo l'approvazione, con nuove connessioni o responsabilità che ne estendono l'ambito di azione. Occorre stabilire quando questi cambiamenti superano l'autorità originariamente concessa.

Il superamento delle verifiche tecniche per ogni singola azione non garantisce che il risultato complessivo rispetti i limiti autorizzati. L'approvazione deve definire chiaramente l'attività consentita, così da poterne verificare i limiti e valutare l'intero flusso di lavoro.

Secondo la ricerca OneTrust, il 48% degli intervistati segnala almeno un incidente relativo ad azioni non approvate di sistemi o agenti di IA nell'ultimo anno. Solo il 28% dispone di evidenze di governance e audit trail. Autorità e tracciabilità sono già questioni operative concrete.

> **La governance deve definire condizioni applicabili nel flusso di lavoro. Un agente autorizzato a sintetizzare i ticket dell'assistenza potrebbe richiedere un'autorità distinta per aggiornare i dati dei clienti o emettere rimborsi. I limiti vanno verificati dopo l'implementazione e rivalutati quando cambiano attività o policy."**

Sriram Iyer
SVP and GM AI Strategy & Products
OneTrust

“

La supervisione umana non può essere passiva. Servono conoscenze e giudizio critico per mettere in discussione l’IA, anziché affidarsi a un output convincente. Occorre verificare che la finalità sia valida, la direzione corretta e gli errori ridotti al minimo.”

Odia Kagan
Partner & Co-Chair, Privacy & Data Security
Fox Rothschild LLP

Servono registrazioni indipendenti dall’agente che colleghino le azioni rilevanti all’autorità concessa e supportino verifiche tra sistemi, comprese eccezioni e interventi umani. Permettono di ricostruire cosa è accaduto, ma il risultato complessivo va comunque valutato rispetto alla finalità e ai limiti dell’attività.

La verifica deve proseguire dopo l’implementazione. Occorre monitorare i processi in cui opera l’IA, individuare comportamenti inaccettabili e adeguare attività e controlli. Una valutazione iniziale non può prevedere tutte le possibili conseguenze di azioni combinate.

Nel 2027, i limiti all’autonomia degli agenti diventeranno più chiari. Se non è possibile applicare i limiti di un’attività o ricostruirne l’esito, potrebbe essere necessario limitare l’accesso ai dati, rimuovere strumenti o mantenere un controllo umano. Maggiore autorità richiederà controlli comprovati e una chiara responsabilità per il rischio residuo.

Cosa potrebbe cambiare questo scenario

La supervisione umana potrebbe bastare per attività ben delimitate. La valutazione complessiva può aumentare costi e tempi senza individuare in modo affidabile risultati dannosi. Autorità e meccanismi di intervento potrebbero quindi diffondersi più rapidamente rispetto alla valutazione dei risultati.

Probabilità: moderata.

Per criteri di implementazione più rigorosi. In fase iniziale per la valutazione affidabile dell’attività nel suo complesso.

Impatto sul settore

Elevato quando l’autorità degli agenti incide su servizi, transazioni o decisioni sensibili.

Priorità per i responsabili della governance

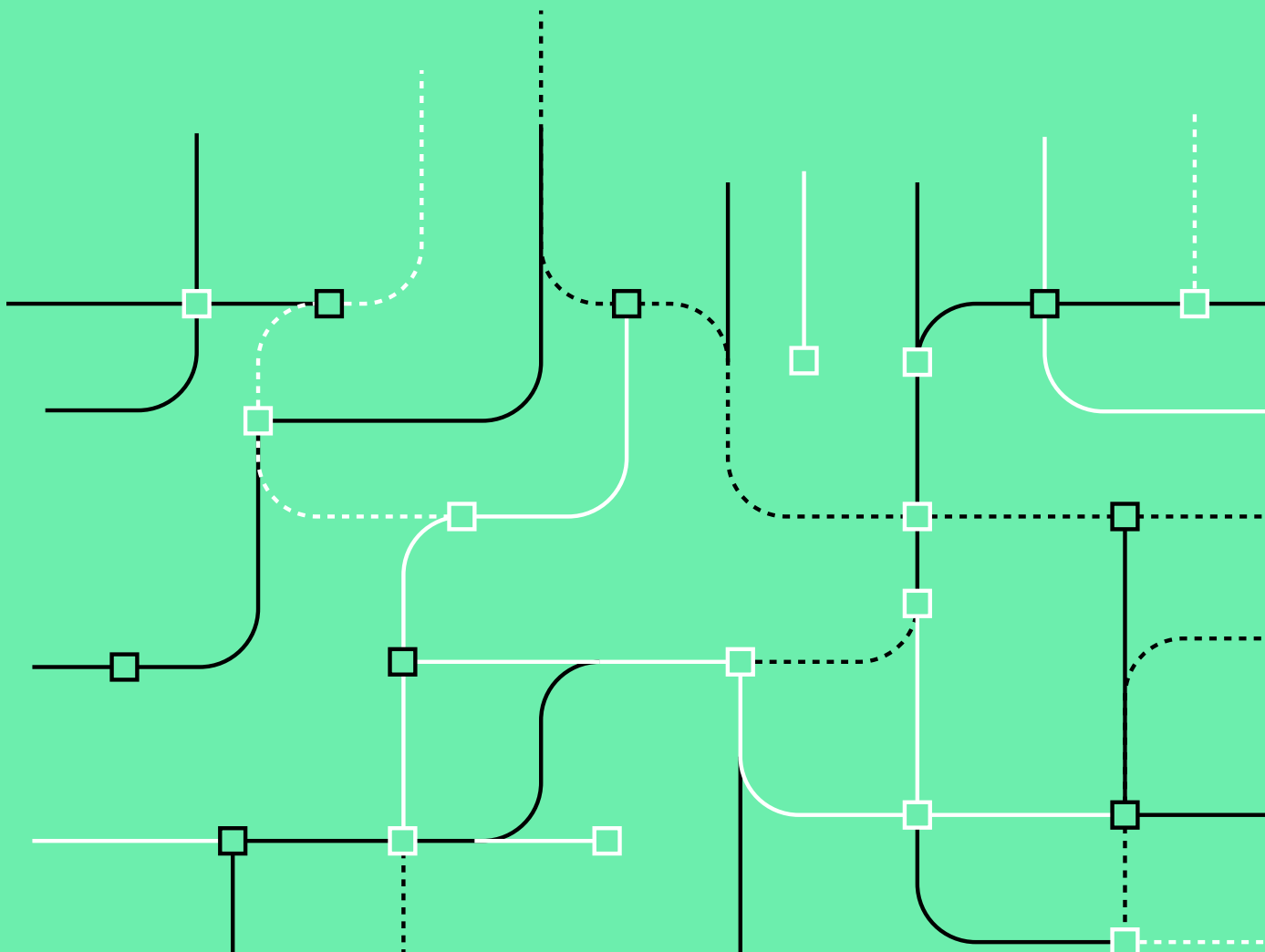
- Responsabili aziendali: definire i risultati inaccettabili, verificare il comportamento nei processi in uso e assegnare la responsabilità degli interventi correttivi.
- Sicurezza e progettazione: testare blocco, scadenza, escalation e revoca.
- Privacy e governance dell’IA: tradurre finalità e propensione al rischio in condizioni applicabili.
- Audit: definire come ricostruire un’attività tra sistemi diversi.

