DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La contrattualizzazione dell'IA in banche e assicurazioni

Perché l'acquisto e disciplina dell'IA non è un normale contratto software

Luglio 2026

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Studio Legale Tributario Associato

DLA Piper

DLA PIPER

1. Introduzione

Per banche, intermediari finanziari e assicurazioni l'intelligenza artificiale, oltre che un tema di innovazione, è anche una componente dell'architettura operativa: entra nella relazione con il cliente, nei controlli antifrode, nell'analisi dei reclami, nella gestione dei sinistri, nel credit scoring, nella cybersecurity, nel supporto alle funzioni interne e, in alcuni casi, nella continuità di processi critici o importanti.

Questo cambia il modo in cui un sistema di AI deve essere acquistato e disciplinato contrattualmente. Non è sufficiente partire da un contratto software o SaaS e aggiungere qualche clausola su privacy, proprietà intellettuale e sicurezza. Nei progetti AI il contratto diventa uno strumento di governance: deve trasformare obblighi regolatori, presidi operativi e allocazione del rischio in impegni verificabili del fornitore.

Il punto è particolarmente rilevante per gli operatori regolati. AI Act, GDPR, DORA, regole su outsourcing e ICT third-party risk, Data Act, NIS2, Cyber Resilience Act, Cybersecurity Act e nuova disciplina sulla responsabilità da prodotto non operano in compartimenti separati. Nella pratica convergono sullo stesso oggetto: una soluzione che utilizza dati, modelli, infrastrutture cloud, API, componenti software, subfornitori e processi umani per generare output che possono incidere su clienti, controlli interni o decisioni aziendali.

2. L'uso previsto è la prima clausola di rischio

La prima clausola davvero critica è la descrizione dell'uso previsto.

Nel software tradizionale la descrizione del servizio tende spesso a coincidere con funzionalità, ambienti, livelli di servizio e supporto. Nell'AI, invece, l'intended purpose è il punto di partenza regolatorio e contrattuale. Serve a capire se il sistema possa essere high-risk ai sensi dell'AI Act, se intervenga in processi decisionali, se supporti funzioni critiche o importanti ai fini DORA, se sia parte di un'esternalizzazione e quali dati utilizzi.

Una descrizione generica del tipo "piattaforma di AI per l'efficientamento dei processi assicurativi" non è sufficiente. Occorre sapere se il sistema assiste il liquidatore, suggerisce l'esito del sinistro, valuta

vedi l'articolo online

indicatori di frode, produce comunicazioni al cliente o incide sul pricing. Allo stesso modo, una soluzione utilizzata per prioritizzare alert antiriciclaggio pone rischi diversi da una soluzione che determina automaticamente il blocco di un'operazione.

Il contratto dovrebbe indicare finalità ammesse e vietate, categorie di utenti e di dati, processi interessati, grado di autonomia del sistema, ruolo dell'output e ipotesi di escalation umana. In una negoziazione, è ragionevole che il cliente regolato chieda che l'estensione dell'uso a nuovi processi, nuove categorie di dati o nuove decisioni rilevanti passi per una valutazione preventiva e un'approvazione scritta. Il fornitore tenderà invece a difendere una maggiore flessibilità evolutiva del prodotto, proponendo notifiche e release note. Il punto di equilibrio è distinguere tra aggiornamenti ordinari e modifiche che cambiano il profilo di rischio, la classificazione regolatoria o il ruolo dell'output.

3. Ruoli AI Act e responsabilità operative

L'AI Act distingue tra provider, deployer e altri soggetti della catena del valore. Nel contratto, però, questa distinzione deve diventare operativa.

Il fornitore può essere provider del sistema AI, rivenditore, integratore, sviluppatore del modello o una combinazione di più ruoli. Il cliente regolato, a sua volta, può essere deployer, titolare del trattamento, committente di un'esternalizzazione e, in certi casi, soggetto che modifica il sistema in modo rilevante.

Per questo non basta una clausola in cui il fornitore dichiara genericamente che la soluzione è "AI Act compliant". Occorre stabilire quali obblighi restano in capo al provider, quali informazioni devono essere fornite al deployer, quali istruzioni d'uso sono vincolanti, quali log sono generati, quali documenti tecnici sono disponibili, quali eventi devono essere comunicati e quale monitoraggio post-deployment è previsto.

Quando la soluzione consente configurazioni, prompt di sistema, policy di guardrail o collegamenti a knowledge base interne, questo perimetro va scritto con precisione: il fornitore potrà limitare la propria responsabilità se il cliente modifica il sistema fuori dalle istruzioni contrattualizzate; il cliente, però, deve conservare spazio sufficiente per adeguare il sistema a policy interne, controlli e requisiti regolatori.

