DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Impiegare gli agenti di intelligenza artificiale nell'attività di impresa

Definizione funzionale, governance, casi d'uso e configurazione operativa

Maggio 2026

Alessandro del Ninno, Partner, Fivers

Alessandro del Ninno, Partner, Fivers

Alessandro del Ninno

Alessandro del Ninno è titolare delle Cattedre di Informatica Giuridica e di Intelligenza Artificiale, Machine Learning e Diritto presso la LUISS Guido Carli di Roma. Avvocato del Foro di Roma e Socio dello Studio legale e tributario Fivelex. È altresì: Appointed member del Pool of Experts europei di supporto e consulenza al Comitato europeo per la protezione dei dati personali; Presidente del Comitato Scientifico dell'Associazione Nazionale per la protezione dei dati personali; Membro e Vicepresidente del Comitato Scientifico dell'Istituto Italiano Privacy.

1. Che cosa sono gli agenti di IA? Una possibile definizione pratica, tecnica e funzionale

Un agente di intelligenza artificiale può essere descritto come un sistema dotato dei seguenti elementi strutturali, operativi, funzionali:

1. riceve un obiettivo
2. organizza una sequenza di azioni secondo regole prestabilite
3. accede ed utilizza strumenti, basi documentali e fonti autorizzate
4. mantiene una memoria operativa
5. concorre al compimento di un processo
6. con livelli di autonomia variabile entro soglie predefinite
7. potendo essere sempre supervisionato o interrotto.

La cifra distintiva dell'agente non è quindi la sola capacità di rispondere a domande, produrre testi o suggerire, ma la capacità di incidere sul flusso operativo aziendale, collegando più passaggi verso un risultato pratico.

Dal punto di vista delle funzioni, un agente di IA può raccogliere informazioni, ordinare documenti, predisporre minute, attivare passaggi interni, segnalare anomalie, proporre scelte operative e, nei casi più evoluti, coordinare attività fra più applicativi o più moduli.

In termini di inquadramento normativo, occorre rilevare che il Regolamento (UE) 2024/1689 costruisce la nozione di "*sistema di IA*", ma non introduce una categoria giuridica autonoma e nominata di "*agente di IA*". Ne deriva che, sul piano del diritto positivo, l'agente deve essere normalmente trattato come una specifica modalità di impiego di uno o più sistemi di IA, la cui disciplina concreta varia in funzione del caso d'uso, del ruolo dell'operatore coinvolto (fornitore, deployer, importatore, distributore), del livello di rischio e degli effetti che l'impiego del sistema produce su persone, diritti o processi.

vedi l'articolo online

2. Inquadrare gli agenti di Intelligenza Artificiale: le differenze tra l'IA generativa e l'IA agentica

La differenza essenziale tra IA generativa e IA agentica non sta tanto nella sofisticazione tecnica del sistema, quanto nella funzione che esso svolge all'interno dell'attività aziendale. L'IA generativa, infatti, opera soprattutto come strumento di produzione di contenuti: redige un testo, sintetizza documenti, propone una bozza, formula una risposta. L'IA agentica, invece, utilizza eventualmente anche queste capacità, ma le inserisce in una sequenza più ampia di azioni finalizzate a raggiungere un risultato operativo. In altri termini, mentre l'IA generativa produce un output, l'IA agentica partecipa allo svolgimento di un compito, combinando memoria, regole, strumenti e accesso a fonti informative per far avanzare il processo. Da qui deriva anche una diversa natura del rischio. Nel caso dell'IA generativa, il problema principale riguarda l'attendibilità del contenuto prodotto; nel caso dell'IA agentica, invece, l'attenzione deve estendersi al comportamento del sistema nel processo aziendale in cui l'agente è inserito: conta non solo ciò che il sistema scrive o suggerisce, ma anche ciò che fa, in quale momento lo fa, su quali dati interviene e con quali possibili conseguenze organizzative o giuridiche per l'impresa.

La distinzione emerge con particolare chiarezza se si immagina, ad esempio, la gestione di un reclamo assicurativo complesso presentato da un cliente della Compagni che vi acclude e-mail, modulo di denuncia, documentazione medica e precedenti interlocuzioni con il call center.

In un primo scenario, l'impresa utilizza una IA generativa in forma meramente ausiliaria. Un addetto carica i documenti nel sistema e gli chiede di riassumere i fatti, mettere in evidenza i profili critici e predisporre una prima bozza di risposta interna. In questo caso il sistema non compie alcun passaggio autonomo nel procedimento: si limita a restituire un testo, una sintesi, eventualmente una traccia di lavoro, e si arresta lì. Sarà poi l'operatore umano a leggere il materiale, confrontarlo con i documenti originali, correggere eventuali errori e decidere se utilizzare o meno la bozza predisposta. L'IA, dunque, resta esterna al flusso operativo vero e proprio: supporta il lavoro umano, ma non incide direttamente sulla sequenza delle attività.

Diversa è l'ipotesi in cui l'impresa -nel medesimo scenario ipotizzato - si avvalga di una IA agentica. In quel caso l'IA non si limita a produrre una sintesi, ma riceve il reclamo, apre il fascicolo, classifica la contestazione, recupera i precedenti dal gestionale che la Compagnia utilizza, consulta la documentazione interna pertinente, elabora una proposta di risposta, la trasmette al referente competente, segnala l'eventuale urgenza e predispone il successivo passaggio autorizzativo. In tale scenario il sistema entra nel processo della Compagnia (gestione reclami) e contribuisce a orientarlo. Non è più soltanto uno strumento di supporto redazionale, ma una componente che organizza e fa avanzare una serie di attività. Proprio per questo la differenza tra i due scenari è profonda.

Nel primo caso il rischio si concentra soprattutto sulla qualità del testo o della sintesi prodotta; nel secondo, invece, il rischio investe anche la correttezza dell'azione compiuta dal sistema, la pertinenza delle fonti selezionate, la linearità della catena operativa, la tracciabilità dei passaggi e il grado di affidamento che l'organizzazione ripone nell'agente.

Se un sistema generativo sbaglia una sintesi, l'errore può normalmente essere intercettato e corretto prima che produca effetti; se, invece, un sistema agentico classifica male il reclamo, richiama documenti non pertinenti o attiva il passaggio sbagliato, l'errore si innesta direttamente nel procedimento e può propagarsi con maggiore rapidità e con conseguenze più incisive.

3. Agenti di intelligenza artificiale: perché il tema riguarda già oggi l'impresa?

Il passaggio dall'intelligenza artificiale generativa all'intelligenza artificiale agentica incide in profondità sull'assetto di governo dell'impresa, poiché non si traduce in un mero incremento qualitativo o quantitativo dell'output prodotto dal sistema, ma comporta un mutamento ben più rilevante: la diversa collocazione funzionale della tecnologia all'interno dei processi organizzativi.

L'IA generativa, infatti, opera ordinariamente sul piano della produzione di contenuti, della sintesi, della classificazione o della formulazione di proposte, mantenendosi, di regola, esterna alla determinazione conclusiva e all'azione esecutiva. L'agente di intelligenza artificiale, per converso, non si esaurisce nella dimensione di supporto, suggerimento o redazionale, ma si inserisce – come detto - nella sequenza operativa del processo aziendale, concorrendo al suo avanzamento attraverso l'attivazione, il coordinamento o l'orientamento di una pluralità di passaggi funzionalmente collegati.

Ne deriva che il valore dell'agente non può essere apprezzato unicamente alla luce della qualità del contenuto restituito, bensì in ragione della sua capacità di incidere sull'esecuzione concreta di attività

aziendali. Ed è precisamente tale traslazione dal piano dell'assistenza cognitiva a quello dell'interferenza operativa a rendere il tema immediatamente rilevante per l'impresa. Ove tale distinzione non venga adeguatamente colta, vi è il rischio che gli agenti di IA vengano introdotti come meri fattori di efficienza, con conseguente sottovalutazione degli effetti che essi producono sulla ripartizione delle responsabilità, sulla formazione e conservazione della documentazione, sull'assetto dei controlli interni e, in ultima analisi, sull'esercizio stesso dei poteri decisionali.