Tendenze da monitorare nel 2027

- Revisioni dell’implementazione che richiedono limiti chiari per le attività e test dei meccanismi di intervento.
- Registrazioni protette dal controllo dell’agente che esegue le azioni.
- Valutazioni in grado di individuare conseguenze dannose derivanti dalla combinazione di azioni consentite.
- Assegnazione della responsabilità e dismissione degli agenti collegate a controlli degli accessi effettivamente applicabili.
- Evidenze che dimostrano che le modifiche sostanziali alle policy raggiungono gli agenti interessati e vengono testate nei relativi flussi di lavoro.
- Risultati delle verifiche successive all’implementazione che portano a rivedere limiti delle attività, controlli o procedure operative.

Previsione 3

Le modifiche sostanziali all’IA richiedono nuove valutazioni delle garanzie



Previsione 3

Le modifiche sostanziali all'IA richiedono nuove valutazioni delle garanzie

Nel 2027, le modifiche sostanziali all'IA acquistata, sviluppata o integrata richiederanno sempre più spesso una nuova valutazione, anche senza un nuovo fornitore. Le verifiche riguarderanno funzionalità, strumenti connessi, accesso ai dati, finalità ed efficacia dei controlli.

Un team di assistenza utilizza un'applicazione di IA in hosting, un team di progettazione gestisce un modello open-weight e una piattaforma aziendale approvata integra un assistente con accesso ai dati interni.

L'ecosistema comprende IA acquistata, sviluppata o già integrata nelle applicazioni esistenti. Servizi in hosting e modelli gestiti o operati internamente comportano responsabilità diverse. Un modello open-weight, di per sé, non indica chi gestisce o supporta l'implementazione.

> “Non si può governare ciò che non si può vedere. Ogni giorno vengono creati nuovi agenti e questi agenti non si limitano a rispondere ai messaggi: eseguono azioni e accedono a dati personali e sensibili. Serve visibilità sugli agenti che vengono sviluppati e un modo per individuare quelli che richiedono ulteriori valutazioni.”

Manuel
AI and Data Protection Specialist
Scania Svezia

Un ecosistema di IA più eterogeneo non richiede una governance separata per ogni modello, strumento o implementazione. Occorre invece estendere le responsabilità esistenti per sicurezza, privacy, rischio, procurement e gestione aziendale alle nuove combinazioni tecnologiche.

> “L'IA non crea una nuova categoria di governance, ma amplia quella già necessaria alle organizzazioni. Con la crescita dell'adozione dell'IA e dei requisiti globali in materia di privacy e normativa, la governance diventerà sempre più centrale per le aziende.”

Damian Apone
Director, Global Retail Cybersecurity
Genuine Parts Company

La questione centrale è chiarire come sono distribuite le responsabilità.

Un fornitore può gestire il servizio e il cliente la configurazione. Un team interno può gestire un modello e un responsabile aziendale definirne gli utilizzi consentiti. Connettori, strumenti o integrazioni Model Context Protocol possono introdurre accessi non previsti nella valutazione iniziale.

“

La sfida principale è mantenere la visibilità operativa mentre l’IA viene integrata nei processi aziendali esistenti. Quando sono coinvolti più soggetti, può essere difficile stabilire chiaramente le responsabilità. Con l’evoluzione di modelli, fornitori e casi d’uso, la compliance diventa un’attività continua: occorre tenere traccia dei cambiamenti, monitorare le decisioni e rivalutare i rischi tra i diversi team.

Olivia Roth
DPO/AI Governance
Yves Rocher Germania

Il 39% indica la scarsa visibilità su componenti di IA di terze parti, fornitori o fonti di dati come un fattore di rallentamento. Il 28% segnala inoltre l’adozione di strumenti di IA dei fornitori prima di una valutazione completa. Questa visibilità è necessaria per stabilire quali cambiamenti richiedano una nuova valutazione.

Una modifica è sostanziale quando altera un presupposto dell’approvazione iniziale. Nuovi connettori, autorizzazioni più ampie o modifiche a modelli e configurazioni possono cambiare l’esposizione o l’efficacia dei controlli. La nuova valutazione dovrebbe concentrarsi su questi cambiamenti e riutilizzare le evidenze ancora valide.

“

Una valutazione si basa su una specifica funzionalità, configurazione e profilo di rischio. Nuovi modelli, connettori o fonti di dati possono modificarne i presupposti. Una notifica segnala il cambiamento, ma occorre stabilire se l’approvazione resti valida o se la funzionalità debba essere rivalutata, limitata o disattivata.”

Sriram Iyer
SVP and GM AI Strategy & Products
OneTrust

Una modifica sostanziale può richiedere di riconsiderare una decisione anche nell’ambito di un contratto esistente. Limitare una funzionalità critica può interrompere le operazioni, mentre continuare senza una nuova valutazione può introdurre rischi non previsti dall’approvazione iniziale. Responsabilità chiare e meccanismi di fallback facilitano la risposta dell’organizzazione.

