METODO GIURIDICO — IUS ET RATIO
ISSN 3103-7305
Rivista Scientifica Telematica di Diritto e Giurisprudenza • Edizione Ufficiale (Roma)
DIAMOND OPEN ACCESS • FASCICOLO A4

SEZ. I • SAGGIO (DOUBLE-BLIND PEER REVIEW) • DIRITTO BANCARIO E… Anno I (Vol. 1), Fasc. 3 (2026) • Art. 7349 • pp. 1–16 • §§ 1–58

Intelligenza artificiale in vigilanza bancaria e riserva umana ABF

English Edition Title: Artificial Intelligence in Banking Supervision and Human Oversight in Banking ADR

Federico Palumbo [Co-Direttore Scientifico]
Avvocato del Foro di Roma
Profilo Accademico e Bibliografia: https://www.metodogiuridico.it/autori/federico-palumbo/

Pubblicato il: 25 Nov 2026 • Revisione paritaria a doppio cieco (Sez. I ANVUR) • Testo integrale: pp. 1–16 (§§ 1–58)

ABSTRACT SCIENTIFICO
L'impiego dell'intelligenza artificiale nella vigilanza bancaria e nella risoluzione stragiudiziale delle controversie segue una doppia traiettoria regolatoria. Sul versante prudenziale e ispettivo, l'evoluzione verso l'audit digitale continuo e la disciplina DORA e della Comunicazione Banca d'Italia 17 luglio 2026 ridefiniscono i poteri ex art. 54 TUB e i rischi contrattuali dell'AI as a Service. Sul versante della tutela individuale, invece, le carenze di spiegabilità nel credit scoring rilevate dall'indagine QEF n. 721 si misurano con l'art. 22 GDPR (Schufa), con la valutazione FRIA ex art. 27 AI Act e con il modello di supporto ancillare alle segreterie ABF del Provvedimento 3 settembre 2026, verificato contro i rischi di influenza algoritmica occulta e in chiave comparata.

CITAZIONE UFFICIALE CONSIGLIATA (STANDARD ACCADEMICO AREA 12 — SCIENZE GIURIDICHE & OSCOLA)
F. Palumbo, Intelligenza artificiale in vigilanza bancaria e riserva umana ABF, in Metodo Giuridico (ISSN 3103-7305), Anno I, n. 3, 25 novembre 2026, art. 7349, pp. 1–16, DOI: 10.5281/zenodo.24539172, disponibile su https://www.metodogiuridico.it/2026/11/25/ia-vigilanza-bancaria-abf-banca-italia/.

OSCOLA: Federico Palumbo, 'Intelligenza artificiale in vigilanza bancaria e riserva umana ABF' (2026) 1(3) Metodo Giuridico (ISSN 3103-7305) Art 7349, 1–16 <https://www.metodogiuridico.it/2026/11/25/ia-vigilanza-bancaria-abf-banca-italia/> DOI: 10.5281/zenodo.24539172 accessed 25 November 2026.

DOI Persistente:	**10.5281/zenodo.24539172 (https://doi.org/10.5281/zenodo.24539172) — CERN DataCite / Zenodo**
Permalink Canonico:	https://www.metodogiuridico.it/2026/11/25/ia-vigilanza-bancaria-abf-banca-italia/
English Edition:	https://www.metodogiuridico.it/2026/11/25/ia-vigilanza-bancaria-abf-banca-italia/en/
AEA JEL Codes:	K22 (Diritto societario, commerciale e dei mercati finanziari); G21 (Banche, intermediari creditizi e mutui ipotecari); L86 (Servizi digitali, software e intelligenza artificiale)
EuroVoc (UE):	MT 2416 istituti finanziari e di credito • diritto bancario [521]; regolamentazione finanziaria [560]; intelligenza artificiale [3030]
ECLI Pronunce:	**ECLI:EU:C:2023:957 • ECLI:IT:CASS:2021:14381CIV • ECLI:IT:COST:2011:218**

DIAMOND OPEN ACCESS • LICENZA CC BY-NC-ND 4.0 • ZERO APC
© 2026 Federico Palumbo. L'Autore conserva integralmente la titolarità dei diritti d'autore senza restrizioni. Distribuito con licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale (CC BY-NC-ND 4.0). È consentita l'auto-archiviazione immediata senza embargo della presente versione editoriale (VoR) nei repository istituzionali (IRIS/CINECA, SSRN, OpenAIRE, Zenodo).

VERIFICA ONLINE

Metodo Giuridico
Ius et Ratio • ISSN 3103-7305

APPROFONDIMENTO • DIRITTO CIVILE & DIRITTO BANCARIO E FINANZIARIO

ISSN 3103-7305 • 25 NOVEMBRE 2026

Intelligenza artificiale in vigilanza bancaria e riserva umana ABF

Doppia traiettoria tra audit digitale continuo, contratti AIaaS e resilienza DORA, credit scoring ad alto rischio e perimetro ancillare delle segreterie ABF

SCHEDA RICERCA

ORDINAMENTO
Italiano ed Europeo

MATERIA
Diritto Civile & Diritto Bancario e Finanziario

NORME CARDINE
Regolamento (UE) 2024/1689 del 13 giugno 2024 (AI Act) • Regolamento (UE) 2022/2554 del 14 dicembre 2022 (DORA) • Regolamento (UE) 2016/679 del 27 aprile 2016 (GDPR)

TAGLIO
Analisi sistematica e giurisprudenziale

JEL: K22, G21, L86 • EuroVoc: 521, 560, 3030 • Lettura 30 min

Federico Palumbo • Avvocato del Foro di Roma ISSN 3103-7305

PRINCIPIO DI DIRITTO / MASSIMA REDAZIONALE

L'impiego di sistemi algoritmici nella vigilanza bancaria e nel supporto all'Arbitro Bancario Finanziario resta legittimo solo se subordinato a base legale, piena conoscibilità tecnica e imputabilità decisoria umana.

PUNTI CHIAVE DELL'ANALISI

01
L' audit digitale continuo amplia il perimetro ispettivo ex art. 54 TUB ma impone limiti di proporzionalità contro la sorveglianza totale e presidi DORA sui contratti AIaaS esternalizzati.

02
Nel credit scoring , il censimento empirico QEF n. 721 (ottobre 2022) registrava l'assenza di restituzione XAI ai clienti (0%) e di mitigazione dei bias storici: una baseline pre- Schufa da colmare entro la scadenza FRIA del 2 dicembre 2027.

03
Il Provvedimento 3 settembre 2026 limita l'IA nelle segreterie ABF a reti isolate e decisioni anonimizzate, mentre il parere Garante 28 maggio 2026 raccomanda il monitoraggio ex art. 35, par. 9, GDPR e riserva il vaglio sull' AI Act .

04
Il raffronto con Regno Unito, Singapore, Stati Uniti e Australia conferma la necessità di separare il supporto istruttorio dalla decisione umana imputabile, prevenendo ogni influenza algoritmica occulta.

ABSTRACT (ITALIANO)

Abstract: L'impiego dell'**intelligenza artificiale nella vigilanza bancaria** e nella risoluzione stragiudiziale delle controversie segue una doppia traiettoria regolatoria. Sul versante prudenziale e ispettivo, l'evoluzione verso l'**audit digitale continuo** e la disciplina DORA e della Comunicazione Banca d'Italia 17 luglio 2026 ridefiniscono i poteri *ex* art. 54 TUB e i rischi contrattuali dell'*AI as a Service*. Sul versante della tutela individuale, invece, le carenze di spiegabilità nel *credit scoring* rilevate dall'indagine QEF n. 721 si misurano con l'art. 22 GDPR (*Schufa*), con la valutazione **FRIA *ex* art. 27 *AI Act*** e con il modello di **supporto ancillare alle segreterie ABF** del Provvedimento 3 settembre 2026, verificato contro i rischi di influenza algoritmica occulta e in chiave comparata.