La questione, pertanto, non si esaurisce nel domandarsi se l'impresa possa utilizzare agenti di IA, ma impone di stabilire se, in quali ambiti e secondo quali limiti tale impiego risulti giuridicamente e organizzativamente sostenibile. Quando una tecnologia partecipa in modo attivo, e talora parzialmente autonomo, al flusso operativo, diviene infatti necessario ridefinire con precisione ruoli, competenze, verifiche, autorizzazioni e presìdi di responsabilità, nonché individuare ex ante il perimetro entro cui l'agente può legittimamente muoversi. L'impatto sull'organizzazione varia sensibilmente a seconda che il sistema si limiti a consultare fonti documentali, predisponga atti interni, avvii segmenti procedimentali o segnali anomalie suscettibili di incidere su decisioni ulteriori. Per tale ragione, il problema centrale non consiste nell'accertare il grado di "intelligenza" della soluzione adottata, quanto nel verificare se l'ampiezza del suo spazio operativo sia compatibile con la struttura di governo dell'impresa, con la natura del processo interessato e con i vincoli giuridici che lo presidiano.

Proprio perché l'IA agentica interviene nel processo, e non soltanto sul contenuto, essa non può essere governata mediante i soli strumenti regolatori che molte organizzazioni avevano approntato per l'impiego dell'IA generativa, quali istruzioni d'uso di carattere generale, divieti indistinti di inserimento di dati riservati o controlli meramente successivi sull'output. L'adozione dell'IA agentica esige, al contrario, una vera e propria architettura preventiva di governo, fondata sulla (1) puntuale delimitazione del caso d'uso, sulla (2) classificazione dei dati trattati, sulla(3) segregazione degli accessi, sulla (4) predeterminazione di soglie di rischio e di livelli autorizzativi, (5) sulla registrazione e tracciabilità delle attività compiute, sulla (6) definizione di regole di intervento umano e sulla (7) chiara imputazione delle responsabilità tra funzione richiedente, funzione tecnica, funzione legale e fornitore della soluzione. Solo entro una simile cornice di governo l'impresa può utilizzare l'IA agentica in modo effettivamente controllato, coerente con il proprio assetto organizzativo e compatibile con le esigenze di compliance, accountability e difendibilità del processo.

4. I principali impatti dell'IA agentica sull'organizzazione d'impresa: tempi, costi, controlli, responsabilità e qualità dei risultati

L'introduzione di un agente IA in azienda non modifica un solo elemento del processo, ma ne altera contemporaneamente tempi di esecuzione, struttura dei costi, intensità dei controlli, distribuzione delle responsabilità e qualità attesa dei risultati.

Sul piano dei tempi, l'agente promette una forte accelerazione, perché riduce passaggi manuali, tempi di ricerca e attività ripetitive. In molti casi, soprattutto nei processi documentali o nei flussi interni di verifica, questo vantaggio è reale e immediatamente percepibile. Tuttavia, proprio la velocità costituisce anche un fattore di rischio, perché un errore compiuto da un agente, se non intercettato in tempo, tende a propagarsi lungo il processo con la stessa rapidità con cui il sistema genera efficienza.

Sul piano dei costi, l'impatto è altrettanto ambivalente. Da un lato, l'agente può ridurre il fabbisogno di lavoro su attività a basso valore aggiunto, liberando tempo del personale per attività di supervisione, valutazione e decisione. Da questo punto di vista, il beneficio economico esiste, soprattutto nei contesti in cui vi siano volumi elevati di operazioni standardizzabili. Dall'altro lato, però, l'adozione dell'agente non elimina il costo del processo, ma ne sposta la composizione, aumentando il costo del presidio.

Sul piano dei controlli, l'introduzione dell'agente impone un salto di qualità nelle procedure interne. Un agente non è uno strumento che si limita a essere "usato", ma una componente del processo che deve essere progettata, delimitata, verificata e riesaminata nel tempo. Per questo motivo, le procedure aziendali devono diventare più precise: occorre stabilire quali attività il sistema possa svolgere, quali dati possa utilizzare, quali strumenti possa interrogare, in quali casi possa procedere in autonomia e in quali altri debba invece fermarsi e rimettere la decisione a un essere umano. Il controllo non può più essere pensato solo come verifica finale dell'output, ma deve diventare controllo del comportamento del sistema, della sua collocazione nel processo e della sua conformità rispetto alle regole organizzative definite dall'impresa.

Anche sul piano delle responsabilità gli agenti producono un effetto immediato e spesso sottovalutato.

Più il sistema incide sui flussi operativi, più diventa necessario chiarire chi abbia deciso l'adozione, chi abbia autorizzato il caso d'uso, chi abbia definito il perimetro operativo, chi sia incaricato del controllo e chi abbia il potere di approvare o bloccare i passaggi più sensibili. Questo è un punto decisivo, perché l'automazione tende facilmente a generare zone grigie nelle quali tutti partecipano al processo, ma nessuno appare chiaramente titolare della responsabilità finale. Una *governance* seria degli agenti deve invece fare l'opposto: deve rendere più visibile, e non meno visibile, la distribuzione delle responsabilità interne. Solo così l'impresa evita che il ricorso all'IA diventi un fattore di deresponsabilizzazione diffusa.

Quanto alla qualità dei risultati, questo è forse l'impatto più insidioso, proprio perché spesso viene frainteso. La qualità non coincide con la scorrevolezza del testo generato, con la rapidità della risposta o con l'apparente persuasività dell'output. Un risultato di qualità della operatività di un agente di IA, in ambito aziendale, è un risultato coerente con il processo in cui si inserisce, verificabile nella sua base informativa, ripetibile secondo criteri ragionevoli e adeguato alle finalità concrete dell'attività. In altre parole, non basta che l'agente "scriva bene" o "riassuma bene": occorre che ciò che produce sia corretto, controllabile e utilizzabile senza alterare il processo o introdurre errori sistemici. Questo vale ancora di più nei contesti in cui il risultato del sistema si avvicina a decisioni, comunicazioni o valutazioni che hanno rilievo verso l'esterno o verso altri soggetti dell'organizzazione.

5. La mappatura dei casi d'uso più frequenti di impiego degli agenti di IA in azienda

Prima di introdurre agenti di intelligenza artificiale nei processi aziendali, è indispensabile individuare con precisione i relativi casi d'uso, evitando di assumere la tecnologia come punto di partenza in astratto. L'esigenza preliminare non è, infatti, quella di verificare se l'agente sia tecnicamente utilizzabile, bensì di comprendere in quali ambiti il suo impiego sia effettivamente idoneo a generare un'utilità concreta e in quali, al contrario, rischi di accrescere la complessità organizzativa o il livello di esposizione al rischio senza un corrispondente vantaggio operativo. In questa prospettiva, è possibile ricondurre gli impieghi più frequenti a cinque aree ricorrenti:

1. gli uffici amministrativi, legali e acquisti;
2. l'assistenza alla clientela e la gestione dei reclami;
3. le risorse umane e la formazione;
4. l'area commerciale, il marketing e la comunicazione;
5. le tecnologie informatiche e la sicurezza.

Una simile attività di mappatura è essenziale perché ciascuna funzione aziendale presenta caratteristiche proprie, utilizza dati differenti, è soggetta a diverse soglie di rischio e si colloca in rapporti non omogenei con interlocutori interni o esterni all'organizzazione.

Mappare i casi d'uso significa, dunque, distinguere i processi che esauriscono i propri effetti all'interno dell'impresa da quelli suscettibili di produrre conseguenze nei confronti di clienti, lavoratori, partner commerciali o autorità. Significa, altresì, stabilire quali impieghi possano essere governati mediante forme di supervisione relativamente semplici e quali richiedano, invece, presìdi più intensi, controlli strutturati e validazioni rafforzate. Un agente può rivelarsi estremamente efficace, ad esempio, nelle attività di *triage* documentale o di supporto istruttorio, ma risultare del tutto inadeguato ove venga collocato in fasi di decisione finale o di comunicazione ufficiale verso l'esterno. Proprio per questo, la mappatura dei casi d'uso non costituisce un adempimento meramente ricognitivo o descrittivo, ma rappresenta il presupposto sostanziale di ogni adozione consapevole, proporzionata e responsabile dell'IA agentica.

5.1 *Casi d'uso in uffici amministrativi, legali e acquisti*

Negli uffici amministrativi, gli agenti di IA possono essere impiegati per sostenere l'avanzamento ordinato del procedimento, soprattutto nelle fasi iniziali di verifica, instradamento e monitoraggio della pratica. Il loro contributo è particolarmente utile quando il processo richiede controlli ripetitivi, accesso a documentazione standardizzata e gestione di passaggi interni già definiti dalla procedura aziendale. In questo contesto, l'agente non assume decisioni sostanziali, ma aiuta a rendere più rapidi e più lineari i passaggi preparatori e organizzativi.