Rivedere manualmente ogni componente sarebbe difficile. Le priorità devono riflettere potenziali danni, sensibilità dei dati e dipendenza aziendale. Per gli utilizzi ad alto impatto occorre definire chi rileva i cambiamenti e decide come intervenire. Non ogni aggiornamento richiede una nuova valutazione completa.

“

I clienti richiederanno garanzie, ma verificare continuamente ogni fornitore con metodi tradizionali non è sostenibile. Occorre concentrarsi sui sistemi con il maggiore potenziale di danno e valutarne i risultati. Le garanzie devono diventare un processo che si adatta ai cambiamenti, non una risposta che diventa obsoleta.”

Ojas Rege
SVP Emerging Products and Technologies
OneTrust

Cosa potrebbe cambiare questo scenario

I fornitori di servizi gestiti potrebbero offrire informazioni e controlli sufficienti per adattare i programmi esistenti. Una visibilità limitata potrebbe invece ostacolare una nuova valutazione efficace. La previsione si rafforza se le modifiche sostanziali portano a decisioni documentate, non solo a nuove notifiche.

Probabilità: moderata.

Le lacune nella visibilità e nella valutazione dell'IA di terze parti rafforzano la necessità di rivalutare in caso di cambiamenti. Nel 2027, questo approccio potrebbe diffondersi negli utilizzi ad alto impatto, mentre resta meno matura la rivalutazione sistematica dell'intero ecosistema di IA.

Impatto sul settore

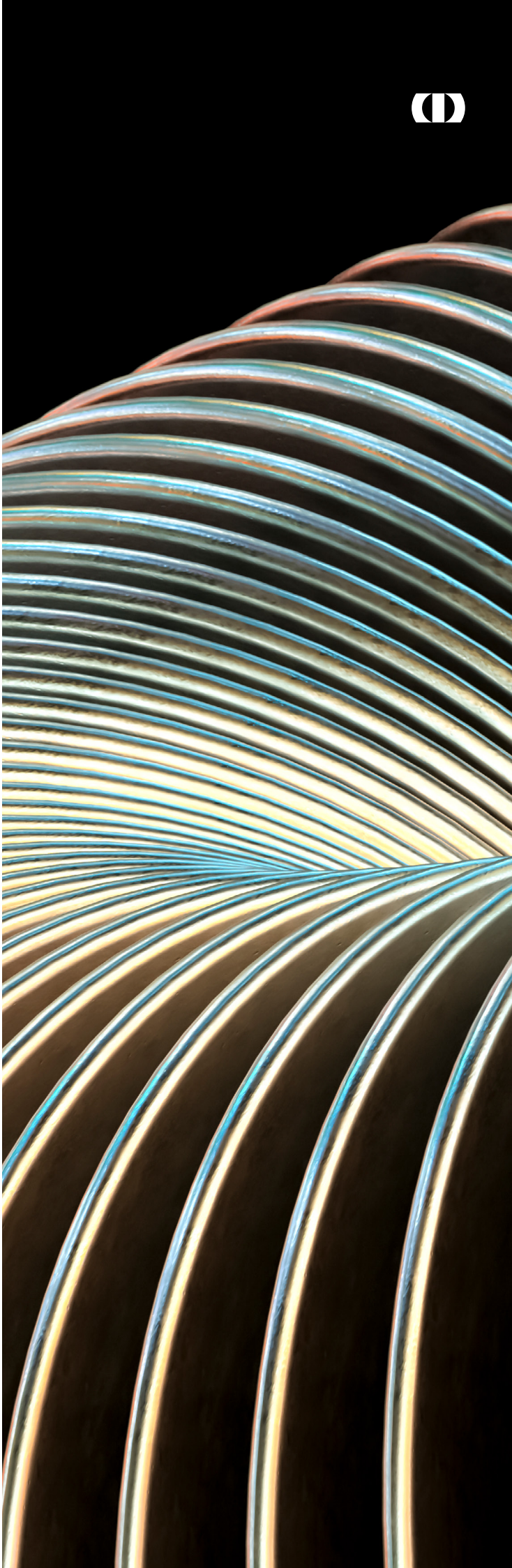
Elevato per continuità operativa, sicurezza e responsabilità nelle implementazioni esistenti.

Priorità per i responsabili della governance

- Tecnologia e dati: mappare modelli, applicazioni, connettori e flussi di dati rilevanti.
- Approvvigionamento e ufficio legale: definire diritti di notifica delle modifiche, limitazione e disattivazione.
- Sicurezza: rivalutare le modifiche agli accessi e l'efficacia dei controlli.
- Responsabili aziendali: definire chi può continuare, limitare, correggere o interrompere un utilizzo, prevedendo meccanismi di fallback ove necessario.