ABSTRACT (ENGLISH)

Artificial Intelligence in Banking Supervision and Human Oversight in Banking ADR – *The deployment of artificial intelligence across prudential supervision and alternative dispute resolution follows two distinct trajectories in Italy. On the supervisory side, continuous digital auditing and predictive tools under Article 54 of the Consolidated Banking Act intersect with DORA resilience duties, AIaaS outsourcing contracts, and the Bank of Italy Communication of 17 July 2026, exposing vulnerabilities tied to ICT third-party concentration. On the customer-protection front, structural explainability and fairness gaps in automated credit scoring conflict with Article 22 GDPR (Schufa), Fundamental Rights Impact Assessments under Article 27 AI Act, and the constitutional reserve of human decision-making. Against this backdrop, the Bank of Italy Regulation of 3 September 2026 confines AI tools supporting Banking and Financial Ombudsman secretariats to closed-network analytics on anonymized decisions, echoing comparative benchmarks in the UK, Singapore, the US, and Australia.*

01. INTRODUZIONE: LA DOPPIA TRAIETTORIA DELL'IA TRA SUPERVISIONE PRUDENZIALE E TUTELA DEL CLIENTE

La regolazione giuridica dell'automazione finanziaria vive un singolare paradosso: mentre il mercato evolve verso ecosistemi di calcolo unificati, la risposta dell'ordinamento si biforca in due regimi concettualmente asimmetrici. Da un lato si colloca l'ingresso dell'**intelligenza artificiale nella vigilanza bancaria**, ove i modelli predittivi modificano la fisionomia del controllo prudenziale, con un'evoluzione che impone inoltre nuovi vincoli di **resilienza operativa digitale** lungo le catene di fornitura tecnologica. Dall'altro lato emerge invece il fronte della tutela individuale, nel quale il calcolo automatizzato del merito creditizio e il supporto alle procedure stragiudiziali si misurano con la **riserva di umanità** e con la conoscibilità giuridica delle decisioni.

§ 2 Sarebbe tuttavia riduttivo leggere una simile dicotomia come semplice convivenza tra efficienza pubblica e garanzie private, poiché entrambe le traiettorie convergono dinanzi alla medesima autorità creditizia nazionale. La Banca d'Italia è chiamata oggi a governare il potenziale del *SupTech* e a vigilare sull'**esternalizzazione verso grandi piattaforme tecnologiche**, gestendo al contempo in proprio applicativi di ausilio documentale per le segreterie dell'Arbitro Bancario Finanziario. La recente stagione regolatoria del 2026 consente di saggiarne la tenuta complessiva.

§ 3 Sotto il profilo normativo, il quadro muove dalle attribuzioni previste dal testo unico bancario, cui si affiancano la disciplina europea sulla resilienza operativa del settore finanziario, il regolamento generale sulla protezione dei dati e l'*AI Act*, il cui calendario per i sistemi autonomi ad alto rischio ha peraltro registrato il rinvio al **2 dicembre 2027**. Sul piano interno interviene infine la legge n. 132/2025, sancendo il carattere strumentale delle tecnologie algoritmiche rispetto al giudizio umano. L'architettura stratificata che ne emerge esige una lettura sistematica unitaria.

§ 4 L'indagine procede lungo quattro direttrici tra loro connesse. Si esamineranno dapprima il passaggio all'*audit* digitale continuo, i contratti di fornitura *AI as a Service* e i presidi interni di controllo, per poi analizzare i divari empirici rilevati nel *credit scoring* rispetto all'art. 22 GDPR e alla valutazione d'impatto sui diritti fondamentali. Si verificherà quindi il **Provvedimento Banca d'Italia 3 settembre 2026** alla luce delle patologie dell'atto algoritmico e del rischio di influenza occulta, completando il percorso con un confronto comparato e due prove di resistenza contenziosa.

02. L'INTELLIGENZA ARTIFICIALE NELLA VIGILANZA BANCARIA: DAL CONTROLLO ISPETTIVO TRADIZIONALE ALL'AUDIT DIGITALE CONTINUO

2.1 — La circolarità degli artt. 51, 53 e 54 TUB tra SupTech , audit continuo e limiti alle serie storiche

§ 5 Nel diritto bancario classico la vigilanza poggiava su una netta cesura temporale tra acquisizione di flussi periodici e verifica ispettiva episodica. Come ha illustrato Alberto Urbani (*Rivista di Diritto Bancario*, 2026)[D1], l'impiego di soluzioni ***SupTech*** supera questa scansione rigida, saldando in una **circolarità dinamica dei controlli** gli artt. 51, 53 e 54 del D.Lgs. 1° settembre 1993, n. 385. I dati trasmessi dagli intermediari alimentano così in tempo pressoché reale motori analitici capaci di segnalare anomalie gestionali e orientare gli accessi ispettivi.

§ 6 Il controllo successivo lascia così spazio a un ***audit* digitale continuo** e a tecniche di **ispezione predittiva**, poiché l'acquisizione costante di tracciati consente all'autorità di applicare algoritmi di *data mi-*

ning e generare indicatori di allerta precoce idonei a ricostruire piste di verifica granulari lungo l'intera operatività aziendale. Superando i limiti delle verifiche campionarie, l'accertamento bancario cessa dunque di limitarsi a una fotografia statica dei conti per intercettare direttamente la traiettoria evolutiva dei rischi aziendali.

§ 7 L'ampiezza della formulazione legislativa sostiene senza forzature questa estensione digitale dei poteri istruttori. L'art. 54, comma 1, TUB abilita la Banca d'Italia a «effettuare ispezioni presso le banche e i soggetti ai quali esse abbiano esternalizzato funzioni aziendali e richiedere l'esibizione di documenti e gli atti che ritenga necessari», coprendo così l'accesso alle **architetture software esternalizzate**, ai registri di addestramento e ai percorsi logici dei modelli. La potestà ispettiva segue la funzione bancaria ovunque allocata, neutralizzando schermi contrattuali tra vigilato e fornitore ICT.

§ 8 L'affidamento su modelli computazionali apre tuttavia una criticità metodologica che Urbani individua nella **fragilità delle serie storiche**. Apprendendo correlazioni da dati passati per proiettarne la validità sul futuro, l'algoritmo predittivo rischia, dinanzi a shock macroeconomici o discontinuità strutturali inedite, di riprodurre distorsioni latenti e perdere capacità selettiva. Sotto il profilo procedimentale occorre inoltre presidiare il **contraddittorio ispettivo**, consentendo al soggetto vigilato – esposto a interventi correttivi o sanzioni – di risalire alla logica delle anomalie segnalate attraverso la tracciabilità delle interrogazioni digitali.

§ 9 L'art. 5 TUB fissa poi un preciso limite ordinamentale all'espansione dei flussi di controllo, saldandosi con il **principio di proporzionalità** che governa l'approccio *risk-based* della vigilanza europea (compendiato per lo SREP nell'art. 97 della direttiva 2013/36/UE) e i criteri di modularità dell'azione ispettiva richiamati da Urbani. Se la supervisione persegue la sana e prudente gestione degli intermediari, frequenza e granularità dell'estrazione dati vanno calibrate sul profilo di rischio effettivo senza degenerare in una **sorveglianza totale** lesiva della libertà d'impresa o in una cogestione occulta delle scelte di portafoglio. L'equilibrio costituzionale richiede dunque un ispettore ***AI-assisted*, mai *AI-driven***, nel quale il calcolo automatizzato orienta le priorità istruttorie mentre la qualificazione giuridica dei fatti resta saldamente affidata al funzionario.

2.2 — Resilienza operativa digitale DORA, contratti AIaaS , vendor lock-in e doveri degli organi sociali

§ 10 Sul versante degli intermediari vigilati, l'impiego di modelli avanzati accresce le vulnerabilità lungo l'intera filiera tecnologica. In coerenza con la vigilanza regolamentare *ex* art. 53, comma 1, lett. d), TUB sul «governo societario, l'organizzazione amministrativa e contabile, nonché i controlli interni e i sistemi di remunerazione e di incentivazione», la **Comunicazione al mercato 17 luglio 2026** raccorda i presidi del regolamento (UE) 2022/2554 (DORA) con l'intelligenza artificiale nella vigilanza bancaria lungo sei direttrici operative. Le aspettative coprono *governance* (aggiornamento del RAF, competenze tecnologiche e governo dei fornitori), igiene informatica e segmentazione delle reti, censimento delle risorse ICT e *cloud*, gestione prioritaria delle vulnerabilità e delle *patch*, monitoraggio delle anomalie sotto supervisione umana e attività di test DORA *ex* artt. 24 e 25, con relazione consiliare entro il **31 dicembre 2026**.