Un agente di IA può:

1. verificare se la pratica sia completa
2. accedere agli archivi autorizzati
3. segnalare i documenti mancanti
4. aprire una richiesta interna
5. indirizzarla al referente competente
6. predisporre il passaggio autorizzativo successivo e
7. monitorare e aggiornare lo stato del flusso.

Nelle funzioni legali, l'impiego dell'agente può risultare utile soprattutto nelle attività di supporto alla revisione documentale e alla gestione del primo livello istruttorio. In tale ambito, il sistema può agevolare il lavoro del referente legale mettendo in evidenza scostamenti, anomalie o clausole meritevoli di attenzione, ma non può mai sostituirsi alla valutazione professionale richiesta dal caso concreto. Il suo ruolo, dunque, è quello di assistere il processo di analisi, non di prendere posizione sul merito giuridico o negoziale delle soluzioni esaminate .Nelle funzioni legali un agente IA può essere istruito per:

1. ricevere una bozza del contratto
2. confrontarla con il modello approvato dall'azienda
3. individuare le deviazioni rispetto alle clausole standard
4. classificare le deviazioni per livello di sensibilità
5. aprire una pratica interna di revisione
6. indirizzarla automaticamente al referente legale competente
7. segnalare che una determinata clausola esce dai limiti normalmente accettati e
8. predisporre il fascicolo per il successivo livello autorizzativo.

Occorre però ribadire con chiarezza che l'agente non può essere confuso con il titolare del giudizio professionale. Una cosa, infatti, è rilevare una difformità testuale o segnalare uno scostamento rispetto a uno standard interno; altra cosa è stabilire se quella difformità sia giuridicamente sostenibile, contrattualmente accettabile o coerente con l'interesse dell'impresa nel caso concreto. Tale valutazione resta necessariamente rimessa al professionista competente.

Anche nella funzione acquisti l'agente può essere inserito in modo utile nel procedimento di qualifica del fornitore, in particolare per rendere più ordinata, rapida e controllabile la gestione documentale e il passaggio tra le diverse fasi del processo di *due diligence* o di qualifica. In questo caso, il sistema può svolgere una funzione di supporto operativo particolarmente efficace, purché resti ben delimitato il confine tra attività istruttoria e decisione finale.

Nella funzioni acquisti/procurement un agente IA può essere istruito per:

1. controllare automaticamente la check-list documentale prevista dalla procedura aziendale
2. verificare quali allegati siano mancanti
3. creare una richiesta di integrazione
4. inviarla al referente del fornitore
5. aggiornare il fascicolo interno
6. segnalare alla funzione acquisti che il procedimento può passare alla fase successiva e
7. predisporre il dossier per la successiva approvazione.

L'elemento di maggiore delicatezza, comune alle funzioni amministrative, legali e acquisti, risiede nel fatto che tutte e tre operano su documenti e informazioni che possono assumere rilievo giuridi-

co, economico o anche probatorio. Proprio per questo, il ricorso all'agente presenta certamente utilità concrete, ma richiede un presidio organizzativo più rigoroso di quello normalmente sufficiente per un semplice strumento di IA generativa. Non basta, dunque, affermare in termini generici che "*l'umano resta al centro*". Occorre piuttosto definire con precisione quali attività l'agente possa limitarsi a preparare, quali azioni possa effettivamente attivare, quali passaggi debbano essere sempre sottoposti a conferma umana e quali effetti non possano in nessun caso prodursi senza una validazione espressa del referente competente..

5.2 *Casi d'uso nell'area assistenza alla clientela e gestione dei reclami*

Nell'ambito dell'assistenza alla clientela, gli agenti di IA possono offrire un contributo particolarmente utile nelle attività di prima analisi, di ricostruzione del contesto e di organizzazione delle informazioni rilevanti. Il loro impiego risulta funzionale soprattutto quando il processo richiede una rapida classificazione delle richieste ricevute, il recupero ordinato dei documenti pertinenti e l'individuazione del canale interno più appropriato per la successiva gestione del caso. In tale prospettiva, l'agente può agevolare il lavoro degli operatori, alleggerendo le attività preliminari a più basso valore aggiunto e rendendo più lineare la fase istruttoria.

Nella gestione dei reclami, in particolare, l'agente può ricevere la richiesta del cliente, distinguere la tipologia di problematica segnalata, interrogare le basi documentali autorizzate, recuperare i precedenti rilevanti e predisporre una prima traccia di risposta o di lavorazione interna. Il suo apporto, dunque, può risultare prezioso nel riordinare i fatti, nel collegare la documentazione disponibile e nel predisporre un primo quadro di sintesi utile ai referenti competenti.

Proprio questo settore, tuttavia, rende particolarmente evidente il limite dell'automazione non adeguatamente presidiata. Quando il reclamo assume rilievo patrimoniale, reputazionale, regolatorio o persino precontenzioso, l'impresa non può tollerare che il rapporto con il cliente sia governato da comunicazioni opache, logicamente fragili o non coerenti con il caso concreto. Un agente che organizzi in modo inesatto il fascicolo, qualifichi in maniera scorretta la contestazione o suggerisca formulazioni improprie può aggravare la controversia invece di contribuire alla sua ordinata gestione.

Per tale ragione, la funzione dell'agente, in questo ambito, deve essere generalmente configurata come funzione istruttoria e preparatoria, non come sede della decisione finale o della comunicazione conclusiva verso l'esterno. Diviene quindi essenziale stabilire con precisione quali contenuti il sistema possa predisporre, quali valutazioni debbano restare riservate al referente umano e, soprattutto, quali formule, impegni o prese di posizione non possano mai essere comunicate al cliente senza una preventiva validazione espressa.

5.3 *Casi d'uso in risorse umane e gestione del personale*

Nell'area delle risorse umane, l'utilizzo di agenti di IA può rivelarsi utile, ma soltanto a condizione che esso venga circoscritto ad attività di carattere organizzativo, informativo e procedurale, evitando ogni impropria sovrapposizione tra supporto operativo e valutazione della persona. In questo ambito, infatti, il valore dell'agente non consiste nel sostituire il giudizio del responsabile HR o del management, bensì nel rendere più ordinata, uniforme e accessibile la gestione delle attività ripetitive e dei flussi informativi interni.

L'agente può, ad esempio, supportare i processi di *onboarding,* guidando il nuovo assunto nel reperimento dei documenti aziendali rilevanti, delle policy applicabili, dei regolamenti interni, dei moduli da compilare e delle attività iniziali da completare entro termini prestabiliti.

Può, inoltre, assistere la funzione HR nella gestione delle richieste ricorrenti provenienti dal personale, fornendo indicazioni sui percorsi autorizzativi, sulle procedure amministrative, sulla fruizione dei corsi obbligatori, sulla raccolta di attestazioni o sulle principali scadenze formative. In tali ipotesi, la funzione dell'agente è quella di facilitare l'accesso corretto e uniforme alle informazioni aziendali, di ridurre il tempo assorbito da richieste standardizzate e di migliorare la tracciabilità dei passaggi interni.

Tuttavia, proprio la delicatezza dei dati trattati e la possibile incidenza sull'organizzazione del lavoro impongono una delimitazione particolarmente rigorosa del perimetro operativo del sistema. Occorre, infatti, evitare che l'agente venga impropriamente impiegato in processi valutativi, selettivi o decisionali suscettibili di produrre effetti diretti sul dipendente, sul suo percorso professionale o sulla sua posizione organizzativa. Per questa ragione, l'impresa deve definire con chiarezza:

1. quali dati del personale siano effettivamente utilizzabili

2. quali categorie di informazioni debbano restare escluse

3. quali attività possano essere delegate all'agente di IA e quali passaggi debbano invece essere necessariamente rimessi a un referente HR o a un responsabile di funzione.

È altresì indispensabile assicurare che il sistema non diffonda informazioni obsolete, istruzioni non aggiornate o contenuti non coerenti con le policy vigenti. In un settore così sensibile, la qualità della base informativa, la responsabilità sui contenuti restituiti e la rigorosa delimitazione dei compiti assegnati all'agente costituiscono condizioni imprescindibili di liceità, affidabilità e difendibilità organizzativa.