4. Dati: il punto in cui molti contratti AI diventano fragili

La disciplina dei dati è spesso il punto in cui i contratti AI mostrano la loro debolezza. Servono regole diverse per dati personali, dati non personali, dati sintetici e derivati, prompt, log, output, dataset di training e dati utilizzati per fine-tuning. Una clausola unica sulla "titolarità dei dati" non basta.

Sul piano GDPR occorre qualificare i ruoli privacy e disciplinare istruzioni, sub-responsabili, misure tecniche e organizzative, trasferimenti, data breach e audit. Ma nei progetti AI il problema va oltre. Occorre stabilire se il fornitore possa utilizzare prompt, output, log o feedback per addestrare o migliorare modelli propri o di terzi; se possa farlo in forma aggregata o anonimizzata; come siano gestiti segreti commerciali, dati bancari e assicurativi, know-how e informazioni riservate.

La posizione naturale di una banca o assicurazione è chiedere che dati del cliente, dati dei clienti finali, prompt, output, log e feedback non siano utilizzati per training generalizzato o a beneficio di altri clienti, salvo autorizzazione espressa, specifica e revocabile. Il fornitore tenderà a preservare almeno l'uso di telemetrie, dati aggregati e informazioni tecniche per sicurezza, debugging, prevenzione degli abusi e miglioramento del servizio. Una soluzione sostenibile distingue tra utilizzo necessario per erogare e proteggere il servizio reso al cliente e utilizzo per addestramento, riaddestramento o miglioramento di modelli generali.

Il Data Act aggiunge un ulteriore livello, soprattutto quando l'AI si alimenta con dati generati da prodotti connessi e infrastrutture IoT, flotte, sensori o sistemi industriali. In questi casi accesso, uso, condivisione, portabilità, switching, interoperabilità e tutela dei segreti commerciali possono incidere direttamente sull'architettura contrattuale. Per una compagnia assicurativa che utilizzi dati telematici per pricing, prevenzione del rischio o gestione sinistri, il punto non sarà solo chi può trattare il dato personale, ma chi può accedere ai dati generati, con quali limiti, per quali finalità e con quale possibilità di migrare verso un diverso fornitore.

5. Output, errori e responsabilità: il disclaimer non basta

Molti contratti AI contengono disclaimer secondo cui l'output può essere inesatto e deve essere verificato dall'utente. È una clausola comprensibile, ma spesso insufficiente per un operatore regolato.

vedi l'articolo online

È vero che un sistema AI può generare errori, bias o output non spiegabili in modo pienamente lineare. Proprio per questo il contratto deve definire presidi di performance, test, benchmark, soglie di errore, limiti d'uso, remediation, escalation e sospensione. Se il sistema supporta valutazioni di merito creditizio, antifrode, pricing, reclami o assistenza clienti, il fornitore non può limitarsi a dire che l'output è fornito "as is".

La questione contrattuale è quindi quali presidi il fornitore possa garantire affinché il cliente sia in grado di utilizzare il sistema in modo governabile: metriche, tracciabilità, monitoraggio di drift e bias, notifica di degrado, supporto investigativo e correzione.

In un contratto con una banca o un'assicurazione, è ragionevole prevedere che il fornitore mantenga evidenze documentate dei test effettuati rispetto alle finalità concordate e comunichi degradi significativi, vulnerabilità o anomalie ricorrenti. Il fornitore, dal canto suo, vorrà evitare garanzie di risultato e responsabilità per decisioni assunte dal cliente sulla base dell'output. La clausola dovrebbe quindi spostare il baricentro dalla correttezza del singolo risultato alla qualità dei presidi, alla trasparenza sulle limitazioni, alla cooperazione e alla tempestiva remediation.

6. Human oversight effettivo, non dichiarato

La sorveglianza umana è spesso trattata come formula di stile. Nei processi regolati non può esserlo.

Scrivere che "la decisione finale resta sempre all'utente" non basta se l'utente non dispone di informazioni, tempo, competenza e strumenti per contestare l'output. Un human-in-the-loop puramente formale può addirittura creare un falso senso di controllo.

Nei contratti AI occorre quindi disciplinare cosa il fornitore mette a disposizione affinché il controllo umano sia effettivo: spiegazioni operative, confidence score, alert, log, interfacce, possibilità di override e informazioni sui limiti del sistema. Non si tratta necessariamente di ottenere accesso al codice sorgente o ai "pesi" del modello. Si tratta di avere una spiegabilità sufficiente per l'uso regolato e per la difesa della decisione.