§ 11 Il disegno nazionale si inscrive in un'azione coordinata con la **Banca Centrale Europea** nell'ambito del Meccanismo di Vigilanza Unico, dove le **Priorità di vigilanza 2026–2028** collocano resilienza operativa digitale, attuazione di DORA e strategie IA al centro del dialogo prudenziale. Già con la ***Guide on outsourcing cloud services to cloud service providers* del 16 luglio 2025**, la BCE ha precisato le aspettative

non vincolanti sulle esternalizzazioni *cloud* delle banche significative – inclusi gli applicativi di intelligenza artificiale ospitati su infrastrutture terze – concentrandosi su concentrazione dei fornitori, subappalto e piani di uscita; successivamente, con la **lettera di vigilanza del 7 luglio 2026** rivolta agli enti significativi sulle minacce informatiche potenziate da modelli IA di frontiera, l'Istituto europeo ha richiesto piani d'azione cyber approvati dal consiglio entro il 31 ottobre 2026, differendo al contempo al febbraio 2027 il questionario annuale sui rischi IT.

§ 12 Su entrambi i livelli opera quale criterio ordinatore il **principio di proporzionalità *ex* art. 4, par. 1, DORA**, espressamente richiamato dalla Comunicazione Banca d'Italia del 17 luglio 2026 affinché gli adempimenti siano graduati secondo costi-benefici, dimensioni, profilo di rischio e complessità dei servizi dell'intermediario. La clausola assume valenza sostanziale. Senza un'effettiva modulazione dimensionale, gli oneri di conformità su *governance* IA, test e presidi ICT rischierebbero paradossalmente di sospingere gli intermediari minori verso una dipendenza ancora più stretta dai grandi operatori *cloud* globali.

§ 13 La portata concreta di tali rischi trova riscontro nei numeri riferiti dalla Banca d'Italia nell'audizione parlamentare del 5 novembre 2026. Nel 2025 il sistema finanziario italiano ha subito **101 eventi operativi gravi** (137 segnalazioni), mentre nei primi nove mesi del 2026 si registrano già 68 eventi per 92 segnalazioni, di cui **quasi il 60 per cento** attribuibile a fornitori terzi. La mappatura DORA rivela del resto una rete di 3.600 prestatori su cinque livelli di subappalto, per 9.600 contratti e oltre 2,6 miliardi di euro l'anno, guidata da 19 fornitori ICT critici designati in sede europea.

§ 14 Questa dipendenza tecnologica trova un puntuale inquadramento civilistico nello studio di Costanza Morato sui contratti di ***AI as a Service* (*AIaaS*)** (*Contratto e impresa*, 2026)[D2], nel quale si osserva come l'acquisizione di capacità predittive nel comparto bancario non passi più dall'acquisto di software locale, bensì dalla fruizione remota in *cloud* multi-utente. Distinguendo tre livelli di erogazione – servizi di inferenza pronti via API, ambienti per lo sviluppo di modelli su misura e infrastrutture di calcolo – Morato mostra come, al crescere del grado di esternalizzazione dai moduli *AutoML* ai servizi gestiti, l'intermediario finisca per cedere al fornitore il governo diretto dei pesi e degli aggiornamenti.

§ 15 Dal punto di vista qualificatorio emerge una divaricazione netta tra la nozione unitaria di **servizi TIC** dell'art. 3, par. 1, n. 21, DORA e le categorie del diritto privato interno. Le prestazioni infrastrutturali dedicate e lo sviluppo personalizzato di algoritmi tendono a ricondursi allo schema dell'**appalto di servizi *ex* art. 1655 c.c.**, giacché il prestatore assume un'obbligazione organizzativa e di risultato modellata sulle specifiche dell'intermediario. La fornitura standardizzata tramite API sfugge invece al tipo legale, configurando piuttosto un contratto o **collegamento negoziale atipico** soggetto al vaglio di meritevolezza *ex* art. 1322, comma 2, c.c., nel quale il godimento remoto della piattaforma si fonde inscindibilmente con la manutenzione evolutiva e il riaddestramento continuo gestiti dal fornitore. La distinzione rileva sul riparto dei rischi di conformità, senza attenuare in ambito creditizio gli orientamenti EBA recepiti dalla Circolare Banca d'Italia n. 285/2013: la responsabilità dell'ente vigilato resta indivisa.

§ 16 Lo squilibrio negoziale rispetto ai grandi operatori globali del *cloud* genera così un acuto pericolo di ***vendor lock-in***. Risultando insufficiente tra imprese la tutela delle clausole vessatorie *ex* art. 1341 c.c., Morato richiama due correttivi esterni: l'abuso di **dipendenza tecnologica** *ex* art. 9 della L. n. 192/1998 e l'art. 13 del *Data Act* (reg. UE 2023/2854) contro le clausole inique di accesso ai dati. Il presidio europeo colpisce le asimmetrie sui dati di addestramento, ma non si estende alle clausole generali di esonero da

responsabilità. Sul piano prudenziale si aggiungono gli artt. 29 e 30 DORA, imponendo alle banche di verificare prima dell'affidamento la **sostituibilità del fornitore critico** e di inserire garanzie contrattuali obbligatorie su incidenti, formazione di sicurezza e clausole tipo europee.

§ 17 L'asimmetria negoziale così descritta conferma l'allarme istituzionale espresso da Urbani riguardo ai grandi operatori extra-europei, giacché l'imposizione unilaterale di condizioni opache fa venir meno la subalternità organizzativa su cui poggiava la vigilanza mediata, esponendo a rischio la **sana e prudente gestione *ex* art. 5, comma 2, TUB**. Gli organi gestori ne rispondono in prima persona. Come messo in luce da Carlo De Gennaro su questa Rivista in tema di responsabilità degli amministratori per l'intelligenza artificiale[D3], il dovere di istituire **assetti organizzativi adeguati *ex* art. 2086 c.c.** vieta di rimettere il governo dei rischi a scatole nere esterne.

§ 18 I contratti *AIaaS* in essere esigono dunque una rinegoziazione tempestiva prima di fine esercizio, volta ad assicurare diritti di audit illimitati, **piani di uscita verificabili**, tracciamento integrale dei *log* e portabilità effettiva dei dati di addestramento.

ADEMPIMENTI PER GLI ORGANI SOCIALI ENTRO IL 31 DICEMBRE 2026
In vista della Relazione alla Banca d'Italia prevista dalla Comunicazione 17 luglio 2026, il consiglio di amministrazione deve approvare l'inventario integrale dei modelli IA e degli strumenti di terzi in uso, estendendo il *Risk Appetite Framework* e il perimetro DORA ai rischi di modello. Occorre inoltre mappare i subfornitori sino ai livelli inferiori, verificare il rischio di *vendor lock-in ex* art. 29 DORA e inserire clausole di uscita, audit e segnalazione incidenti conformi all'art. 30 DORA e alla Circolare n. 285/2013.

2.3 — Burocrazia algoritmica, stress test digitali e antiriciclaggio nella tenuta della discrezionalità tecnica

§ 19 L'espansione dei modelli computazionali dentro la macchina bancaria alimenta un rischio che Urbani qualifica come **burocrazia algoritmica**: quando le funzioni interne automatizzano punteggi sintetici e semafori di allerta, la scelta gestoria tende ad appiattirsi sulla ratifica dell'indice numerico, generando una pericolosa **illusione di sicurezza negli *stress test*** digitalizzati. Se le simulazioni poggiano su serie storiche prive di crisi analoghe a quella sopravvenuta, la precisione apparente del calcolo occulta fragilità patrimoniali reali. La verifica tecnica automatizzata non può dunque sostituire il giudizio prospettico di adeguatezza patrimoniale rimesso agli organi amministrativi.

§ 20 La medesima tensione affiora nella prevenzione del riciclaggio rispetto agli obblighi di conservazione e segnalazione *ex* art. 36 del D.Lgs. n. 231/2007. Il sistema informatico eccelle nel rilevare anomalie statistiche ricorrenti ma fatica a decifrare il contesto economico lecito di operazioni societarie complesse, favorendo un ***over-reporting* difensivo** che scarica sull'autorità investigativa un flusso ridondante di allarmi non filtrati. Preservare la **discrezionalità tecnica dell'amministratore** impedisce che il *business judgment* si riduca a mera osservanza dell'algoritmo: ogni determinazione ad alto rilievo prudenziale esige un riesame critico motivato.