5.4 *Casi d'uso in area commerciale, marketing e comunicazione*

Nell'area commerciale, nel marketing e nella comunicazione aziendale, gli agenti di IA possono offrire vantaggi significativi, purché siano collocati con precisione all'interno di attività preparatorie, organizzative e redazionali, senza essere trasformati in una fonte autonoma di messaggi esterni, promesse commerciali o affermazioni rivolte al mercato prive di adeguato presidio umano. In tali ambiti, infatti, l'utilità operativa del sistema è reale, ma altrettanto immediata è la sua potenziale incidenza sul piano reputazionale, regolatorio e contrattuale.

Nell'area commerciale, ad esempio, l'agente può ricevere la richiesta proveniente dal cliente o dalla rete vendita, recuperare i modelli autorizzati, richiamare le condizioni standard applicabili, predisporre una bozza coerente con il perimetro del prodotto o del servizio e trasmetterla internamente al soggetto tenuto alla verifica conclusiva. In questo contesto, il valore dell'agente consiste nell'accelerare il lavoro istruttorio e documentale, non già nel sostituire il presidio commerciale, tecnico o legale sul contenuto finale destinato all'esterno.

Nel marketing e nella comunicazione, il confine da presidiare è ancor più delicato. Qui, infatti, il rischio non è soltanto quello di un'imprecisione operativa interna, ma quello di una comunicazione non conforme, fuorviante, eccessivamente assertiva o incoerente con i vincoli normativi e con il posizionamento aziendale. L'agente può certamente contribuire alla predisposizione di materiali, all'adattamento dei messaggi ai diversi canali, al controllo della coerenza terminologica, al recupero di precedenti già approvati o alla preparazione di varianti redazionali per campagne, comunicazioni istituzionali o contenuti informativi. Tuttavia, quanto più il messaggio si avvicina al cliente, al pubblico o al mercato, tanto meno è ammissibile lasciare al sistema un margine non presidiato nella sua formulazione conclusiva.

In tali contesti, il ruolo dell'agente deve rimanere ancillare e preparatorio, mentre la responsabilità del contenuto finale, della sua correttezza e della sua sostenibilità giuridica e reputazionale deve restare saldamente in capo ai referenti umani competenti.

5.5 *Casi d'uso in tecnologie informatiche e sicurezza*

Nelle funzioni informatiche, e ancor più in quelle deputate alla sicurezza, l'impiego di agenti di intelligenza artificiale può produrre vantaggi operativi di notevole rilievo, ma proprio in tali ambiti emerge con maggiore evidenza la necessità di una disciplina d'uso particolarmente rigorosa. Il beneficio, infatti, è reale soprattutto nelle attività caratterizzate da elevata ripetitività, forte assorbimento di tempo e frequente dispersione informativa: si pensi alla gestione dei ticket di assistenza, alla raccolta ordinata degli elementi tecnici trasmessi dagli utenti, alla ricostruzione preliminare della sequenza degli eventi, al recupero delle procedure interne pertinenti o alla predisposizione di un primo quadro informativo utile al supporto di primo livello. In questo contesto, l'agente può ricevere una segnalazione, classificarla secondo criteri interni, verificare l'eventuale esistenza di precedenti analoghi, richiamare le istruzioni autorizzate e predisporre una traccia iniziale di lavorazione da trasmettere al gruppo tecnico competente. Il suo apporto, dunque, si misura soprattutto nella capacità di ridurre i tempi morti, migliorare l'ordine dei dati disponibili, rendere più lineare il triage iniziale e alleggerire il carico manuale che grava sulle strutture tecniche nelle fasi preliminari di presa in carico.

Il quadro muta, però, in modo significativo quando dall'ordinaria funzione IT ci si sposta sul terreno della sicurezza. In tale ambito, l'agente può certamente risultare utile nella fase iniziale di analisi, ad esempio per aggregare segnalazioni tra loro connesse, evidenziare priorità, leggere in via preliminare i log, ricostruire una prima cronologia tecnica degli eventi o predisporre elementi utili per un successivo approfondimento umano.

Tuttavia, proprio qui si colloca il punto di maggiore delicatezza. L'utilità dell'agente nell'organizzare e rendere intellegibili le informazioni non può essere impropriamente trasformata in un titolo per attribuirgli poteri operativi diretti su ambienti critici. È infatti essenziale distinguere, con assoluta nettezza,

vedi l'articolo online

tra un agente che assiste nell'analisi e nella preparazione del contesto decisionale e un agente che sia invece posto nelle condizioni di intervenire direttamente sull'infrastruttura, mediante l'uso di credenziali privilegiate, la modifica di configurazioni, l'interazione con sistemi di produzione, la gestione degli accessi o l'esecuzione di azioni correttive automatiche.

Questa distinzione non è meramente tecnica, ma investe il nucleo della *governance* del rischio. In materia di sicurezza, infatti, un errore dell'agente non si esaurisce nella produzione di un contenuto inesatto o di una classificazione imperfetta, ma può tradursi in un'alterazione del perimetro operativo, in un blocco improprio di servizi, nell'isolamento ingiustificato di risorse, nell'attivazione di misure tecniche sproporzionate o, al contrario, nell'omesso rilievo di segnali che avrebbero richiesto un'immediata *escalation*. In altri termini, se in altri reparti l'errore dell'agente può spesso essere riassorbito nella normale revisione umana dell'output, nel dominio della sicurezza esso rischia di propagarsi con effetti assai più incisivi, sia sul piano della continuità operativa, sia su quello della protezione dei dati, della resilienza infrastrutturale e della responsabilità interna. Per questa ragione, un agente mal progettato o mal configurato può esso stesso trasformarsi in un vettore di rischio ulteriore: non soltanto per errore funzionale, ma anche per abuso, uso eccedente rispetto al perimetro autorizzato o impropria combinazione di privilegi, fonti informative e capacità di esecuzione.

Ne deriva che, in questo ambito, la corretta disciplina organizzativa deve essere sensibilmente più severa rispetto a quella adottabile in altre funzioni aziendali. L'impresa deve stabilire *ex ante*, in modo puntuale, quali dati tecnici l'agente possa consultare, quali *repository* o strumenti possa interrogare, quali operazioni gli siano radicalmente precluse e quali passaggi debbano rimanere in ogni caso riservati a personale dotato di specifica legittimazione tecnica e organizzativa. Non è sufficiente, dunque, introdurre un generico presidio umano "a valle"; occorre piuttosto costruire un'architettura di contenimento "a monte", nella quale il sistema operi entro ambienti segregati, con permessi graduati, accessi strettamente necessari, registrazioni complete delle attività svolte e costante possibilità di monitoraggio, sospensione, revisione e arresto. In una configurazione matura, l'agente non deve mai trovarsi nella condizione di superare, per via tecnica o funzionale, il perimetro che l'organizzazione gli ha assegnato.

È per tale ragione che, nelle strutture più evolute, l'impiego di agenti di IA in ambito informatico e, soprattutto, nella sicurezza, non viene affidato a logiche di mera efficienza, ma viene subordinato a un sistema formale di segregazione degli ambienti, *workflow* autorizzativi, *logging* robusto, controlli periodici, revisione delle eccezioni e meccanismi chiari di esclusione automatica da determinate attività. Solo entro una simile cornice l'agente può essere valorizzato quale strumento di supporto ad alta utilità operativa, senza che la ricerca di rapidità o di automazione si traduca in una indebita compressione dei presìdi di controllo che, in questo settore, costituiscono parte integrante della sicurezza stessa.

6. Dove si configura un agente di IA?

Una delle prime domande che un'impresa si pone quando si avvicina all'IA agentica è, molto semplicemente, dove l'agente venga effettivamente configurato. Si tratta di una domanda tutt'altro che banale, benché spesso venga data per presupposta o oscurata dal dibattito sulle capacità dell'agente. Nell'esperienza dell'IA generativa tradizionale, infatti, l'azienda tende a muoversi secondo uno schema tecnico e commerciale relativamente semplice: sottoscrive un servizio offerto da un provider e utilizza il modello di IA (ChatGPT, Gemini, Copilot, Claude, etc) per interrogazioni, sintesi, bozze o analisi. In quel contesto, il punto di accesso coincide spesso con l'interfaccia del fornitore e il problema della "configurazione" resta limitato.