Se per esempio un assistente AI suggerisce di respingere un sinistro o di classificare un alert come falso positivo, il presidio umano non può limitarsi a un click di conferma. Il contratto dovrebbe imporre al fornitore di rendere disponibili elementi sufficienti per comprendere la raccomandazione, mentre il fornitore potrà ragionevolmente escludere la consegna dei "pesi" del modello.

7. Cybersecurity e AI supply chain

L'AI amplia la superficie di attacco. Alle vulnerabilità software tradizionali se ne aggiungono molte altre: prompt injection, data poisoning, abuso di API, manipolazione di sistemi di retrieval-augmented generation e leakage di informazioni riservate.

Per gli operatori finanziari la sicurezza del sistema AI deve essere letta insieme a DORA, NIS2, Cyber Resilience Act e disciplina sulla supply chain ICT. Se il sistema AI è erogato come servizio ICT a supporto di funzioni critiche o importanti, le clausole su sicurezza, incidenti, audit, subfornitura, business continuity ed exit assumono rilievo regolatorio diretto.

Il Cyber Resilience Act può essere rilevante quando l'AI è incorporata in prodotti con elementi digitali o componenti software distribuiti. Anche quando non si applichi direttamente alla specifica fornitura, i suoi principi possono diventare benchmark contrattuale per la cosiddetta "secure-by-design", gestione delle vulnerabilità, aggiornamenti di sicurezza e documentazione dei componenti.

Una clausola efficace dovrebbe imporre al fornitore un programma documentato di AI security e vulnerability management, con test specifici contro le minacce proprie dei sistemi AI, notifica tempestiva di vulnerabilità critiche e cooperazione in caso di incidente. Il fornitore cercherà di allineare questi obblighi ai propri processi standard e di limitare la trasparenza su dettagli tecnici sensibili. Il cliente regolato, però, ha bisogno di informazioni tempestive e utilizzabili per adempiere ai propri obblighi di incident reporting, valutare l'impatto sui processi e attivare misure di contenimento.

8. Concentration risk: il modello può sparire

Uno dei rischi più sottovalutati è la dipendenza dal modello sottostante.

Il caso Anthropic Fable 5 e Mythos 5 lo mostra con chiarezza. Nel giugno 2026, a seguito di una direttiva statunitense, Anthropic ha dichiarato di dover disabilitare l'accesso ai modelli per tutti i propri clienti.

Successivamente, Legion, una LegalTech americana, ha poi avviato un contenzioso contro il governo sostenendo che la perdita di accesso al modello aveva inciso in modo immediato sulla propria operatività.

Per banche e assicurazioni, questa può essere una lezione contrattuale. Se un processo dipende da un modello, da una API, da un cloud provider, ma anche da una regione, l'indisponibilità può derivare non solo da outage tecnici, ma anche da export control, sanzioni, restrizioni regolatorie, aumento dei prezzi o modifica delle policy d'uso da parte del fornitore.

DORA già impone agli operatori finanziari di considerare il rischio di concentrazione e la sostituibilità dei fornitori ICT. L'AI rende questo tema ancora più concreto. Non basta sapere chi eroga il servizio applicativo; occorre sapere quali modelli, infrastrutture, subfornitori e componenti lo rendono possibile.

Per questo il contratto dovrebbe imporre al fornitore di comunicare modelli, cloud provider, API e subfornitori rilevanti utilizzati per l'erogazione del servizio AI, nonché ogni modifica che possa incidere su disponibilità, performance, sicurezza, localizzazione, compliance o sostituibilità. La banca o l'assicurazione chiederà un piano di continuità, un modello alternativo, assistenza alla migrazione e conservazione di log, configurazioni, dati e documentazione. Il fornitore tenderà a qualificare restrizioni governative o indisponibilità di subfornitori come eventi fuori dal proprio controllo. La posizione ragionevole non è imporre una responsabilità assoluta per eventi esogeni, ma prevedere obblighi robusti di trasparenza, continuità, sostituibilità, cooperazione ed exit assistita.

9. Subfornitura, change management e audit

Molti sistemi AI sono costruiti su catene complesse: model e cloud provider, data provider, integratori, API esterne e fornitori di cybersecurity. Il cliente vede un'interfaccia unica, ma il rischio è distribuito su più livelli.

Per soggetti sottoposti a DORA e regole di outsourcing, la subfornitura non può, in questi casi, essere disciplinata con una generica autorizzazione. Servono mappatura, diritto di informazione, criteri di approvazione o opposizione, obblighi flow-down, localizzazione, audit, continuità, exit e controllo sulle modifiche significative.