PRESIDIO NORMATIVO / ATTO	AMBITO OPERATIVO	SCADENZA / SOGLIA CHIAVE	PRINCIPIO / RICADUTA OPERATIVA
Artt. 5, 51, 53, 54 TUB	Vigilanza informativa, regolamentare e ispettiva	Controllo continuo e accessi presso terzi esternalizzati	Ispettore AI-assisted ; divieto di sorveglianza totale
Reg. (UE) 2022/2554 (DORA) e D.Lgs. n. 23/2025	Resilienza operativa ICT e contratti AIaaS	19 fornitori critici UE; 3.600 prestatori mappati in Italia	Valutazione lock-in ex art. 29 e clausole ex art. 30 DORA
Comunicazione BI 17 luglio 2026	Aspettative su resilienza digitale e IA avanzata	Relazione consiliare entro 31 dicembre 2026	Sei aree: RAF/governance, igiene ICT, risorse cloud , patch , monitoraggio e test DORA
Reg. (UE) 2024/1689 e Reg. (UE) 2026/1744	Sistemi ad alto rischio nel credito e autorità settoriale	Differimento al 2 dicembre 2027 (Allegato III)	Sorveglianza umana art. 14, FRIA art. 27, vigilanza BI

03. IL CREDIT SCORING ALGORITMICO TRA SCHUFA , INDAGINE QEF N. 721, AI ACT E FRIA

3.1 — L'estensione dell'art. 22 GDPR nella giurisprudenza Schufa e l'invalidità del consenso opaco

§ 21 Nella valutazione del merito creditizio emerge il conflitto diretto tra automatismi predittivi e diritti della persona. La tutela poggia sull'art. 22, par. 1, GDPR, che riconosce il diritto a «non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Per anni gli operatori hanno aggirato il divieto scomponendo la filiera, così che la centrale rischi elaborava il punteggio statistico mentre la banca firmava il diniego.

§ 22 La **sentenza *Schufa* della Corte di Giustizia UE**[1] ha superato questo schema ricomponendo le tre condizioni cumulative della norma – l'esistenza di una decisione, la base automatizzata mediante profilazione e l'incidenza significativa – per chiarire che anche il calcolo di un tasso di probabilità integra una decisione *ex* **art. 22 GDPR** quando guida in via decisiva il rifiuto del mutuo. Come rileva Luljeta Plakolli-Kasumi[D4], la clausola che scaricava la scelta finale sulla banca lasciava il cliente in un limbo di responsabilità incrociata, oggi colmato dalla piena **trasparenza della logica significativa** *ex* art. 15, par. 1, lett. h), GDPR.

§ 23 Sul piano interno l'indirizzo europeo converge con il principio affermato dalla **Cassazione Civile** in materia di rating reputazionale[2], secondo cui il consenso dell'interessato non può ritenersi valido quando restino ignoti lo schema esecutivo dell'algoritmo e gli elementi ponderati. Il difetto di trasparenza preventiva determina dunque l'**invalidità del consenso opaco** e priva il trattamento di base giuridica, con una lacuna originaria che nessuna accettazione formale di mercato può sanare.

§ 24 Trasportato nell'istruttoria creditizia, il raccordo tra *Schufa* e legittimità restringe drasticamente le deroghe dell'art. 22, par. 2, GDPR, impedendo tanto alla necessità contrattuale quanto al consenso di validare un modello opaco privo di accesso ai fattori determinanti dello *score*. Dovendo inoltre assicurare all'aspirante mutuatario un effettivo **diritto di riesame umano** e di contestazione sulla determinazione

sfavorevole, l'opacità cessa di fungere da prerogativa aziendale protetta per convertirsi in vizio di liceità del trattamento.

3.2 — I divari empirici nei modelli italiani secondo l'indagine QEF n. 721

§ 25 La profondità dello scarto originario tra standard legale e prassi bancaria emerge con chiarezza dalla **Questione di Economia e Finanza n. 721** della Banca d'Italia[D5], pubblicata nell'**ottobre 2022** su **38 modelli di apprendimento automatico** adottati da dieci tra i principali intermediari italiani nel comparto creditizio. Lo scarto cronologico va dichiarato con nettezza. La rilevazione precede di oltre un anno la sentenza *Schufa* del dicembre 2023 e l'adozione dell'*AI Act*, sicché non può valere quale fotografia automatica del grado di adeguamento raggiunto nel 2026; in assenza di un censimento pubblico successivo di pari ampiezza, resta però la principale **base empirica di partenza** sulle vulnerabilità strutturali del mercato. Già allora i sistemi risultavano maturi sul piano applicativo – con il 61 per cento in produzione effettiva e una prevalenza di algoritmi ad albero decisionale rispetto alle reti neurali –, ma accompagnavano la diffusione a una marcata asimmetria di trasparenza verso la clientela.

§ 26 I dati raccolti sulla spiegabilità mostravano infatti una frattura netta tra controlli interni e tutela esterna. Sebbene il **92 per cento dei modelli** impiegasse tecniche *post hoc* – soprattutto valori di Shapley e indici di rilevanza delle variabili – riservate ai comitati tecnici e al dialogo con il supervisore, la quota di spiegazioni restituite ai clienti esterni si fermava allo **zero per cento**. Nessuna delle banche censite traduceva dunque i test interni in motivazioni comprensibili al richiedente respinto, rendendo impervio l'esercizio delle prerogative di intervento umano e contestazione previste dall'art. 22, par. 3, GDPR.

§ 27 Altrettanto critici apparivano i riscontri sull'equità statistica e sull'esternalizzazione. Solo il 46 per cento dei sistemi adottava test di *fairness*, fondati per intero sulla tecnica formale della *fairness through unawareness*, con un'impostazione che escludeva gli attributi protetti dall'ingresso senza neutralizzare le correlazioni indirette veicolate da variabili sostitutive quali la residenza o le abitudini di spesa. Alla totale assenza di interventi correttivi contro i pregiudizi radicati nelle serie storiche si sommava infine una marcata dipendenza esterna: il **47 per cento dei modelli** coinvolgeva fornitori terzi e l'**8 per cento** ricorreva al doppio *outsourcing*, accrescendo l'esposizione ai rischi di *data drift*.

> ***Un modello di credito tecnicamente spiegabile solo agli ispettori interni resta giuridicamente opaco per il cliente inciso, trasformando la promessa di equità statistica in un diniego sottratto a effettivo contraddittorio.***

3.3 — Alto rischio, sorveglianza umana e valutazione d'impatto FRIA ex artt. 14 e 27 AI Act

§ 28 Le lacune evidenziate dalla *baseline* dell'indagine QEF n. 721 assumono rilievo sanzionatorio diretto sotto il regolamento (UE) 2024/1689 (*AI Act*), il cui Allegato III, punto 5, lettera b), classifica ad **alto rischio** i sistemi destinati a valutare il merito creditizio delle persone fisiche, eccettuati quelli dedicati al rilevamento delle frodi. Scatta così l'obbligo di conformità all'art. 14 AI Act sulla **sorveglianza umana effettiva**, in forza del quale i sistemi vanno «progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso».

§ 29 Il paragrafo 4 del medesimo articolo precisa la portata operativa di questo controllo. Al sorvegliante spetta il potere reale di «decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio», insieme alla piena consapevolezza rispetto alla distorsione dell'automazione. Come osservano Giulia Taraborrelli e Luca Megale (*Giornale di diritto amministrativo*, 2026)[D6], la disposizione vieta la semplice ratifica formale del punteggio ed esige la comprensione dei limiti del modello e un potere effettivo di dissenso motivato.

§ 30 Sul piano degli adempimenti preventivi, le banche che adottano tali sistemi devono effettuare la **valutazione FRIA *ex*** art. 27 AI Act, verificando i rischi «sui diritti fondamentali che l'uso di tale sistema può produrre». L'analisi descrive processi applicativi, frequenza d'uso, categorie di consumatori coinvolte, misure di sorveglianza e meccanismi di reclamo. I relativi esiti vanno notificati all'autorità competente e raccordati con la **valutazione d'impatto *ex* art. 35 GDPR** per evitare duplicazioni, tenendo tuttavia distinti i piani della tutela antidiscriminatoria e della protezione dei dati.

§ 31 Sotto il profilo temporale, il **Regolamento (UE) 2026/1744** ha differito al **2 dicembre 2027** gli obblighi applicabili ai sistemi autonomi ad alto rischio dell'Allegato III. Come riferito dall'Istituto nell'audizione parlamentare del 5 novembre 2026, da quella data la Banca d'Italia opererà a pieno titolo quale autorità di vigilanza del mercato per il comparto creditizio. Il rinvio non autorizza tuttavia alcuna inerzia nel **governo algoritmico del credito**, giacché i principi dell'art. 22 GDPR e gli obblighi di controllo del rischio risultano già oggi vincolanti e anticipano lo standard europeo.