Quando, invece, si passa all'agente, questo schema non è più sufficiente. Un agente non coincide con il solo modello linguistico (LLM): per operare concretamente, esso deve essere configurato in un ambiente nel quale riceve istruzioni stabili, viene collegato a fonti informative e documentali e a sistemi aziendali, può utilizzare determinati strumenti, è sottoposto a limiti operativi ed è inserito in un flusso di lavoro definito dall'impresa che lo utilizza.

In altri termini, l'agente non "nasce" dal semplice accesso a un modello, ma prende forma in una piattaforma o in un'applicazione in cui il modello viene organizzato, istruito e governato in funzione di uno specifico processo aziendale.

È proprio questo il punto che molte imprese, soprattutto quando partono da zero, tendono inizialmente a sottovalutare: non basta scegliere il provider del modello, perché il vero tema applicativo è individuare anche il contesto tecnico e organizzativo nel quale l'agente viene costruito e fatto operare. In tale prospettiva, i principali ecosistemi oggi disponibili offrono soluzioni che, pur con architetture differenti, rispondono tutte alla medesima esigenza: affiancare al modello un ambiente di configurazione

agentica. OpenAI, ad esempio, distingue tra configurazioni pronte all'uso, come i GPTs in ChatGPT, e sviluppo più strutturato tramite *Responses API*; Anthropic mette a disposizione API, Agent SDK e collegamenti a strumenti esterni tramite *Model Context Protocol*; Google offre *Vertex AI Agent Builder* e *l'Agent Development Kit;* Microsoft utilizza *Copilot Studio* come ambiente di creazione, test e pubblicazione di agenti connessi a dati e workflow aziendali.

Al di là delle differenze di prodotto, il dato comune è che l'agente non si configura nel solo modello, ma in una *piattaforma agentica* o in un'applicazione della stessa azienda che viene integrata con l'agente e il suo modello, cioè in uno spazio tecnico nel quale vengono definite le sue istruzioni permanenti, le fonti che può consultare, gli strumenti che può usare, i passaggi che può attivare e i limiti entro i quali deve arrestarsi.

Se, dunque, la domanda è "*dove si configura un agente di IA?*", la risposta corretta, in termini aziendali, è che esso si configura sempre in una combinazione di componenti, e non in un unico punto isolato. Per un'impresa che parta da zero, ciò significa comprendere che la configurazione dell'agente richiede almeno cinque elementi essenziali.

Il primo è il *motore di IA*, vale a dire il modello o il servizio messo a disposizione dal fornitore, senza il quale l'agente non sarebbe in grado di comprendere richieste, elaborare informazioni o generare output.

Il secondo è la *piattaforma di configurazione*, cioè l'ambiente nel quale l'agente viene effettivamente istruito, parametrato e governato.

Il terzo è la *base documentale o di conoscenza,* costituita dall'insieme delle fonti informative da cui l'agente attinge per operare in modo coerente con il contesto aziendale.

Il quarto è rappresentato dai *collegamenti ai sistemi dell'impresa*, realizzati mediante API, connettori o protocolli di interoperabilità, che consentono all'agente di interagire con dati, applicativi e strumenti esterni.

Il quinto, infine, è dato *dall'insieme delle componenti di governance,* e dunque da identità digitali, permessi, logging, approvazioni, regole di controllo e meccanismi di supervisione.

In questa prospettiva, la configurazione dell'agente non deve essere intesa come un'operazione meramente tecnica o come un semplice settaggio iniziale del software. Essa coincide, piuttosto, con la costruzione del suo perimetro operativo. Configurare un agente significa decidere dove può lavorare, quali dati può vedere, quali strumenti può utilizzare, quali azioni può compiere, quali passaggi deve sottoporre a validazione umana e in quale ambiente tecnico tali regole vengono effettivamente rese operative. È proprio per questo che la domanda posta dal titolo non è affatto accessoria: per un'impresa che muova i primi passi, essa costituisce la premessa logica e pratica di ogni successiva scelta di adozione.

6.1 *Il motore di IA*

Il motore di IA è, in sostanza, il componente che rende possibile il funzionamento dell'agente. È la parte più vicina all'idea che le imprese già conoscono quando sottoscrivono un servizio presso un fornitore di modelli: una soluzione *enterprise* che consente al sistema di comprendere richieste, elaborare informazioni, leggere contenuti e generare risposte o proposte operative. Senza questo motore, l'agente non sarebbe in grado di svolgere alcuna attività, perché mancherebbe la capacità stessa di "ragionare" sul compito assegnato. Tuttavia, il motore non coincide ancora con l'agente. Esso rappresenta soltanto la componente di base, ossia l'infrastruttura cognitiva del sistema, ma non basta, da solo, a determinare come l'agente debba operare nel contesto aziendale.

Perché si possa parlare veramente di un agente, occorre infatti anche un ambiente di configurazione, vale a dire il luogo tecnico in cui vengono stabilite in concreto le istruzioni permanenti, le procedure da seguire, i limiti operativi, le regole di comportamento e gli eventuali collegamenti con dati, documenti o strumenti esterni. È in questo ambiente che l'impresa traduce il caso d'uso in un assetto operativo effettivo, decidendo che cosa l'agente possa fare, quali fonti possa consultare, quali azioni possa attivare e in quali casi debba invece arrestarsi o rimettere il passaggio a un operatore umano.

Se l'obiettivo dell'impresa è realizzare un assistente interno relativamente semplice, tale ambiente di configurazione può coincidere anche con uno strumento già disponibile all'interno della piattaforma del fornitore, come ad esempio un GPT aziendale configurato in *ChatGPT Enterprise o Business*, corre-

dato da istruzioni, documenti di conoscenza ed eventuali azioni verso servizi esterni.

Se, invece, l'impresa intende sviluppare un agente più strutturato, inserito in processi articolati e connesso in modo più profondo ai sistemi aziendali, allora l'ambiente di configurazione non può più essere una semplice interfaccia conversazionale, ma deve assumere la forma di una piattaforma applicativa dedicata o di un'applicazione aziendale sviluppata sopra le API del fornitore. In questa seconda ipotesi, l'agente non "vive" più in una chat, ma opera all'interno di un'applicazione o di una piattaforma in cui le sue funzioni, i suoi collegamenti e i suoi limiti vengono definiti in modo molto più preciso e governato.

6.2 *L'ambiente di configurazione*

Una volta chiarito che il solo modello non basta a far esistere un agente di IA in senso proprio, il secondo elemento decisivo è la piattaforma agentica, o ambiente di configurazione, nella quale l'agente viene concretamente costruito e governato. È qui, infatti, che il sistema smette di essere una capacità generica del modello e assume una forma operativa coerente con il caso d'uso aziendale.

In tale ambiente si definiscono le istruzioni permanenti, si selezionano le fonti informative utilizzabili, si stabiliscono gli strumenti a cui l'agente può accedere, si regolano i flussi di lavoro che esso può attivare e si fissano i limiti entro i quali il sistema deve restare confinato. In altri termini, la piattaforma è il luogo in cui l'impresa traduce un'esigenza organizzativa in un assetto tecnico effettivo.

Questo punto merita particolare attenzione, perché è proprio qui che molte aziende, quando si avvicinano per la prima volta al tema, tendono a semplificare eccessivamente il problema. Si immagina, infatti, che basti "*usare un modello*" per avere un agente. In realtà, il modello fornisce la capacità di elaborazione, ma la piattaforma ne disciplina il comportamento. È la piattaforma che consente di dire all'agente quali compiti debba svolgere (a proposito: dove si indicano le istruzioni e le regole all'agente, materialmente? Esiste un apposito campo nelle piattaforme agentiche dove l'azienda scrive direttamente regole e procedure), quali documenti possa consultare, quali strumenti possa utilizzare, quali azioni gli siano consentite e in quali casi, invece, debba fermarsi, chiedere conferma o rimettere il passaggio a un operatore umano. Senza questo livello di configurazione, il sistema resta un semplice strumento conversazionale o redazionale; con esso, invece, può diventare una componente organizzata del processo aziendale.

La forma concreta di tale ambiente può variare in funzione della complessità del progetto e del livello di integrazione richiesto. Se l'obiettivo dell'impresa è realizzare un assistente interno relativamente semplice, destinato soprattutto a consultare documenti, restituire sintesi, seguire istruzioni stabili ed eventualmente interagire con pochi servizi esterni, l'ambiente di configurazione può coincidere con una soluzione già disponibile all'interno della piattaforma del fornitore. In questo caso, l'agente può essere configurato mediante strumenti nativi messi a disposizione dal *provider*, con caricamento di documenti, definizione di istruzioni e attivazione di funzioni circoscritte.