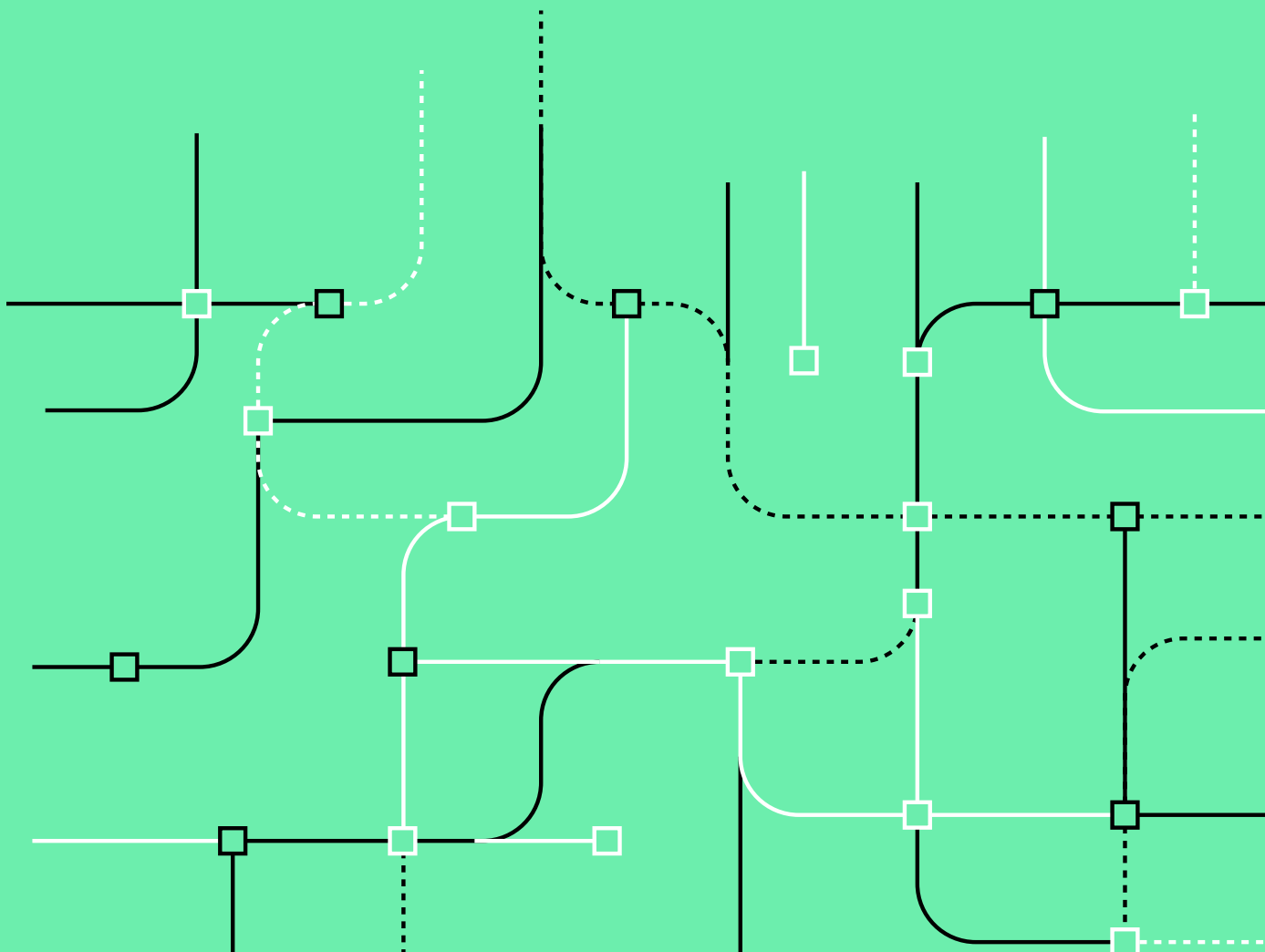
Tendenze da monitorare nel 2027

- Nuove valutazioni avviate anche senza un nuovo processo di acquisto.
- Notifiche delle modifiche collegate agli utilizzi e alle dipendenze interessati.
- Revisioni avviate in seguito a una minore efficacia dei controlli, oltre che all'introduzione di nuove funzionalità.
- Decisioni documentate per continuare, limitare, correggere o sostituire un servizio modificato.
- Meccanismi di fallback testati per i flussi di lavoro critici.



Previsione 4

Le interazioni con l’IA integrano le scelte sull’utilizzo dei dati nel percorso del cliente



Previsione 4

Le interazioni con l'IA integrano le scelte sull'utilizzo dei dati nel percorso del cliente

Nel 2027, le prime esperienze cliente mediate dall'IA collegheranno scelte più esplicite sull'utilizzo dei dati ai trattamenti consentiti. Le conversazioni possono raccogliere informazioni oltre quanto necessario e riutilizzarle per finalità diverse da quelle attese dal cliente. I primi sviluppi potrebbero riguardare singoli servizi, mentre un'applicazione coerente tra fornitori richiederà più tempo.

Un cliente chiede a un assistente IA di prenotare un cappotto della taglia desiderata in un negozio vicino. Durante la conversazione, spiega che è un regalo e descrive le preferenze del destinatario, fornendo dettagli che un normale modulo di prenotazione non avrebbe richiesto.

La finalità immediata è trovare l'articolo e riservarlo per il ritiro. Riutilizzare le informazioni raccolte per finalità pubblicitarie richiede una scelta distinta. Quando necessaria, questa scelta deve essere spiegata e rispettata nei trattamenti successivi.

La sfida è offrire personalizzazione senza creare incertezza sull'uso autorizzato dei dati. Richieste ripetute possono interrompere l'esperienza, mentre utilizzi inattesi possono compromettere la fiducia. Anche il momento e gli effetti della scelta diventano quindi parte dell'esperienza del cliente.

La scelta deve incidere sui trattamenti successivi. Se il cliente rifiuta l'uso dei dati per finalità pubblicitarie, il servizio deve rispettare tale scelta senza impedire, ove possibile, la prenotazione. In caso di revoca, occorre individuare i trattamenti interessati e applicare la modifica.

I trattamenti successivi devono essere coerenti con le finalità e gli utilizzi consentiti registrati nella mappa dati e nelle valutazioni privacy. Utilizzi che esulano da tale ambito richiedono una verifica. Se il contesto originario non può essere ricostruito con certezza, la situazione va risolta prima di procedere.

I requisiti della California sui sistemi decisionali automatizzati evidenziano una sfida analoga: spiegare una decisione richiede di capire come il flusso di lavoro utilizza le informazioni personali e produce il risultato. Servono quindi contesto e responsabilità chiare tra le diverse funzioni.

La ricerca OneTrust evidenzia una sfida più ampia legata ai dati: per il 52%, qualità, accesso, privacy o sicurezza rallentano le iniziative, mentre il 39% considera prioritario migliorare la visibilità su rischi e utilizzo dei dati.

> "Un'informativa pre-utilizzo può sembrare un semplice obbligo informativo, ma richiede di comprendere in anticipo cosa fa l'ADMT, come utilizza le informazioni personali e come il risultato incide sulla decisione. Il team legale deve quindi coordinarsi con prodotto, progettazione, risorse umane e operations."

Jake Harrison
Associate
Crowell & Moring LLP

“

La questione privacy riguarda ciò che accade alle informazioni nel flusso di lavoro. L’IA può combinarle o riutilizzarle per finalità diverse da quelle iniziali. Occorre quindi verificare gli utilizzi successivi e garantire che le condizioni applicate ai dati continuino a essere rispettate.”