04. L'IA NEL SUPPORTO ALL'ABF: PROVVEDIMENTO 3 SETTEMBRE 2026, PARERE DEL GARANTE E RISERVA DI UMANITÀ

4.1 — Natura giustiziale dell'ABF, funzioni delle segreterie nel provvedimento 3 settembre 2026 e rilievi del Garante

§ 32 Nel contenzioso davanti all'Arbitro Bancario Finanziario la Banca d'Italia assume in proprio la veste di titolare del trattamento di sistemi analitici di supporto. Istituito ai sensi dell'art. 128-bis, comma 2, TUB, secondo cui le procedure «devono in ogni caso assicurare la rapidità, l'economicità della soluzione delle controversie e l'effettività della tutela», l'Arbitro opera tramite collegi indipendenti assistiti dalle segreterie tecniche, in una cornice organizzativa che poggia tuttora sulla delibera CICR del 29 luglio 2008, n. 275.

§ 33 La **Corte costituzionale**[3] ha escluso la natura giurisdizionale dei collegi ABF, chiarendo che essi, pur decidendo secondo diritto nel contraddittorio delle parti, esercitano una **funzione giustiziale amministrativa** priva di forza cogente e di giudicato, la cui efficacia riposa sull'effetto reputazionale verso l'intermediario, fermo il pieno accesso al giudice ordinario. L'automazione istruttoria nelle segreterie va quindi vagliata anzitutto sotto il profilo della legittimità amministrativa e della tutela dei dati personali.

§ 34 Su tali premesse il **Provvedimento Banca d'Italia 3 settembre 2026** (*G.U.* n. 215/2026) disciplina applicativi privi di connessioni esterne lungo cinque funzioni specifiche. Anzitutto, strumenti di ricerca avanzata su testi integrali scandagliano i ricorsi dell'ultimo decennio per redigere la relazione tecnica, escludendo i dati ex artt. 9 e 10 GDPR dalle chiavi di ricerca. In secondo luogo, appositi modelli estraggono date, importi e intermediari per vagliare ammissibilità e divieto di *ne bis in idem* decennale.

§ 35 In terzo luogo, algoritmi di apprendimento automatico eseguono una **clusterizzazione semantica** sulle sole decisioni già anonimizzate dei collegi, estraendo etichette gerarchiche ed evidenziando tanto le pronunce tipiche (**centroidi**) quanto quelle divergenti (***outlier***). Seguono l'ausilio alla verifica dell'anonimizzazione prima della pubblicazione e il monitoraggio spazio-temporale aggregato dei flussi, utile dinanzi al balzo del **21 per cento dei ricorsi ABF** sulle frodi nei pagamenti nel 2025. Le analisi statistiche non attivano ispezioni automatiche di vigilanza.

§ 36 Sul piano delle garanzie tecniche, il provvedimento scandisce tre termini di conservazione differenziati. I fascicoli sulla nomina e revoca dei membri restano negli archivi venti anni, mentre quelli del procedimento ABF durano trenta anni internamente e cinque sul portale; i dati processati negli applicativi algoritmici sono invece conservati per **dieci anni** dall'acquisizione del ricorso per verificare l'affidabilità delle serie storiche. Completano il quadro formazione periodica, riaddestramento vigilato da giuristi e data scientist, tracciamento delle versioni e informativa sul portale con i limiti dell'art. 2-undecies del Codice privacy.

§ 37 Nel preambolo del regolamento, la Banca d'Italia esclude la qualifica di alto rischio invocando la deroga dell'art. 6, par. 3, e il considerando 61 *AI Act*, che sottrae a tale regime i sistemi impiegati nelle procedure ADR per attività amministrative puramente accessorie – come l'anonimizzazione di documenti o la gestione dei fascicoli – prive di incidenza sulla decisione dei singoli casi. Sul versante della protezione dei dati, lo schema regolamentare recepisce invece le osservazioni maturate nelle interlocuzioni informali con gli uffici del Garante Privacy (art. 25 GDPR). Nel **parere del Garante Privacy del 28 maggio 2026** (doc. web 10259660), l'Autorità ha espresso un assenso limitato al GDPR e al Codice privacy, raccomandando di aggiornare periodicamente la valutazione d'impatto *ex* art. 35, par. 9, GDPR mediante il coinvolgimento di collegi e parti, e ha formulato un'**espressa riserva sull'*AI Act***, rinviando ogni giudizio alla piena vigenza del regolamento europeo.

4.2 — Legalità algoritmica, influenza occulta, patologie dell'atto e riserva di umanità nella L. n. 132/2025

§ 38 La clausola di non interferenza decisoria su cui regge il regolamento ABF va misurata con i principi del giudice amministrativo. Nella sequenza tracciata dal **Consiglio di Stato** tra il 2019 e il 2020[4][5][6], la regola tecnica del software assume natura di atto amministrativo generale soggetto ai canoni di trasparenza, ragionevolezza e pieno sindacato giurisdizionale. Ne discendono la traduzione della formula tecnica in regola giuridica, l'inopponibilità del segreto del fornitore e la verifica umana non esclusiva.

§ 39 Le medesime garanzie trovano oggi ulteriore conferma nella pronuncia del **T.A.R. Veneto n. 1845/2025**[7], che esclude di poter fondare l'automazione decisoria su generiche norme di autorganizzazione. Richiamando l'art. 14 della L. 23 settembre 2025, n. 132 – come già osservato da chi scrive su questa Rivista riguardo all'IA nella P.A. *ex* L. n. 132/2025[D7] –, i giudici affermano la **legalità algoritmica**, subordinando ogni soluzione informatica a espressa base di legge e a un ruolo meramente strumentale sotto la responsabilità dell'uomo.

§ 40 La vera prova di tenuta della clausola di non interferenza si gioca però sul discrimine, ancora aperto dopo il 2 dicembre 2027, tra esenzione preparatoria e alto rischio *ex* **Allegato III, punto 8, *AI Act***. La norma include tra i sistemi ad alto rischio quelli destinati ad assistere autorità giudiziarie e organismi ADR nella ricerca e interpretazione dei fatti e del diritto. Occorre perciò scomporre analiticamente le cinque funzioni del Provvedimento 3 settembre 2026 anziché trattarle in blocco. Ricerca *full-text* su ri-

corsi pregressi, estrazione di date e importi per il *ne bis in idem*, ausilio all'anonimizzazione e monitoraggio aggregato restano con coerenza dentro il perimetro preparatorio dell'art. 6, par. 3, e del considerando 61 *AI Act*; la **clusterizzazione semantica** delle decisioni anonimizzate si colloca invece su un crinale assai più esposto. Raggruppando i precedenti secondo una gerarchia statistica tra *centroidi* e *outlier* a monte della relazione tecnica, l'algoritmo orienta la precomprensione del collegio, alimentando il pericolo cognitivo dell'***automation bias*** evidenziato da Giulia Taraborrelli e Luca Megale in relazione agli artt. 3, 24 e 97 Cost.

§ 41 A nostro giudizio, la clusterizzazione semantica potrà reggere dentro l'eccezione dell'art. 6, par. 3, *AI Act* anche oltre il 2027 solo se l'architettura regolamentare traduce l'assenza di automazione decisoria in garanzie procedurali verificabili. Entra qui in gioco la doppia esigenza di ***AIxplainability*** individuata da Antonino Ripepi (*Giurisprudenza Italiana*, 2026)[D8] per i modelli adattivi non deterministici: la **conoscibilità** dell'architettura tecnica nel bilanciamento con il segreto industriale e la **comprensibilità** concreta della logica applicata. Scongiurare un'**influenza algoritmica occulta** richiede perciò tre presidi cogenti: la **tracciabilità integrale delle interrogazioni** *ex* art. 9 del D.P.R. n. 62/2013 (coerentemente con l'onere probatorio gravante su chi sceglie l'opacità), la restituzione neutra di *centroidi* e *outlier* senza gerarchie presuntive, e un effettivo onere del collegio di motivare autonomamente rispetto al grappolo di precedenti richiamato.

§ 42 La medesima esigenza di imputabilità chiarisce il regime delle patologie quando il supporto informatico sconfini oltre il proprio perimetro ancillare. Inquadrando il **provvedimento algoritmico** come *species* procedimentale ordinaria in cui il software rimane un semplice *instrumentum*, Giovanni Gallone e Angelo Giuseppe Orofino (*Giurisprudenza Italiana*, 2026)[D9] ancorano l'imputazione all'ente tramite l'**immedesimazione organica** del funzionario decidente e l'oggettivazione della volontà nelle regole operative. L'affidamento al supporto digitale conserva così natura reversibile, mentre eventuali barriere tecniche delle piattaforme violano i doveri di buona fede e collaborazione *ex* art. 1, comma 2-bis, della L. n. 241/1990.