Se, al contrario, l'impresa intende sviluppare un agente più articolato, inserito in processi complessi, connesso a più basi dati, capace di interagire con applicativi interni e soggetto a regole di workflow più sofisticate, allora l'ambiente di configurazione non può più ridursi a una semplice interfaccia conversazionale. In tale ipotesi, esso assume piuttosto la forma di una piattaforma applicativa dedicata o di un'applicazione aziendale costruita sopra le API del fornitore.

La differenza tra queste due ipotesi non è di mera scala tecnica, ma di collocazione funzionale dell'agente. Nel primo caso, il sistema opera ancora in una logica relativamente vicina a quella dell'assistente evoluto: utile, configurabile, ma pur sempre concentrato su interazioni abbastanza delimitate. Nel secondo caso, invece, l'agente viene collocato all'interno di una vera architettura applicativa e smette di "vivere" in una semplice chat, perché opera in un ambiente in cui istruzioni, fonti, strumenti, autorizzazioni e workflow sono parte di una progettazione più ampia. È in questa seconda configurazione che l'agente assume, più chiaramente, la natura di componente del processo aziendale e non di semplice interfaccia intelligente.

Sotto questo profilo, la piattaforma non è soltanto un supporto tecnico, ma il punto in cui si rende effettiva la governance dell'agente. È lì che si decide, in modo operativo, quale margine di autonomia attribuirgli, quali dati rendergli accessibili, quali controlli imporre, quali blocchi predisporre e quali passaggi sottoporre a supervisione umana. Proprio per questa ragione, la scelta della piattaforma non può essere compiuta guardando soltanto alla qualità del modello o alla facilità d'uso dell'interfaccia, ma deve essere valutata alla luce del tipo di processo che l'impresa intende affidare all'agente, del grado di integrazione richiesto e del livello di controllo che si reputa necessario garantire.

vedi l'articolo online

6.3 *La base documentale e informativa*

Un agente deve poter consultare documenti selezionati: restando all'esempio di un agente nel comparto di una Compagnia assicurativa, esso deve poter consultare le procedure di gestione dei sinistri, i manuali della Compagnia su come gestire i reclami, i modelli di comunicazione, le FAQ interne, le regole di *escalation* o le tassonomie documentali, solo per restare alle basi documentali e informative principali.

Questa *knowledge base* va preparata, pulita, selezionata e mantenuta aggiornata.

Ma come si fa a far accedere l'agente ai documenti, ai dati e alle informazioni selezionate dall'azienda?

La base documentale da mettere a disposizione dell'agente può – banalmente - essere direttamente caricata sulla piattaforma agentica (soluzione più semplice quando si vuole dare all'agente una base controllata, stabile e selezionata) oppure collegando l'agente ai sistemi aziendali tramite connettori/app/API, così da fargli cercare o recuperare i contenuti direttamente da dove già si trovano (per esempio su *SharePoint*, in un database documentale interno o in altri *repository* o database aziendali). Ma in questo caso, l'agente non recupererà comunque mai in autonomia i documenti: è l'azienda che lo configura a decidere *ex ante* in quali fonti può cercare, con quali permessi, su quale perimetro e, se c'è sincronizzazione, quale contenuto viene indicizzato in anticipo.

Il terzo modello, che in azienda è spesso il più sensato, è ibrido: si carica sulla piattaforma la parte più stabile e normativa dei documenti, cioè quelli che devono essere e sotto controllo, e si collega invece l'agente ai sistemi aziendali per i contenuti che devono essere aggiornati, contestuali o recuperati caso per caso.

6.4 *Il collegamento ai sistemi aziendali*

Il collegamento ai sistemi aziendali rappresenta uno dei passaggi più delicati, e spesso anche uno dei meno compresi, quando un'impresa intende introdurre un agente di intelligenza artificiale in un processo reale. Finché il sistema si limita a generare testi, sintesi o proposte sulla base di documenti caricati manualmente, il suo impiego può restare confinato in un ambiente relativamente separato dall'operatività ordinaria. Ma quando l'agente deve realmente concorrere allo svolgimento di un'attività aziendale, non è più sufficiente che sia in grado di leggere un documento o formulare una risposta plausibile: occorre che possa interagire, entro limiti rigorosamente definiti, con i dati, gli stati di avanzamento e le informazioni di contesto custoditi nei sistemi dell'impresa.

In termini concreti, ciò significa che l'agente, per essere davvero utile, deve poter accedere almeno ad alcune informazioni strutturate indispensabili al processo in cui è inserito. Se, ad esempio, l'agente opera nel contesto di una pratica assicurativa, non basta che analizzi una denuncia o riassuma un reclamo: deve anche poter verificare, nei limiti del perimetro autorizzato, se esista un fascicolo già aperto, quali allegati risultino presenti, quale sia lo stato della pratica, chi sia il referente assegnato, quali passaggi siano già stati compiuti e quale regola procedurale si applichi a quello specifico caso. In assenza di tale collegamento, il sistema resta un supporto esterno, magari utile sul piano redazionale o informativo, ma non ancora integrato nel processo aziendale in senso proprio.

È proprio per questo che il collegamento ai sistemi interni dell'impresa costituisce il punto in cui l'agente cessa di essere una semplice interfaccia intelligente e diventa una componente operativa, sia pure entro confini prestabiliti, del flusso di lavoro dell'impresa. Tale collegamento avviene normalmente mediante API, connettori applicativi o altre forme di integrazione predisposte dal fornitore, dal *system integrator* o dai responsabili dei sistemi gestionali interni. Non si tratta, però, di una questione esclusivamente tecnica. Ogni integrazione implica una scelta preventiva sul piano organizzativo e giuridico: bisogna stabilire quali sistemi possano essere interrogati, quali dati possano essere resi accessibili, con quale livello di dettaglio, per quali sole finalità e con quali limiti di utilizzo. Collegare un agente a un sistema aziendale non significa, dunque, "aprire" indiscriminatamente i database o i gestionali dell'impresa, ma costruire un canale di interazione selettivo, proporzionato e governato.

Sotto questo profilo, il tema centrale non è tanto la possibilità astratta di integrazione, quanto la sua corretta delimitazione. L'impresa deve infatti evitare che l'agente disponga di un accesso eccedente rispetto al compito che gli è stato attribuito, o che possa combinare informazioni provenienti da fonti e sistemi diversi in modo non coerente con il mandato operativo ricevuto. Quanto più l'agente è integrato nei sistemi aziendali, tanto più diventa necessario definire in modo puntuale quali informazioni possa leggere, quali azioni possa attivare, quali dati debbano restare esclusi e quali passaggi debbano comunque essere subordinati a verifica o approvazione umana. Il problema, in altri termini, non è sol-

tanto far dialogare il modello con i sistemi dell'impresa, ma farlo dialogare secondo regole che siano tecnicamente sicure, organizzativamente sostenibili e giuridicamente difendibili.

Per questa ragione, il collegamento ai sistemi aziendali deve essere sempre concepito come parte integrante della *governance* dell'agente. L'utilità operativa dell'integrazione è indubbia, perché consente al sistema di lavorare su dati aggiornati, di inserirsi nel flusso reale delle attività e di evitare duplicazioni o passaggi manuali inutili. Tuttavia, proprio questa utilità aumenta il rischio che l'agente venga impropriamente trasformato in un operatore occulto del processo, dotato di una capacità di intervento non pienamente percepita dall'organizzazione. Ne consegue che ogni integrazione deve essere progettata secondo il principio di necessità: solo i dati strettamente pertinenti, solo gli strumenti effettivamente indispensabili, solo i collegamenti ai sistemi aziendali coerenti con il caso d'uso approvato.

In mancanza di tale disciplina, l'agente rischia di diventare non un fattore di efficienza governata, ma un punto di opacità tecnica e di vulnerabilità organizzativa.

