

Le delibere del CSM sull'intelligenza artificiale nell'amministrazione della giustizia

di Giovanni Pascuzzi

[27 luglio 2026]

SOMMARIO. 1. Introduzione e tesi. – 2. La cornice normativa e il riparto di competenze. – 3. Da ottobre 2025 a luglio 2026: gli sviluppi e le garanzie tecniche. – 4. La riscrittura del perimetro: dodici voci, sette conferme, cinque aggiunte (e tre sparizioni). – 5. Il nodo: «fase analitica e ricostruttiva» o attività valutativa? – 6. La parabola dell'anonimizzazione. – 7. RAG, profilazione e indipendenza interna. – 8. Il contraddittorio: il convitato di pietra. – 9. Lo strumento e il criterio della sua scelta: Copilot come modello GPAI. – 10. Il contrappunto tecnico: la ricognizione della STO e il monito della prassi. – 11. Le condizioni cumulative e i loro corollari: formazione, supervisione bloccante, responsabilità. – 12. Il piano istituzionale: piattaforma dedicata, *sandbox*, gruppo tecnico. – 13. Ciò che l'aggiornamento lascia cadere. – 14. La natura delle raccomandazioni e il perimetro soggettivo. – 15. Conclusioni: le questioni aperte.

ABSTRACT. Il contributo analizza le due delibere con cui il Consiglio superiore della magistratura è intervenuto in materia di intelligenza artificiale nell'amministrazione della giustizia — quella dell'8 ottobre 2025 e l'aggiornamento del 22 luglio 2026 — assumendo come chiave di lettura il confine, tracciato dall'aggiornamento, tra «fase analitica e ricostruttiva del processo» e attività valutativa. La tesi sostenuta è che l'aggiornamento conserva l'approccio della cautela — e anzi lo irrigidisce sul piano redazionale, isolando per la prima volta gli usi non consentiti in un elenco autonomo — ma sul piano operativo sposta il confine dell'ammissibile in una zona che la delibera del 2025 aveva collocato fuori dall'ambito applicativo dell'art. 6, par. 3, del regolamento (UE) 2024/1689, senza fornire la motivazione di tale spostamento. Attorno a questo nodo si dispongono quattro profili ulteriori, tutti ricostruiti attraverso il confronto testuale fra i due documenti: la parabola dell'anonimizzazione, degradata da necessità a buona pratica; il divieto di profilazione mediante tecniche di *retrieval augmented generation* e la sua rilevanza per l'indipendenza interna; l'assenza di ogni riferimento al contraddittorio e alla parità informativa fra le parti; la qualificazione di Microsoft 365 Copilot come modello per finalità generali e il criterio con cui esso è stato prescelto. Si segnala infine ciò che l'aggiornamento lascia cadere: il registro, presente nel documento del 2025, che legava l'uso dell'intelligenza artificiale alla tutela del tempo della decisione e alla centralità dell'esperienza processuale.

1. Introduzione e tesi

Il presente contributo analizza le due delibere con cui il Consiglio superiore della magistratura è intervenuto in materia di intelligenza artificiale nell'amministrazione della giustizia: la delibera dell'8 ottobre 2025¹, recante le raccomandazioni originarie (di seguito, delib. 2025), e la delibera del 22 luglio 2026, che le

¹ CSM, delibera 8 ottobre 2025, *Raccomandazioni sull'uso dell'intelligenza artificiale nell'amministrazione della giustizia* (pratica n. 118/VV/2024).

Il testo si può trovare a questo indirizzo <https://www.csm.it/portale/web/csm-internet/w/raccomandazioni-intelligenza-artificiale>.

aggiorna (di seguito, delib. agg. 2026)². A distanza di poco più di nove mesi dalla prima, il Consiglio è tornato sul tema adottando un documento che esso stesso qualifica come integrazione e non come sostituzione: le raccomandazioni del 2025 *«costituiscono il quadro di riferimento vigente e conservano piena validità nei principi, nel perimetro normativo e nelle cautele operative ivi indicate»*, sicché *«l'odierno intervento consiliare, dunque, non le sostituisce ma le integra e aggiorna alla luce degli sviluppi tecnici, istituzionali e normativi intervenuti nel periodo compreso tra ottobre 2025 e maggio 2026»* [delib. agg. 2026, par. 1].

Il breve lasso di tempo trascorso tra i due atti è di per sé un dato significativo: segnala la velocità con cui la materia si sta evolvendo sul piano tecnico, su quello istituzionale e su quello normativo. Ma è anche la ragione per cui i due documenti possono essere letti come un unico testo stratificato, in cui le formule del 2025 restano formalmente in vigore mentre le formule del 2026 vi si sovrappongono: è nelle giunture fra i due strati che si annidano i problemi interpretativi di cui questo scritto intende occuparsi.