§ 43 Ne discende una graduazione rigorosa dei vizi dell'atto amministrativo automatizzato, utile quale parametro anche nel sindacato sull'istruttoria tecnica. La **nullità** radicale resta circoscritta ai soli casi di carenza dell'atto di investitura che legittima il ricorso al sistema informatico. La mancata formalizzazione dei criteri di calcolo in un atto presupposto, il difetto di direttive umane o l'elusione della riserva decisionale integrano invece di regola l'**annullabilità per violazione di legge**, affiancata dai vizi intrinseci di logicità e dal sindacato su **inadeguatezza del mezzo e qualità dei dati** che impone tarature periodiche del software. Sul piano istituzionale, infine, Ilaria Speziale (*Contratto e impresa*, 2026)[D10] evidenzia l'attrito tra la designazione governativa di AgID e ACN *ex* art. 20 della L. n. 132/2025 e i requisiti di indipendenza dell'art. 70 *AI Act*. Senza un presidio trasversale autonomo, grava su Banca d'Italia e Garante Privacy la tenuta del confine tra ausilio istruttorio e giudizio collegiale.

ORGANO E DATA	ESTREMI	PRINCIPIO DI DIRITTO RILEVANTE
Corte cost. 21 luglio 2011	ord. n. 218	L'ABF svolge funzione giustiziale amministrativa non cogente con efficacia reputazionale e senza preclusione del giudizio ordinario.
Cons. Stato 8 aprile 2019	sent. n. 2270	La regola algoritmica ha valenza giuridica di atto informatico e richiede traduzione intellegibile nonché pieno sindacato giurisdizionale.
Cons. Stato 13 dicembre 2019	sent. n. 8472	Sancisce conoscibilità con inopponibilità del segreto del fornitore, intervento umano non esclusivo e non discriminazione algoritmica.
Cons. Stato 4 febbraio 2020	sent. n. 881	Ribadisce l'imputabilità della decisione all'organo competente e la verifica di logicità tecnica a carico dell'amministrazione.
Cass. Civ. 25 maggio 2021	ord. n. 14381	Il consenso a un sistema algoritmico di rating è nullo se restano ignoti lo schema esecutivo e gli elementi di calcolo.
CGUE 7 dicembre 2023	causa C-634/21	Il calcolo automatizzato dello score integra una decisione ex art. 22 GDPR quando condiziona in modo decisivo il credito bancario.
T.A.R. Veneto 21 ottobre 2025	sent. n. 1845	La decisione automatizzata richiede espressa base legale primaria e rispetto della riserva di umanità ex art. 14 L. n. 132/2025.

05. PROFILI COMPARATI: L'UNIONE EUROPEA A CONFRONTO CON REGNO UNITO, SINGAPORE, STATI UNITI, AUSTRALIA E MODELLI ODR

5.1 — Trapiantabilità modulare dell' AI Act e modelli di vigilanza FinTech tra USA, Regno Unito e Asia-Pacifico

§ 44 Le tensioni emerse nel sistema italiano acquistano maggiore nitidezza se confrontate con i tre modelli regolatori più significativi fuori dall'Unione Europea, muovendo dalla diagnosi comparata di Van Thanh Hoang e Ngoc Mai Nguyen[D11] sull'*AI Act* quale **architettura modulare** a portabilità diseguale. Mentre la grammatica del rischio, gli obblighi documentali e le *sandbox* circolano con facilità tra ordinamenti, resiste alla trasposizione il nucleo più garantista del modello europeo: l'**operabilità dei diritti** (*rights-operability*), ossia la possibilità effettiva per il singolo di impugnare una decisione algoritmica dinanzi a un organo indipendente.

§ 45 Proprio su questa faglia si divaricano le risposte di **Regno Unito** e **Singapore** rispetto alla codificazione europea. L'esperienza britannica privilegia un approccio pro-innovazione affidato ai regolatori settoriali senza legge unitaria sull'IA, mentre Singapore punta su strumenti tecnici volontari di validazione

e *sandbox* attraverso la piattaforma *AI Verify*. Ne guadagna l'agilità applicativa, ma si riduce l'azionabilità soggettiva dei rimedi individuali.

§ 46 Sul piano strettamente finanziario, il raffronto sviluppato da Ádám Köteles[D12] contrappone la frammentazione multi-agenzia degli **Stati Uniti** all'armonizzazione dell'Unione Europea. Oltreoceano il controllo *FinTech* si ripartisce tra SEC, CFTC e CFPB su scala federale e statale, stimolando la sperimentazione ma moltiplicando sovrapposizioni e oneri di conformità. L'Europa coordina invece il settore mediante PSD2, MiFID II, EBA e l'art. 74, par. 6, AI Act, concentrando nelle **autorità di vigilanza finanziaria** la sorveglianza sugli intermediari regolati. Comune a tutti e tre i modelli resta però la sfida tecnica segnalata da Köteles: l'uso di dati non tradizionali, come geolocalizzazione e metadati sociali, eccede spesso la verifica immediata dei supervisori, esigendo test controllati e una **proporzionalità regolamentare calibrata** sul rischio.

5.2 — Credit scoring post- Schufa e lezione Robodebt : dall' automation bias alla AI Golden Rule

§ 47 Il problema dell'effettività rimediale torna al centro dell'analisi bancaria svolta da Plakolli-Kasumi[D4] dopo il caso *Schufa*, mostrando come un intervento umano puramente formale non valga a sottrarre il processo decisionale al divieto dell'art. 22 GDPR. Le corti europee pretendono una valutazione attiva da parte di operatori dotati di competenza, autorità, diligenza e indipendenza rispetto al punteggio statistico. Né il segreto commerciale né le clausole di manleva tra agenzia e banca possono dunque bloccare l'accesso *ex* art. 15, par. 1, lett. h), GDPR.

§ 48 Nel diritto pubblico di *common law*, la lezione australiana del caso ***Robodebt*** esaminata da Benedict Sheehy e Yee-Fui Ng[D13] offre un riscontro speculare. Quel sistema automatico di accertamento e recupero crediti assistenziali colpì migliaia di cittadini vulnerabili violando legalità, equità procedurale e responsabilità pubblica. I due studiosi distinguono opportunamente la **scatola nera tecnica**, legata alla complessità del modello, dalla più insidiosa **scatola nera giuridica**, che insorge quando l'opacità impedisce di enunciare le ragioni legali della decisione paralizzandone l'impugnazione davanti al giudice.

§ 49 Per superare la doppia opacità, Sheehy e Ng valorizzano la cosiddetta ***AI Golden Rule*** sperimentata in Australia nei settori dell'immigrazione e dei veterani. L'architettura di **progettazione regolatoria** limita l'automazione di smistamento alle sole decisioni pienamente favorevoli al richiedente fondate su criteri certi, devolvendo ogni esito sfavorevole o discrezionale a funzionari umani responsabili che operano secondo il diritto amministrativo ordinario. Il nesso con l'art. 14 della L. n. 132/2025 e con il regolamento ABF è netto: ogni determinazione restrittiva esige un decisore umano identificabile e contestabile.

5.3 — Intelligenza artificiale generativa, rischi di allucinazione e progettazione dei sistemi ODR per i consumatori

§ 50 Sul piano delle controversie di consumo, il diritto comparato offre una conferma empirica delle scelte del regolamento ABF attraverso la ricerca di Vivi Tan, Jeannie Paterson e Julian Webb[D14] sull'uso dell'IA generativa nei sistemi di *Online Dispute Resolution* (**ODR**) per reclami di modico valore. I grandi modelli linguistici manifestano una vulnerabilità strutturale alle allucinazioni giuridiche. Su quesiti diretti relativi a precedenti giudiziari, i test citati registrano tassi di errore tra il **58 per cento** (GPT-4) e l'**88 per cento** (Llama 2), con forte propensione a recepire premesse inesatte dell'utente e a proiettare schemi nordamericani su altri ordinamenti.

§ 51 Neppure le architetture di *Retrieval-Augmented Generation* (**RAG**) su banche dati legali commerciali eliminano il rischio. Superando la definizione ristretta di pura invenzione di precedenti inesistenti per includervi ogni asserzione giuridica priva di supporto nella fonte richiamata, gli autori documentano tassi di allucinazione tra il **17 e il 33 per cento** persino su piattaforme specialistiche di ricerca legale. Margini di errore di questo ordine risultano incompatibili con l'istruttoria delle liti bancarie e rafforzano le cautele già raccomandate alle corti britanniche verso i chatbot pubblici.