Brett Tarr
Head of Privacy & AI Governance
OneTrust

Preferenze dei clienti, autorizzazioni tecniche e consenso legale restano distinti. Un’istruzione a un assistente non costituisce automaticamente consenso, né un’autorizzazione registrata dimostra di per sé la liceità del trattamento.

I passaggi tra fornitori complicano l’applicazione delle scelte, perché un’autorizzazione potrebbe non indicarne finalità e limiti. Il servizio che riceve i dati deve avere un contesto sufficiente per valutare l’utilizzo proposto oppure sospenderlo in attesa di chiarimenti.

Le prime implementazioni potrebbero collegare le scelte espresse durante un’interazione con l’IA ai trattamenti dello stesso servizio. La loro efficacia dipenderà dalla comprensione del cliente e dagli effetti concreti di un rifiuto o una revoca. L’applicazione coerente tra fornitori resta meno matura.

Cosa potrebbe cambiare questo scenario

Le informative e le conferme esistenti potrebbero bastare per molte esperienze. Ulteriori richieste possono interrompere il percorso e i fornitori interpretare diversamente le autorizzazioni. L’adozione potrebbe quindi restare limitata a singoli servizi, con poche evidenze dell’applicazione delle scelte ai trattamenti successivi.

Probabilità: in fase iniziale.



Impatto sul settore

Elevato per esperienza del cliente e utilizzo dei dati, con adozione inizialmente limitata.

Priorità per i responsabili della governance

- Prodotto e marketing: individuare cambiamenti di finalità o destinatario nei percorsi prioritari.
- Privacy e ufficio legale: stabilire quali scelte e requisiti si applicano.
- Progettazione: verificare che utilizzo consentito, rifiuto e revoca si riflettano nei trattamenti successivi.
- Team responsabili dei dati: preservare le informazioni su finalità e destinatario necessarie per le decisioni successive.

Tendenze da monitorare nel 2027

- Percorsi prioritari che richiedono una scelta pertinente nel momento in cui viene proposto un determinato utilizzo.
- Registrazioni che specificano finalità e destinatario previsto.
- Trattamenti che cambiano in seguito a un rifiuto o una revoca.
- Progetti pilota che sospendono il trattamento o richiedono una nuova scelta quando il passaggio tra servizi supera l’ambito originario.
- Test che verificano come una revoca si propaga ai sistemi coinvolti nei trattamenti successivi.

Le normative sull’IA nel 2027 secondo gli esperti



Le normative sull'IA nel 2027 secondo gli esperti

Nel 2027, tempistiche e approcci normativi all'IA varieranno notevolmente tra le diverse giurisdizioni. Alcuni governi stanno introducendo requisiti specifici, mentre altri applicano le normative esistenti in materia di privacy, tutela dei consumatori, lavoro e singoli settori.

La sfida per le organizzazioni è operativa: sapere dove viene utilizzata l'IA, quali obblighi si applicano, chi ne controlla le azioni e quali evidenze dimostrano la compliance.



Stati Uniti: le normative diventano operative

Negli Stati Uniti, il quadro normativo resta frammentato. Questo non riduce l'onere operativo, ma lo distribuisce tra requisiti diversi.

A livello federale, il quadro sull'IA della Casa Bianca del 20 marzo 2026 presenta raccomandazioni legislative non vincolanti, comprese proposte sulla prevalenza della normativa federale. I poteri delle agenzie e i requisiti statali continuano a determinare gli obblighi di compliance.

> Nel 2027 ritengo molto improbabile l'introduzione di nuove normative organiche sull'IA a livello statale o federale. Le organizzazioni dovrebbero invece puntare su una governance pronta per il futuro, basata sulla trasparenza, e monitorare l'evoluzione dei rischi di contenzioso legati all'IA."

Tyler J. Thompson
Partner, Co-Chair, Global Artificial Intelligence Practice
Reed Smith LLP

Principali tappe normative

- California: le normative sugli ADMT sono in vigore dal 1° gennaio 2026. Nel 2027 assumono particolare rilievo le informative pre-utilizzo e i diritti di accesso e opposizione applicabili alle decisioni significative.
- Colorado: l'Automated Decision-Making Technology Act sostituisce la precedente normativa sull'IA ad alto rischio, richiedendo alle organizzazioni di rivedere i piani di compliance.
- Illinois: i requisiti sull'IA in ambito lavorativo dell'HB 3773 sono in vigore dal 1° gennaio 2026. Il Frontier AI Safety Measure Act (SB 315) introduce inoltre requisiti di governance della sicurezza per i principali sviluppatori di IA.

Questi requisiti incidono sempre più sulle decisioni di approvvigionamento e implementazione.



“

Le questioni più importanti devono essere affrontate durante l’approvvigionamento, non in fase di aggiornamento della compliance. Il modello di terze parti può essere addestrato sui dati personali e quali garanzie contrattuali lo impediscono? Gli amministratori possono decidere se attivare una nuova funzionalità integrata? Lo strumento di trascrizione IA utilizza impronte vocali, facendo scattare eventuali normative sulla privacy biometrica?”.

Abigail Walker
Associate, Emerging Technologies, Global Corporate Group,
Reed Smith LLP

L’Illinois mostra inoltre come la supervisione dell’IA debba tenere conto dei diritti individuali nelle decisioni in ambito lavorativo.

“

Entro il 2027, l’Illinois potrebbe diventare un punto di riferimento per la governance dell’IA, ponendo l’accento non solo sull’adozione, ma anche sulla responsabilità. Ai datori di lavoro sarà richiesta maggiore trasparenza sulle decisioni automatizzate, insieme alla valutazione dei bias e a strumenti per contestarne i risultati. Il Frontier AI Safety Measure Act (SB 315) amplia inoltre l’attenzione alla sicurezza dell’IA, con quadri di mitigazione dei rischi, segnalazione degli incidenti e audit indipendenti previsti entro il 2028. Nel complesso, emerge un approccio all’innovazione dell’IA più responsabile e incentrato sulle persone.”