6.5 *La governance e il controllo aziendale*

La *governance* e il controllo aziendale costituiscono il presidio essenziale che consente all'impresa di utilizzare un agente di intelligenza artificiale senza smarrire il dominio del processo nel quale esso è inserito. Quando l'agente non si limita a generare contenuti, ma accede a informazioni, consulta fonti, interagisce con strumenti, attiva passaggi procedurali o orienta segmenti dell'operatività aziendale, il problema centrale non è più soltanto quello della qualità dell'output, bensì quello della sua collocazione entro un assetto di regole, poteri, limiti e verifiche chiaramente definiti. In questa prospettiva, la governance non rappresenta un elemento accessorio o successivo rispetto alla configurazione tecnica dell'agente, ma coincide con la cornice organizzativa e giuridica che ne rende legittimo, controllabile e sostenibile l'impiego.

In termini concreti, governare un agente significa anzitutto stabilire chi possa utilizzarlo, in quale contesto, per quali finalità e con quali autorizzazioni. Occorre decidere quali utenti possano accedervi, quali privilegi l'agente possa esercitare nei sistemi aziendali, quali basi documentali possa interrogare, quali strumenti possa utilizzare e quali azioni gli siano consentite o radicalmente precluse. A ciò si aggiunge la necessità di definire i casi in cui il sistema possa procedere autonomamente entro limiti predeterminati e quelli in cui, invece, debba arrestarsi, segnalare l'anomalia o rimettere il passaggio a un soggetto umano dotato del necessario potere di valutazione e approvazione.

Ogni attività rilevante svolta dall'agente deve poi essere adeguatamente tracciata. L'impresa deve poter ricostruire quali dati siano stati consultati, quali istruzioni siano state applicate, quali fonti siano state utilizzate, quali azioni siano state proposte o compiute e quali soggetti abbiano eventualmente validato o corretto il risultato. Senza un sistema effettivo di registrazione e verificabilità, l'impiego dell'agente rischia infatti di generare zone di opacità incompatibili con le esigenze di accountability, audit e difendibilità del processo. La tracciabilità non serve soltanto a controllare *ex post* il comportamento del sistema, ma anche a rendere possibile il riesame degli errori, la correzione delle regole e la verifica della coerenza tra il funzionamento effettivo dell'agente e il mandato operativo che gli è stato attribuito.

Sotto il profilo organizzativo, la *governance* implica poi una chiara distribuzione delle responsabilità interne. Ad esempio, su questo piano, l'impresa dovrebbe indentificare per lo meno:

1. il soggetto o la funzione che richiede l'impiego dell'agente
2. quello che ne presidia il profilo tecnico
3. quello che ne valuta la compatibilità giuridica e regolatoria
4. quello che, sul piano operativo, approva o respinge i passaggi più sensibili.

L'introduzione dell'agente non può, infatti, tradursi in una diluizione indistinta delle responsabilità. Al contrario, quanto più il sistema partecipa al flusso operativo, tanto più diventa necessario rendere trasparente chi abbia deciso la sua adozione, chi ne abbia definito i limiti, chi ne sorvegli il funzionamento e chi sia chiamato a intervenire quando il sistema esca dal perimetro assegnato o produca risultati non coerenti con le regole dell'organizzazione.

7. Configurare un agente di IA step by step: il caso pratico dell'agente per l'istruttoria preliminare di sinistri e reclami nel comparto assicurativo

Immaginiamo una compagnia che voglia introdurre un agente interno per il preliminare trattamento dell'istruttoria su un sinistro o per la gestione iniziale di un reclamo assicurativo ricevuto. L'agente non deve liquidare, non deve rigettare, non deve formulare una decisione finale verso il cliente. Deve invece svolgere una funzione istruttoria e organizzativa: ricevere la pratica, verificare quali documenti sono arrivati, leggere la denuncia, ordinare gli allegati, individuare eventuali mancanze, segnalare anomalie evidenti, recuperare da basi interne le regole procedurali applicabili e preparare una scheda di sintesi per il liquidatore o per il gestore del reclamo. La prima attività, quindi, è definire il perimetro esatto dell'obiettivo: che cosa l'agente deve fare, che cosa non deve fare mai, e in quale punto del processo si deve fermare. È da questa delimitazione iniziale che dipendono l'architettura agentica, il perimetro necessario dei dati, i permessi, i controlli e la definizione delle responsabilità.

7.1 *Primo passo operativo: mappare il processo reale prima della tecnologia*

Prima di configurare qualunque componente tecnica, l'azienda deve partire considerando come oggi, senza tecnologia e con gli esseri umani, gestisce i processi reali. Occorre quindi mappare: quale addetto o ufficio riceve la domanda di liquidazione o le comunicazioni sul sinistro o il reclamo; a quale recapito/ufficio arrivano i documenti; chi verifica la completezza del fascicolo; quali sistemi vengono consultati; dove si generano ritardi; quali controlli sono già previsti e in quali passaggi il personale perde più tempo in attività ripetitive.

Solo dopo questa fotografia del processo è possibile individuare il segmento da affidare all'agente. Se questa mappa non esiste, l'agente non si inserisce in un processo, ma crea un processo parallelo e opaco. E in ambito assicurativo questo errore è particolarmente grave, perché la gestione del fascicolo e la ricostruzione del percorso interno sono decisive anche sul piano difensivo e probatorio.

7.2 *Secondo passo: definire il mandato operativo dell'agente con regole positive e negative*

Una volta mappato il processo per come l'azienda lo gestisce abitualmente con addetti e procedure, bisogna tradurre il caso d'uso in un vero e proprio mandato operativo all'agente. Questo mandato deve essere scritto in forma quasi procedurale. Per esempio: l'agente:

1. può leggere la denuncia di sinistro
2. classificare il tipo di pratica
3. verificare la presenza di allegati obbligatori
4. recuperare dal repertorio interno le istruzioni relative a quella tipologia
5. costruire una sintesi e
6. aprire una richiesta di integrazione documentale interna o verso il canale autorizzato.

Parallelamente, bisogna definire anche le regole negative, cioè ciò che l'agente non può fare: non può promettere un esito al cliente, non può formulare una decisione di copertura, non può valutare da solo la fondatezza economica del danno, non può superare una certa soglia di autonomia, non può inviare comunicazioni esterne non approvate. Questa fase è tecnica e organizzativa insieme: serve per impostare prompt di sistema, regole di orchestrazione, limiti dei tool e criteri di blocco. In sostanza, è in questa fase che si decide se l'agente sarà davvero un ausilio governato o una fonte di rischio.

7.3 *Terzo passo: disegnare l'architettura tecnica minima dell'agente*

A questo punto si passa all'architettura. In una configurazione prudente e realistica, l'agente assicurativo non è un unico blocco indistinto, ma una catena di componenti. Serve anzitutto un canale di ingresso, cioè il punto in cui l'agente riceve la pratica: ad esempio, l'azienda può utilizzare – se esiste – il portale sinistri, oppure una casella strutturata o l'area reclami.

Serve poi un *motore di orchestrazione*, che governa i passaggi e decide quale azione di volta in volta l'agente può compiere per ciascuna fase operativa. In questo motore di orchestrazione sono inclusi: un *modello linguistico* che legge riassume e classifica, etc; una *base documentale controllata* predisposta dall'azienda da cui recuperare istruzioni interne, check-list, tassonomie di sinistro e regole procedurali; i *connettori verso i sistemi aziendali autorizzati*; un *registro delle attività*; la cosiddetta *coda di ap-*

provazione umana e un'area di amministrazione per effettuare il *monitoraggio dell'operatività dell'agente* (può essere, per esempio, un normale pannello di controllo o una *dashboard*).

La regola progettuale corretta è che il modello non operi mai da solo: deve essere sempre inserito in una architettura che ne delimiti fonti, strumenti, azioni e tracciabilità.

Una parte importante dell'architettura può essere trovata o configurata sulla piattaforma agentica del fornitore. Le piattaforme più complete oggi offrono di norma il modello, gli strumenti di orchestrazione (detti *agent building*) e offrono servizi di governance documentale, i connettori ai sistemi aziendali e gli strumenti per collegarsi a servizi esterni, nonché le necessarie funzioni di monitoraggio. Il contesto aziendale in cui l'agente deve lavorare – e che deve essere ovviamente la parte dell'architettura dell'agente – sono tuttavia elementi architetturali di pertinenza dell'azienda che lo sta configurando. In termini più chiari: per esempio, il canale di ingresso viene messo a disposizione dalla compagnia (es: un portale sinistri, una casella strutturata, un workflow reclami o un documentale: l'agente va collegato a tali canali).