§ 52 Riletto insieme al Provvedimento Banca d'Italia 3 settembre 2026, questo dato avvalora la scelta conservativa dell'ordinamento italiano, dove la segreteria ABF esclude connessioni esterne e limita l'automazione alla ricerca full-text e alla clusterizzazione su decisioni anonimizzate sotto controllo multidisciplinare. Tan, Paterson e Webb richiamano tuttavia un ulteriore vincolo di **design istituzionale**, osservando come un portale ODR progettato senza adeguate garanzie di mediazione umana rischi di scoraggiare i consumatori nei reclami minori e ampliare l'asimmetria informativa verso le banche.

ORDINAMENTO	MODELLO REGOLATORIO	PRESIDIO SU CREDITO E ADR	CRITICITÀ COMPARATA
Unione Europea / Italia	Codificazione per rischio (AI Act , DORA, GDPR, L. 132/2025)	FRIA, sorveglianza art. 74(6) a BI, ABF su rete isolata	Complessità di coordinamento AgID/ACN e autorità di settore
Regno Unito	Principi pro-innovazione gestiti dai regolatori settoriali	Vigilanza finanziaria e condotta senza statuto IA unitario	Possibili scarti di tutela orizzontale sui fornitori terzi
Singapore	Framework di test e assicurazione tecnica (AI Verify)	Sandbox regolatorie FinTech e validazione volontaria	Minore azionabilità soggettiva rispetto ai diritti UE
Stati Uniti	Supervisione federale/statale multi-agenzia (SEC, CFTC, CFPB)	Controllo ex post sulle pratiche ingannevoli e creditizie	Frammentazione normativa e oneri di conformità sovrapposti
Australia	Regolazione per principi, AI Golden Rule e design ODR	Automazione limitata agli esiti favorevoli; cautela GenAI/RAG	Lezione Robodebt sulla responsabilità pubblica degli esiti negativi

06. VALUTAZIONE CRITICA, STRESS-TEST APPLICATIVI E PROSPETTIVE

6.1 — Quali tutele e oneri probatori operano nel contenzioso su scoring esternalizzato e decisioni ABF?

§ 53 Nel contenzioso su *scoring* e ricorsi ABF, l'**onere probatorio grava sull'intermediario e sul titolare del trattamento**, i quali non possono opporre il segreto industriale del fornitore per negare l'accesso *ex* art. 15 GDPR né sottrarsi alla prova dell'effettivo intervento umano.

§ 54 Una prima prova di resistenza concerne il **diniego di mutuo fondato su *credit scoring* esternalizzato**. Quando la banca recepisce il punteggio terzo senza spiegazioni individuali, il difensore può attivare l'accesso ai criteri determinanti *ex* art. 15, par. 1, lett. h), GDPR, cumulandolo con l'eccezione *ex* art. 22 GDPR secondo *Schufa*[1] e con la nullità del consenso su clausole opache affermata dalla Cassazione[2]. Alla luce della *baseline* QEF n. 721, spetta alla banca provare verifiche effettive di non discriminazione

oltre l'esclusione formale dei dati sensibili. Sul piano del ***distinguishing***, questa tutela piena **non trova applicazione** dinanzi ai filtri antifrode esclusi dall'Allegato III o a mere segnalazioni preliminari che lascino intatta l'istruttoria umana.

§ 55 Una seconda verifica investe i reclami ABF sulle **frodi nei pagamenti** (+21 per cento nel 2025), esaminati tramite filtri preliminari e raggruppamenti per *cluster*. Qualora il ricorrente tema che un'**influenza algoritmica occulta** abbia appiattito un caso atipico nella relazione tecnica, il difensore può pretendere tracciabilità delle ricerche e piena motivazione giuridica, operando tuttavia un preciso ***distinguishing*** rispetto agli atti autoritativi censurati dal T.A.R. Veneto[7]. **Fattispecie diversa** da una revoca amministrativa priva di base legale è infatti il responso non vincolante dei collegi ABF[3]. Poiché la decisione non forma giudicato *ex* art. 128-bis, comma 3, TUB, il cliente conserva intatta l'azione civile ordinaria, nella quale contestare nel merito tanto la responsabilità contrattuale della banca quanto eventuali difetti di taratura o di qualità dei dati nei presidi antifrode.

§ 56 La difesa più efficace salda quindi le eccezioni sostanziali di nullità e inadempimento agli strumenti istruttori su accesso, versioni del modello, tarature tecniche e valutazione d'impatto.

CHECK-LIST DIFENSIVA SU SCORING ESTERNALIZZATO E RICORSO ABF

In caso di diniego del credito: formulare istanza *ex* art. 15, par. 1, lett. h), GDPR sui fattori determinanti dello *score*; contestare l'inopponibilità del segreto del fornitore e l'assenza di revisione umana effettiva *ex* art. 22 GDPR; sollecitare l'esibizione della DPIA e della futura FRIA. Nei procedimenti ABF: documentare per tempo le peculiarità del caso rispetto ai precedenti tipizzati ed esercitare, se necessario, l'azione civile ordinaria *ex* art. 128-bis, comma 3, TUB.

6.2 — Governance multi-autorità ex art. 70 AI Act e bilancio conclusivo

§ 57 Il bilancio complessivo dell'indagine conduce a un nodo istituzionale decisivo per il biennio verso il **2 dicembre 2027**: come ha osservato Ilaria Speziale esaminando il rapporto tra art. 20 della L. n. 132/2025 e art. 70 *AI Act*, la pluralità di competenze tra AgID, ACN, Garante Privacy e vigilanza creditizia esige protocolli vincolanti di **coordinamento multi-autorità**. Se l'attribuzione alla Banca d'Italia del ruolo di autorità del mercato *ex* art. 74, par. 6, *AI Act* (audizione parlamentare della Banca d'Italia, 5 novembre 2026) assicura continuità prudenziale e impone, come ricorda Köteles, la pronta informativa verso la Banca Centrale Europea per i profili rilevanti nella vigilanza unica, rimane indispensabile raccordare tale azione con il controllo trasversale del Garante Privacy.

§ 58 Sul fronte interno dell'Arbitro Bancario Finanziario, la tenuta del Provvedimento 3 settembre 2026 dipenderà dalla consultazione periodica dei collegi e delle parti raccomandata dal Garante in sede di DPIA e dalla capacità di mantenere la clusterizzazione semantica entro presidi trasparenti e reversibili. Così ricomposta, la disciplina dell'intelligenza artificiale nella vigilanza bancaria e nei rimedi ABF converge verso un principio unitario netto: l'innovazione computazionale legittima l'azione creditizia soltanto quando ispezioni *AI-assisted*, **contratti *AIaaS* sottoposti a DORA** e strumenti delle segreterie restano subordinati alla **conoscibilità tecnica dei modelli** e all'**imputabilità decisoria umana**.

REPERTORIO DELLE FONTI

Apparato delle Fonti e Autorità Citate

I. FONTI NORMATIVE

Regolamento (UE) 2024/1689 del 13 giugno 2024 (AI Act) – sorveglianza umana, valutazione d'impatto FRIA, sistemi ad alto rischio nel merito creditizio e vigilanza del mercato settoriale, con calendario differito dal Regolamento (UE) 2026/1744 (artt. 6, 14, 27, 70, 74 e Allegato III, punto 5, lett. b)).

Regolamento (UE) 2022/2554 del 14 dicembre 2022 (DORA) – resilienza operativa digitale per il settore finanziario, rischio di sostituzione e clausole sui fornitori terzi ICT e AIaaS (artt. 3, 5, 6, 24, 25, 29, 30 e Capo V).

Regolamento (UE) 2016/679 del 27 aprile 2016 (GDPR) – decisioni automatizzate, profilazione, accesso alla logica significativa e valutazione d'impatto (artt. 15, 22 e 35).

D.Lgs. 1 settembre 1993, n. 385 (Testo unico bancario) – sana e prudente gestione, vigilanza informativa, regolamentare e ispettiva e risoluzione stragiudiziale ABF (artt. 5, 51, 53, 54 e 128-bis).

Legge 23 settembre 2025, n. 132 – disciplina nazionale sull'uso strumentale dell'intelligenza artificiale nella pubblica amministrazione, nella giurisdizione e sulle autorità nazionali (artt. 14, 15 e 20).