Megan M. Miller
Founder & Attorney, Miller Mosaic
The Identity Counsel

Le organizzazioni devono integrare i requisiti legali in approvvigionamento, configurazioni, decisioni rilevanti ed evidenze di supervisione, prima che emergano problemi.



Unione europea: dalle regole alle evidenze

La legge sull'IA dell'UE è entrata in vigore nel 2024 ed è stata applicata dal 2 agosto 2026. L'introduzione graduale degli obblighi rende classificazione dei rischi, documentazione, trasparenza e supervisione priorità di attuazione.

Il Digital Omnibus sull'IA, in vigore dal 27 luglio 2026, ha modificato le tempistiche per i sistemi ad alto rischio. Gli obblighi per i sistemi dell'allegato III, inclusi determinati utilizzi in ambito lavorativo, educativo e biometrico, si applicano dal 2 dicembre 2027; per quelli integrati in prodotti regolamentati, dal 2 agosto 2028.

Le nuove date offrono maggiore chiarezza, ma restano dubbi sull'attuazione, soprattutto sulla disponibilità degli standard armonizzati e sulla preparazione delle autorità nazionali.

> **Nel 2027, il cambiamento più significativo sarà l'affermarsi dell'intelligenza infrastrutturale. L'IA non sarà più solo terreno di competizione tecnologica, militare ed energetica tra Stati Uniti, Europa e Cina, ma sarà sempre più integrata nella vita quotidiana, dalla sanità alla ricerca di lavoro e alla distribuzione delle risorse."**
>
> **Mahdi Barkabian Zanjani**
> Esperto indipendente

È importante distinguere tra obblighi rinviati e già applicabili. Il GDPR continua ad applicarsi ai trattamenti di dati personali pertinenti e gli obblighi della legge sull'IA restano applicabili secondo le rispettive tempistiche.

Valutazioni e documentazione devono riflettere i sistemi effettivamente in uso. Un nuovo modello, fornitore o collegamento può rimettere in discussione quanto stabilito dall'approvazione precedente.



Regno Unito: più peso alle norme esistenti che a un nuovo AI Act

Il Regno Unito segue un percorso diverso, senza una normativa organica sull'IA che ne definisca l'approccio. La vigilanza settoriale e i requisiti di sicurezza informatica esistenti potrebbero avere effetti più immediati rispetto a una legge specifica sull'IA.

> "È improbabile che l'atteso AI Bill del Regno Unito si concretizzi nel 2027. Il governo potrebbe invece introdurre misure di sicurezza informatica legate all'IA nel Cyber Security and Resilience (Network and Information Systems) Bill, compresi nuovi obblighi di segnalazione per incidenti gravi e mancati incidenti legati all'IA nei servizi essenziali, oltre a quelli previsti per incidenti e supervisione della catena di fornitura dei fornitori critici."

Katie Hewson
Partner
Stephenson Harwood

Il Cyber Security and Resilience Bill è ancora in fase di iter legislativo. I potenziali obblighi vanno distinti dai requisiti di vigilanza già applicabili.

Nei settori regolamentati, la priorità è comprendere come l'IA incida sulle responsabilità esistenti per responsabilizzazione, supervisione dei fornitori, rischio dei modelli e resilienza operativa. Attendere una normativa specifica sull'IA potrebbe lasciare questi obblighi non adeguatamente gestiti.

Corea del Sud: le evidenze operative diventano centrali

La legge fondamentale sull'IA della Corea del Sud è in vigore dal 22 gennaio 2026. L'applicazione graduale pone l'accento sull'individuazione dei sistemi di IA ad alto impatto e sulla documentazione dei controlli prima dell'implementazione.

> "L'onere più sottovalutato sarà probabilmente l'inventario e la classificazione dell'IA. Le funzionalità di IA sono sempre più integrate nei software e nei servizi di terze parti, mentre il regime sudcoreano per l'IA ad alto impatto riguarda ambiti sensibili come selezione del personale, credito, sanità, istruzione e determinate decisioni della pubblica amministrazione. La sfida sarà individuare l'IA nei processi aziendali esistenti e stabilire quali sistemi comportano obblighi aggiuntivi."

Timothy Dickens
Partner
DR&AJU Law Group LLC

Non basta individuare un sistema: occorre documentarne la classificazione, le misure di tutela, la supervisione umana e le relative evidenze.

Brasile: il rinvio della legge sull'IA non crea un vuoto normativo

La proposta brasiliana di un quadro normativo organico sull'IA, PL 2338/2023, è stata approvata dal Senato nel dicembre 2024, ma l'iter legislativo non è ancora concluso.

Le attività di IA sono già soggette alla normativa vigente. La LGPD, compreso l'articolo 20 sulle decisioni automatizzate, e il Codice di tutela dei consumatori impongono obblighi che non possono essere rinviati in attesa di una normativa organica sull'IA.

> "Le aziende devono andare oltre l'attesa del PL 2338/2023 e basare la governance sulle norme già applicabili: LGPD, linee guida dell'ANPD e norme settoriali a tutela dei consumatori. La ISO/IEC 42001 può dimostrare un livello di diligenza di base, ma non sostituisce gli obblighi di legge né esclude la responsabilità per conseguenze dannose dell'IA."

Adriana Ruggeri Quinelo
Legal Counsel & Advisor
Ruggeri Quinelo

La distinzione è particolarmente importante per chi adotta standard volontari di governance. Una certificazione può dimostrare la diligenza adottata, ma non garantisce la compliance delle decisioni automatizzate alle norme brasiliane su privacy e tutela dei consumatori.



Regimi diversi, questioni di governance comuni

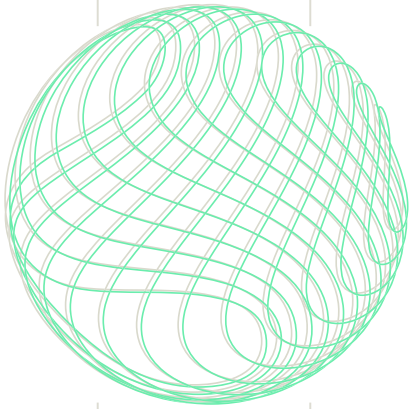
Queste giurisdizioni non stanno convergendo verso regole identiche. Dai contributi degli esperti emerge però un dato più utile: molte delle questioni operative sono sempre più simili.