È prevedibile che il fornitore chieda flessibilità operativa, soprattutto se utilizza infrastrutture standardizzate. La soluzione non è paralizzare la catena tecnica, ma distinguere tra subfornitori significativi per il servizio AI regolato e subfornitori generali. Per i primi, il cliente dovrebbe avere informazione e autorizzazione preventiva e garanzie di equivalenza degli obblighi; per i secondi può essere sufficiente una maggiore standardizzazione.

Anche il change management richiede una disciplina specifica. Un modello AI può essere aggiornato, riaddestrato o riconfigurato. Le performance possono variare nel tempo. Le policy del provider possono evolvere. Non ogni modifica richiede approvazione formale, ma le modifiche materiali devono essere identificate, testate e comunicate. Per sistemi usati in processi critici, il cliente dovrebbe poter chiedere test pre-release, roll-back, processi di parallel-running o sospensione dell'aggiornamento.

In un settore regolato, è poi importante verificare se l'ente sarà in grado di spiegare e documentare come il sistema è stato scelto, configurato, monitorato e corretto. Le clausole di audit non devono limitarsi al diritto di accesso ai locali (spesso poi solo teorica) o alla disponibilità di certificazioni. Devono coprire documentazione tecnica, istruzioni d'uso, test, report di sicurezza, change history, evidenze di monitoring, e supporto in caso di richiesta dell'autorità. Il fornitore potrà legittimamente proteggere IP, segreti industriali e sicurezza del proprio ambiente, ma ciò non può svuotare il diritto del cliente regolato di ottenere le informazioni necessarie per adempiere ai propri obblighi.

10. Proprietà intellettuale ed exit

La proprietà intellettuale nei contratti AI non riguarda solo chi possiede l'output. Occorre disciplinare diritti sul modello preesistente, personalizzazioni, dati e materiali del cliente, output e miglioramenti generati durante il rapporto.

Nei casi di fine-tuning o sviluppo dedicato, è essenziale chiarire se il modello risultante sia riservato al cliente, se possa essere riutilizzato per altri clienti, se incorpori dati o know-how del cliente e se l'exit consenta di portare via configurazioni, prompt, workflow, documentazione o solo dati grezzi.

Il tema è anche difensivo: il fornitore dovrebbe garantire che l'uso del sistema, nei limiti contrattuali, non violi diritti di terzi; il cliente dovrebbe garantire la legittimità dei dati e materiali immessi nel siste-

vedi l'articolo online

ma. Le garanzie devono essere calibrate sul controllo effettivo di ciascuna parte.

L'exit da un servizio AI è più complessa dell'exit da un SaaS. Mentre nel SaaS ci si concentra sulla tematica dell'esportazione dei dati, nei casi di contratti AI, l'exit può richiedere migrazione di prompt, configurazioni, policy, workflow, dataset, documentazione e spiegazioni tecniche, ecc.. Può richiedere anche un periodo di coesistenza tra vecchio e nuovo sistema, con confronto degli output e monitoraggio del rischio.

Qui Data Act, DORA e disciplina cloud convergono su un messaggio pratico: portabilità e switching devono essere pensati prima, non quando il rapporto è già in crisi o in scadenza. Il fornitore vorrà limitare l'assistenza all'esportazione dei dati in formati standard. Il cliente, invece, avrà bisogno di una transizione che preservi continuità operativa, audit trail, spiegabilità delle decisioni pregresse e possibilità di ricostruire il funzionamento del sistema durante il rapporto. La clausola di exit dovrebbe quindi essere collegata non solo alla cessazione del contratto, ma anche a eventi anticipatori: ritiro del modello, peggioramento delle performance, modifica di un subfornitore critico, incidente grave o concentrazione non più accettabile.

11. In definitiva: il contratto AI come architettura di controllo

L'intelligenza artificiale non si contrattualizza aggiungendo un allegato "AI compliance" a un contratto SaaS. Serve un impianto diverso.

Il contratto deve collegare intended purpose, classificazione regolatoria, dati, ruoli, sicurezza, output, supervisione umana, subfornitura, audit, continuità, exit e responsabilità. Deve consentire alla banca o assicurazione di dimostrare non solo di aver acquistato una tecnologia, ma di averla inserita in un sistema di governo controllabile.

Il vero obiettivo negoziale non dovrebbe quindi essere solo quello di trasferire al fornitore tutti i rischi; ci si dovrebbe concentrare soprattutto sul fatto che i rischi non restino invisibili.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it