Regolamento (UE) 2023/2854 del 13 dicembre 2023 (Data Act) e D.Lgs. 10 marzo 2025, n. 23 – clausole inique nell'accesso B2B ai dati (art. 13 Data Act) e adeguamento nazionale al regolamento DORA.

Provvedimento Banca d'Italia 3 settembre 2026 (G.U. n. 215 del 16 settembre 2026) – regolamento sul trattamento dei dati personali nelle attività di supporto all'Arbitro Bancario Finanziario.

Comunicazione Banca d'Italia 17 luglio 2026 e Circolare n. 285/2013 – aspettative di vigilanza sulla resilienza operativa digitale, modelli avanzati di intelligenza artificiale ed esternalizzazione di funzioni aziendali.

II. GIURISPRUDENZA CITATA

[1] **Corte di Giustizia dell'Unione Europea, sentenza 7 dicembre 2023, causa C-634/21 (OQ c. Land Hessen / Schufa) [ECLI:EU:C:2023:957]** ESITO: dichiara ricevibile il rinvio, respinge i motivi di irricevibilità e include lo scoring decisivo nell'art. 22, par. 1, GDPR. PUNTO: punti 35-39 e 43-63.

[2] **Cassazione Civile, ordinanza 25 maggio 2021, n. 14381** ESITO: accoglie i primi quattro motivi, cassa la sentenza impugnata e rinvia al Tribunale di Roma per consenso nullo su algoritmo ignoto. PUNTO: paragrafi VII-VIII.

[3] **Corte costituzionale, ordinanza 21 luglio 2011, n. 218** ESITO: dichiara la manifesta inammissibilità della questione per difetto di legittimazione dell'Arbitro Bancario Finanziario, qualificandolo quale organo giustiziale amministrativo privo di poteri cogenti. PUNTO: considerato in diritto.

[4] **Consiglio di Stato, sentenza 8 aprile 2019, n. 2270** ESITO: accoglie l'appello e il ricorso di primo grado, qualificando il software decisorio quale atto amministrativo informatico soggetto a traduzione giuridica intellegibile e a pieno sindacato giurisdizionale. PUNTO: punti 8.2-9 della motivazione.

[5] **Consiglio di Stato, sentenza 13 dicembre 2019, n. 8472** ESITO: respinge l'appello ministeriale, affermando i principi di conoscibilità con inopponibilità del segreto del fornitore, non esclusività tramite intervento umano e non discriminazione algoritmica. PUNTO: punti 13.1-16 della motivazione.

[6] **Consiglio di Stato, sentenza 4 febbraio 2020, n. 881** ESITO: respinge l'appello, ribadendo la necessità dell'imputabilità umana della scelta autoritativa e dell'onere per l'amministrazione di provare tecnicamente il funzionamento algoritmico. PUNTO: punti 9-12 della motivazione.

[7] **T.A.R. Veneto, sentenza 21 ottobre 2025, n. 1845** ESITO: accoglie i ricorsi riuniti annullando la revoca automatizzata e il diniego di visto, affermando la riserva di legge ex art. 14 L. n. 132/2025. PUNTO: punti 6.2-6.3 e 9.

III. DOTTRINA RICHIAMATA

[D1] Urbani A., L'evoluzione della vigilanza ispettiva sulle banche al tempo della digitalizzazione del sistema finanziario e dell'avvento dell'intelligenza artificiale , in Rivista di Diritto Bancario , aprile-giugno 2026, fasc. II, pp. 85-111 – circolarità degli artt. 51, 53 e 54 TUB, passaggio all'audit digitale continuo, limiti delle serie storiche, sovranità sui grandi fornitori cloud e ispettore AI-assisted.

[D2] Morato C., AI as a Service (AIaaS): prime considerazioni intorno ad un nuovo contratto di impresa , in Contratto e impresa , 2026, n. 3, pp. 838-886 – qualificazione civilistica dei contratti AIaaS in cloud, raccordi con DORA artt. 3, 29 e 30, Circolare Banca d'Italia n. 285/2013, vendor lock-in e art. 13 Data Act.

[D3] De Gennaro C. , La responsabilità degli amministratori per l'intelligenza artificiale , in Metodo Giuridico , 5 maggio 2026 – analisi degli assetti organizzativi ex art. 2086 c.c. e della responsabilità gestoria nell'adozione di sistemi algoritmici.

[D4] Plakolli-Kasumi L., AI in the Banking Sector: Lessons from the Schufa Case , in Białostockie Studia Prawnicze , 2025, vol. 30, n. 3, pp. 155-166, DOI: 10.15290/bsp.2025.30.03.10 – corresponsabilità di agenzie di scoring e banche, inopponibilità del segreto commerciale e requisiti sostanziali dell'intervento umano.

[D5] Bonaccorsi di Patti E., Calabresi F., De Varti B., Federico F., Affinito M. et al., Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano , Banca d'Italia, Questioni di Economia e Finanza , n. 721, ottobre 2022 – indagine empirica su 38 modelli ML bancari, 0% XAI esterna, fairness through unawareness e doppio outsourcing.

[D6] Taraborrelli G., Megale L., Riserva di umanità nei procedimenti amministrativi automatizzati e effetto anticipatorio dell'AI Act , in Giornale di diritto amministrativo , 2026, n. 4, pp. 490-509 – distinzione tra riserva di umanità costituzionale e human oversight ex art. 14 AI Act, automation bias e calendario Digital Omnibus VII.

[D7] Palumbo F. , Intelligenza artificiale nella pubblica amministrazione: la legge n. 132/2025 , in Metodo Giuridico , 29 ottobre 2026 – ricostruzione dell'art. 14 L. n. 132/2025 su uso strumentale, conoscibilità e riserva di umanità.

[D8] Ripepi A., Trasparenza e accesso alle frontiere dell'amministrazione artificiale , in Giurisprudenza Italiana , agosto-settembre 2026, pp. 1946-1950 – AIxplainability tra conoscibilità e comprensibilità, tracciabilità ex art. 9 D.P.R. n. 62/2013 e rischio di influenza algoritmica occulta nelle attività preparatorie.

[D9] Gallone G., Orofino A. G., Il provvedimento algoritmico , in Giurisprudenza Italiana , agosto-settembre 2026, pp. 1935-1940 – inquadramento del software come instrumentum procedimentale, immedesimazione organica, patologie tra nullità e annullabilità e taratura periodica dei dati.

[D10] Speziale I., Le autorità nazionali per l'intelligenza artificiale. Prime riflessioni critiche , in Contratto e impresa , 2026, n. 2, pp. 320-333 – profili critici di indipendenza ex art. 70 AI Act della designazione governativa di AgID e ACN ex art. 20 L. n. 132/2025 e coordinamento con Banca d'Italia.

[D11] Hoang V. T., Nguyen N. M., When the EU AI Act Travels: Legal Transplantability and Modular Adaptation in Third-Country AI Governance , in Review of European and Comparative Law , 2026, vol. 66, n. 3, pp. 191-209, DOI: 10.31743/recl.20136 – valutazione della trapiantabilità modulare dell'AI Act in Regno Unito, Singapore, Giappone e Brasile.

[D12] Köteles Á., FinTech and Artificial Intelligence in Financial Services: Comparative Regulatory Challenges , in Perspectives of Law and Public Administration , 2026, vol. 15, n. 2, pp. 224-236, DOI: 10.62768/plpa/2026/15/2/03 – confronto tra modelli di vigilanza finanziaria in USA, Unione Europea e Asia-Pacifico e analisi dell'art. 74, par. 6, AI Act.

[D13] Sheehy B., Ng Y.-F., The Challenges of AI-Decision-Making in Government and Administrative Law: A Proposal for Regulatory Design , in Indiana Law Review , 2024, vol. 57, pp. 665-700, DOI: 10.18060/28360 – analisi del caso Robodebt, della scatola nera giuridica e della AI Golden Rule australiana.

[D14] Tan V., Paterson J., Webb J. S., Generative Artificial Intelligence in Small Value Consumer Claims: Hallucination Risk, System Design, and Governance in Online Dispute Resolution , in University of New South Wales Law Journal , 2025, vol. 48(4), pp. 1257-1288, DOI: 10.53637/qkhj4842 – tassi di allucinazione della GenAI e progettazione istituzionale dei sistemi ODR per consumatori.

FP

Federico Palumbo Avvocato del Foro di Roma

Si occupa di diritto civile, diritto amministrativo e diritto del lavoro. Per Metodo Giuridico firma approfondimenti e note a sentenza sui profili sostanziali e processuali del contenzioso civile e amministrativo.