Individuazione

È possibile sapere dove viene utilizzata l'IA, comprese le funzionalità integrate nei software esistenti e quelle fornite da terze parti?

Contesto

È possibile identificare le persone, le informazioni, le decisioni e i processi aziendali su cui incidono i sistemi di IA?



Controllo

È possibile stabilire dove si applicano autorizzazioni, intervento umano, trasparenza, restrizioni e procedure di escalation?

Evidenze

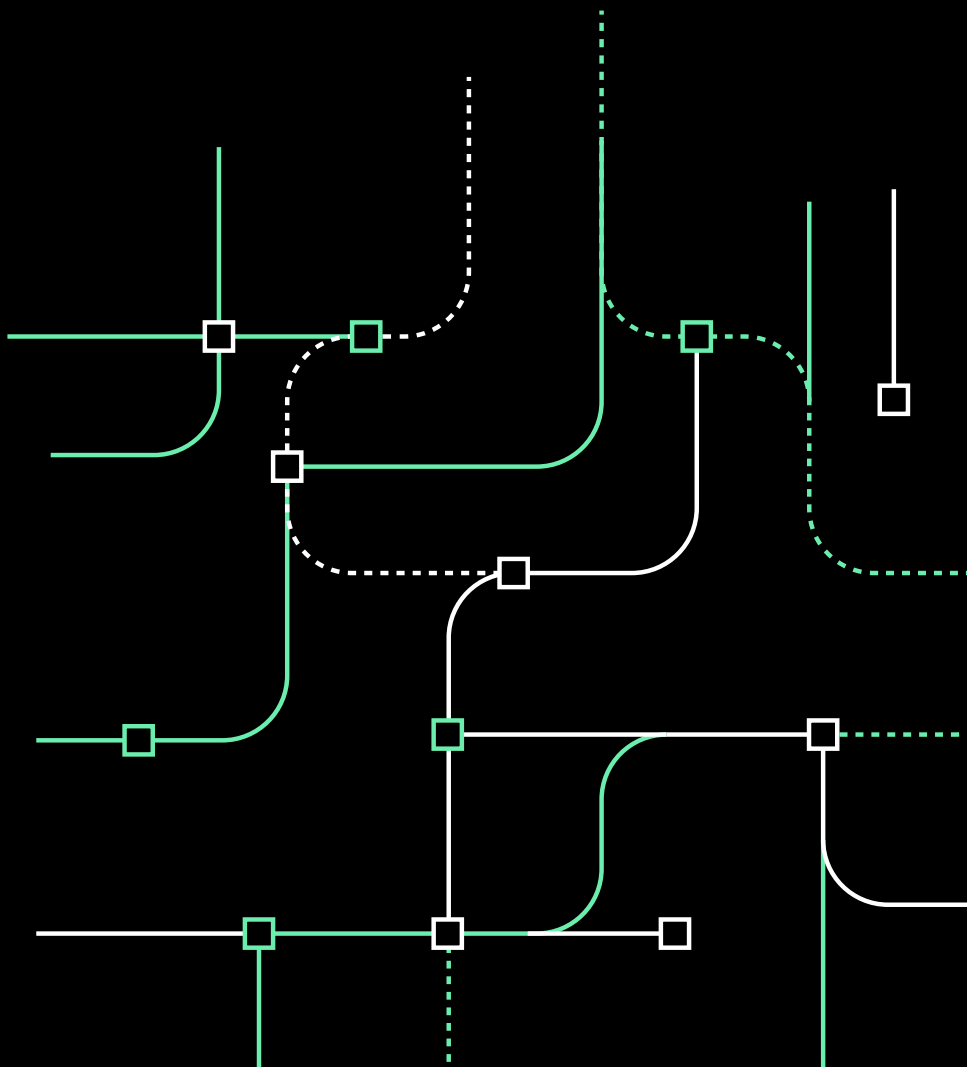
È possibile ricostruire ciò che è stato valutato, quale sistema era in funzione, cosa è cambiato e chi ne era responsabile?

Queste capacità restano rilevanti anche quando cambiano le tempistiche normative. Consentono alle organizzazioni di reagire quando entra in vigore una nuova norma, una legge esistente viene applicata all'IA o un'autorità di vigilanza interviene su una specifica implementazione.

I percorsi normativi continueranno a essere diversi. Ma sul piano operativo il quadro diventa più chiaro: la governance deve accompagnare l'IA dall'approvazione all'utilizzo.

Controprevisioni

Tre scenari poco probabili nel 2027



Controprevisione 1

Le garanzie di base non saranno sufficienti per ogni decisione di implementazione

Una valutazione può restare valida entro il suo ambito originario senza esaminare a sufficienza una modalità di implementazione modificata. La questione è se le evidenze continuino a coprire le capacità del sistema, l'uso previsto e i controlli su cui si fonda l'approvazione.

> “La certificazione può mostrare a regolatori, investitori e partner commerciali che l'organizzazione ha agito con la dovuta diligenza, ma non la mette al riparo da conseguenze legali. Resta necessario conoscere le leggi e gli obblighi di settore che si applicano ai sistemi di IA utilizzati.”

Adriana Ruggeri Quinelo
Legal Counsel & Advisor
Ruggeri Quinelo

Un test di penetrazione svolto a gennaio potrebbe non aver verificato le funzionalità aggiunte a marzo. Lo stesso vale per le ipotesi su cui si basa un'approvazione: una nuova connessione, privilegi più ampi o controlli meno efficaci possono richiedere di rivedere la decisione, anche se il quadro generale delle garanzie dell'organizzazione resta valido.

> “Un cliente può fidarsi delle garanzie di un servizio e chiedere comunque nuovi test prima di attivare una funzionalità modificata. Il punto è capire se le evidenze riguardano davvero ciò che userà. Le garanzie già disponibili ci danno una base, ma dobbiamo chiarire dove il cambiamento richiede qualcosa in più.”