Tuttavia, se invece non esiste nulla, si può anche acquistare anche tale front-end. Allo stesso modo, i connettori verso i sistemi aziendali richiedono comunque che i sistemi della compagnia siano collegabili, abbiano API o connettori disponibili, e siano governati nei permessi.

7.4 *Quarto passo: preparare i dati e costruire la base documentale dell'agente*

Il punto più sottovalutato, e spesso il più decisivo, riguarda i dati. L'agente non deve essere collegato indiscriminatamente a tutto il patrimonio informativo della compagnia. Occorre prima costruire una base documentale pulita, selezionata e governata, composta solo dai contenuti realmente necessari: procedure sinistri, manuali reclami, modelli di richiesta integrazione, tassonomie documentali, istruzioni operative, FAQ interne, repertori di codici evento, regole di *escalation*.

Tale base va poi normalizzata, nel senso che vanno eliminati i documenti duplicati (il cosiddetto processo di deduplicazione); va attribuita una versione a ciascun documento (è il cosiddetto *versioning* documentale) e va indicata una classificazione per livelli di riservatezza.

Successivamente, bisogna decidere quali dati di pratica l'agente possa vedere: anagrafica minima, numero sinistro, tipo evento, stato fascicolo, allegati presenti, ma non necessariamente ogni informazione disponibile nei sistemi (es: i certificati medici).

È poi essenziale anche decidere se i dati servano solo per la singola sessione (gestione di *quel* sinistro o risposta a *quel* reclamo) o se debbano – al contrario - alimentare in via generale una memoria dell'agente per categoria e che a quel punto diventa una memoria più persistente.

Da questa scelta discendono rilevanti cambiamenti pratici in ordine alla gestione del rischio, ai controlli necessari, ai tempi di conservazione e alle garanzie da pretendere dal fornitore.

7.5 *Quinto passo: configurare strumenti, permessi e confini di azione*

Una volta definita la base informativa autorizzata, si configurano gli strumenti aziendali che l'agente può utilizzare. In una compagnia assicurativa prudente, l'agente non riceve subito accesso pieno ai gestionali. Gli si attribuiscono invece permessi minimi e progressivi. Per esempio, in una prima fase lo si può autorizzare a leggere i metadati della pratica, a verificare la presenza o meno di allegati, a consultare il repertorio interno delle procedure e a scrivere una bozza di scheda istruttoria.

In una fase più avanzata, ma sempre controllata, lo si può autorizzare ad aprire una richiesta di integrazione, oppure a cambiare lo stato del flusso in un perimetro definito o ad inserire un *alert* per il referente umano.

L'agente, in ogni caso, non dovrebbe, invece, poter alterare da solo dati sensibili, chiudere il fascicolo, assumere decisioni economiche o utilizzare credenziali ad alto privilegio.

Ma dove si configurano strumenti e permessi? Materialmente, una parte si configura proprio sulla piattaforma agentica che in precedenza si è citata, mentre un'altra parte della configurazione avviene direttamente sui sistemi della compagnia.

7.6 *Sesto passo: impostare i controlli, i guardrail e la supervisione umana*

A questo punto del progetto, la compagnia deve decidere le regole di una fase che può essere delicata: in quali casi l'agente può andare avanti da solo e in quali casi, invece, deve fermarsi e chiedere l'intervento di una persona.

E' il tema dei cosiddetti *guardrail*, le regole negative. In parole semplici, i *guardrail* sono regole di sicurezza che impediscono all'agente di uscire da un perimetro/percorso assegnato. Per esempio, si può stabilire che l'agente lavori solo su documenti appartenenti a certe cartelle o a certe tipologie di pratica; oppure che possa preparare una scheda istruttoria interna ma non inviare mai una risposta definitiva al cliente. Ancora, si può stabilire che l'agente si debba bloccare se mancano allegati essenziali o che non possa andare oltre se la pratica supera una certa soglia economica o presenta elementi di particolare complessità. Infine, sempre per stare agi esempi di *guardrail*, si può stabilire che l'agente debba segnalare subito il caso a un operatore quando trova incongruenze tra i documenti, dati incompleti o anomalie rilevanti.

Dal punto di vista pratico, queste regole si mettono a terra in tre modi.

Il primo è nelle *istruzioni dell'agente*, dove si scrive chiaramente che cosa può fare e che cosa non può fare.

Il secondo è nei *permessi dei sistemi collegati*, perché anche se l'agente volesse fare di più, il sistema non glielo deve consentire tecnicamente (non connettendo a questo o a quel sistema/archivio, etc).

Il terzo è nel workflow operativo, cioè nella sequenza dei passaggi del processo, dove si stabilisce che certi casi non possano andare avanti senza un controllo umano.

Accanto ai *guardrail*, bisogna poi costruire una reale *supervisione umana*: l'azienda deve decidere chi guarda il lavoro dell'agente, quando lo guarda e che cosa può fare se trova un problema.

La supervisione – che abbiamo definito *reale* – è tale solo se c'è una persona individuata, con un compito chiaro e con il potere effettivo di intervenire. Entra qui in gioco il concetto di «*coda da validare*»: una cartella di lavoro o lista di pratiche in attesa di controllo umano. In pratica, l'agente lavora sulla pratica, ma quando incontra un caso che non può chiudere da solo, oppure quando produce un output che deve essere controllato, deposita il risultato in questa coda. A quel punto un operatore umano apre la coda, vede le pratiche da controllare e decide che cosa fare.

La coda serve quindi a evitare che il lavoro dell'agente si perda o proceda automaticamente senza controllo. È, in sostanza, il punto di raccordo tra automazione e responsabilità umana. La coda funziona con tre esiti semplici: approvato: il lavoro dell'agente va bene e il processo può proseguire. Il secondo è corretto: l'operatore sistema o integra il lavoro dell'agente e poi rimette in carreggiata la pratica. Il terzo è respinto.

7.7 *Settimo passo: testare il sistema come se fosse già in esercizio*

Prima della messa in produzione, l'agente va provato su casi reali o realistici, ma in ambiente controllato. Non basta verificare che funzioni, occorre testare se si comporta bene quando la pratica è incompleta, quando i documenti sono disordinati, quando arrivano allegati incoerenti, quando il linguaggio del cliente è ambiguo, quando il sinistro presenta elementi di escalation o quando i dati nei sistemi interni non coincidono perfettamente.

Occorre quindi costruire una *batteria di casi di prova*: casi standard, casi incompleti, casi borderline, casi con documenti non leggibili, casi con informazioni tra loro contraddittorie.

Per ciascun caso l'azienda misurerà: precisione classificatoria, correttezza della check-list, qualità della sintesi, corretto uso degli strumenti, rispetto dei limiti e adeguatezza delle *escalation* previste.

7.8 *Ottavo passo: avviare il pilota in esercizio controllato*

Se il collaudo è soddisfacente, non si passa subito a una piena automazione. Si apre invece una fase pilota con un perimetro ristretto. Per esempio, si può scegliere una sola linea di sinistri, una sola tipologia documentale o una sola unità organizzativa.

In questa fase l'agente lavora in parallelo con il personale umano: prepara la scheda, segnala le mancanze, propone il passaggio successivo, ma ogni risultato viene confrontato con l'operatività umana. E' difatti necessario in questa fase osservare dove il sistema si comporta in modo inatteso, dove tende a

semplificare troppo, dove genera falsi allarmi o dove, al contrario, non vede criticità evidenti.

La fase pilota serve proprio capire se il processo assicurativo regge davvero l'inserimento dell'agente senza perdere qualità, difendibilità e controllo.

7.9 *Nono passo: passare dalla prova pratica alla messa in esercizio stabile*

L'ultima fase è quella che determina il successo o il fallimento dell'intero progetto. Se il pilota ha dato risultati buoni, l'azienda deve *formalizzare* la messa in esercizio dell'agente: definire il proprietario del processo, il responsabile tecnico, i referenti di business, i livelli di servizio, le regole di aggiornamento della base documentale, i controlli periodici, la gestione degli incidenti, i meccanismi di disattivazione e le condizioni di estensione ad altri rami o ad altre fasi del ciclo assicurativo.

Va anche chiarito come trattare i cambiamenti del modello, l'aggiornamento degli strumenti o delle procedure interne, perché un agente che funziona oggi può diventare inaffidabile domani se mutano le fonti o le regole.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it