Tim Mullen
Chief Information Officer
OneTrust

Nel 2027, le organizzazioni dovranno verificare se le garanzie già in essere siano ancora sufficienti per una versione modificata del sistema di IA. Il riesame aggiuntivo dovrebbe riguardare i presupposti su cui il cambiamento ha inciso, senza scartare le evidenze che rimangono valide.

Controprevisione 2

Aumentare il personale non renderà scalabile la supervisione

Per le policy, le decisioni delicate e le eccezioni, le organizzazioni continueranno a fare affidamento sulle persone. Ma, man mano che aumenteranno i flussi di lavoro gestiti da agenti di IA, sarà più difficile far intervenire una persona prima di ogni singola azione.

> “Il monitoraggio umano non sarà scalabile rispetto al volume di attività che stiamo descrivendo. Mi aspetto che il monitoraggio continuo diventi sempre più agentico. Ciò cambierà il modo in cui viene esercitata la supervisione e comporterà un’ulteriore responsabilità: valutare il sistema di monitoraggio stesso.”

Ojas Rege
SVP Emerging Products and Technologies
OneTrust

La scelta pratica è decidere quando serve il giudizio di una persona e cosa può andare avanti a determinate condizioni. In un flusso circoscritto, si può chiedere l’approvazione prima di ogni azione importante. In un altro, può essere meglio delegare meno autorità e coinvolgere un livello superiore se le condizioni cambiano.

Anche il monitoraggio automatico va messo alla prova. I responsabili devono verificare che rilevi il problema giusto, avvisi una persona che ne sia responsabile e permetta di intervenire in modo efficace.

> “Quando l’IA entra nel lavoro di tutti i giorni, tutti devono sapere come usarla in modo responsabile. La sfida è rendere le regole di governance facili da seguire e, allo stesso tempo, mantenere l’uso sicuro.”

Federico Sembolini
Senior Manager AI Transformation - AI Governance
BBVA

L’obiettivo è usare l’IA giusta, senza rallentare inutilmente. Il tempo tra la richiesta e l’approvazione di una funzionalità può mettere in luce attese evitabili. La qualità delle decisioni, la gestione delle eccezioni e gli incidenti dopo l’approvazione aiutano a capire se il processo è responsabile.

Più personale non significa verifiche umane alla velocità delle macchine. Se una persona deve controllare ogni azione, la supervisione non può stare al passo con agenti che operano tra sistemi diversi. Servono limiti applicabili e un monitoraggio che segnali quando è necessario l’intervento umano, dando alle persone la possibilità di agire con efficacia. Assumere può rafforzare la supervisione, ma non risolve la necessità di cambiare il modo in cui il lavoro viene governato.

Controprevisione 3

Non tutte le incertezze potranno essere risolte prima di decidere

La cosa meno credibile che potremmo promettere sul 2027 è di sapere già esattamente cosa ci riserva.

I modelli continueranno a evolversi e nuovi casi d'uso metteranno alla prova decisioni che oggi sembrano consolidate. Alcune previsioni di questo rapporto potrebbero concretizzarsi prima del previsto, mentre altre richiederanno più tempo. Anche il contesto di mercato influenzerà le funzionalità che le organizzazioni sceglieranno di adottare.

Le organizzazioni dovranno comunque stabilire quali applicazioni dell'IA consentire e a chi spetterà rispondere delle conseguenze.

Nel 2027, molte decisioni andranno prese prima di disporre di evidenze consolidate sulla funzionalità successiva o sul nuovo modello operativo. Attendere un quadro di governance completo lascia i team vincolati alle approvazioni e alle abitudini esistenti, anche se il modo di lavorare è cambiato.

> “Non esiste una risposta valida per tutti: ogni azienda deve capire cosa funziona nel proprio contesto. Con la spinta a usare sempre più strumenti di IA, la sfida è stabilire chi è responsabile della governance e come applicarla.”

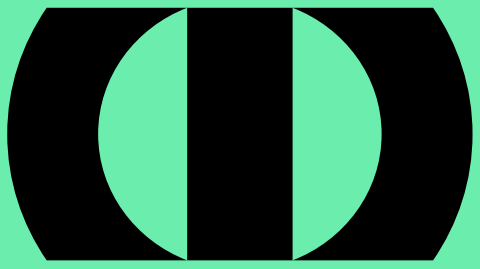
Bruna Baccini
Head of Compliance & DPO
GOL Airlines

> “Non dobbiamo temere le potenzialità dell'IA, ma nemmeno affrettarci a sfruttarle. La tecnologia corre a velocità vertiginosa, ma le persone hanno bisogno di tempo per cambiare. Dobbiamo considerare l'impatto sulle persone, oltre agli aspetti tecnologici.”

Aaron Weller
Leader of Privacy Innovation and Assurance
HP

La risposta pratica è rendere le decisioni rivedibili. Ogni approvazione dovrebbe specificare le condizioni in cui resta valida e cosa richiede un nuovo riesame. I responsabili devono inoltre sapere chi è autorizzato a modificarla quando tali condizioni non sussistono più.

Progettare un sistema di governance significa fare in modo che le decisioni possano essere riviste senza perdere di vista chi ne risponde. Nel 2027, la leadership dovrà verificare se l'organizzazione è in grado di modificare l'autorità concessa a un flusso di lavoro basato sull'IA e di spiegare chi ha approvato la modifica, cosa consente e come interromperlo.



www.onetrust.com

Dichiarazione di non responsabilità
Nessuna parte di questo documento può essere riprodotta in alcuna forma senza il permesso scritto del proprietario del copyright. I contenuti di questo documento sono soggetti a revisione senza preavviso a causa dei continui progressi nella metodologia, nella progettazione e nella produzione. OneTrust LLC non si assume alcuna responsabilità per eventuali errori o danni di qualsiasi tipo derivanti dall'uso di questo documento. I prodotti, i contenuti e i materiali di OneTrust sono esclusivamente a scopo informativo e non hanno il fine di fornire consulenza legale. Si consiglia di rivolgersi al proprio legale per richiedere consulenza su temi specifici. I materiali OneTrust non garantiscono la conformità alle leggi e alle normative vigenti.

Copyright © 2026 OneTrust LLC. Tutti i diritti riservati. Informazioni proprietarie e riservate.