L'aggiornamento del 2026 conserva integro — e anzi irrigidisce sul piano redazionale — l'approccio della cautela: per la prima volta gli usi vietati sono isolati in un elenco autonomo, e il nucleo della funzione giurisdizionale è riaffermato con una nettezza che il testo del 2025 non aveva. Sul piano operativo, però, esso sposta il confine dell'ammissibile in una zona che la delibera del 2025 aveva espressamente collocato fuori dall'ambito applicativo dell'art. 6, par. 3, dell'AI Act; e lo fa per via di mera enunciazione, senza indicare le ragioni per cui le nuove attività ammesse ricadrebbero nella deroga. Non si tratta, dunque, né di una svolta dichiarata né di una mera conferma: si tratta di uno spostamento non tematizzato, che l'apparato di garanzie procedurali — supervisione bloccante, *prompt* strutturati, formazione — presidia senza però giustificarlo sul piano della qualificazione giuridica.

L'esposizione muove da una ricostruzione sintetica della cornice normativa (par. 2) e degli sviluppi che hanno condotto all'aggiornamento (par. 3), per poi affrontare, uno dopo l'altro, i nodi che il confronto testuale fra i due documenti fa emergere: la riscrittura dell'elenco degli usi consentiti (par. 4); la tenuta del confine tra ricostruzione e valutazione (par. 5); il regime dei dati e la sorte dell'anonimizzazione (par. 6); il divieto di profilazione (par. 7); l'assenza del contraddittorio (par. 8); lo strumento prescelto e il criterio della scelta (par. 9); le criticità tecniche documentate (par. 10); le condizioni cumulative e i loro corollari (par. 11); il piano istituzionale (par. 12); ciò che l'aggiornamento lascia cadere (par. 13); la natura giuridica delle raccomandazioni e il loro perimetro soggettivo (par. 14).

2. La cornice normativa e il riparto di competenze

Il riparto di competenze delineato dalla legge delega è la chiave di lettura di entrambi i documenti. L'art. 15 della l. 23 settembre 2025, n. 132 distribuisce le competenze su due piani distinti: il comma 2 assegna al Ministero della Giustizia la disciplina degli *«impieghi dei sistemi di intelligenza artificiale per*

² CSM, *Aggiornamento delle raccomandazioni sull'uso dell'intelligenza artificiale nell'amministrazione della giustizia, adottate con delibera dell'8 ottobre 2025* (pratica n. 118/VV/2024, rel. Cons. Eccher e Forziati, rel. esterno Cons. Bisogni), approvata nella seduta consiliare del 22 luglio 2026.

Una sintesi si può trovare a questo indirizzo <https://www.csm.it/portale/web/csm-internet/w/brevi-dal-plenum-41>.

Il testo si può trovare a questo indirizzo <https://www.csm.it/portale/web/csm-internet/ricerca-documenti-seduta?g=&tipologia=&fromDate=2026-07-22&toDate=2026-07-22&anno=%5B20260722000000+20260722235959%5D>

e in allegato all'articolo di Parodi citato nella bibliografia finale.

l'organizzazione dei servizi relativi alla giustizia, per la semplificazione del lavoro giudiziario e per le attività amministrative accessorie»; il comma 1 riserva invece al magistrato «ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti», nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria [delib. 2025, par. 3]. Organizzazione al Ministero, giurisdizione al magistrato: è entro questo schema che il Consiglio colloca il proprio intervento, e la delib. agg. 2026 ne trae la conseguenza in termini espliciti, riconoscendo che «spetta esclusivamente al Ministero della giustizia, ai sensi dell'art. 15, comma 2, della legge 23 settembre 2025, n. 132, individuare e autorizzare i sistemi di intelligenza artificiale utilizzabili negli uffici giudiziari» [delib. agg. 2026, par. 3].

Sul versante europeo, la delibera del 2025 ricostruisce la classificazione dell'amministrazione della giustizia fra i settori ad alto rischio e, nella nota 14, ne riporta il perimetro esatto: *«Il comma 8 dell'Allegato III [dell'AI Act: n.d.r.] indica come ad alto rischio “i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie”. Ma, nel contempo, il “considerando” 61 precisa che “Non è tuttavia opportuno estendere la classificazione dei sistemi di IA come ad alto rischio ai sistemi di IA destinati ad attività amministrative puramente accessorie che non incidono sull'effettiva amministrazione della giustizia nei singoli casi” e l'art. 6 §3 [del testo normativo dell'AI Act: n.d.r.] introduce limitazioni alla stessa classificazione come uso ad alto rischio: “In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale”»* [delib. 2025, nota 14].

È su questa deroga che poggia l'intervento del CSM. La delibera del 2025 ne enuncia le quattro condizioni alternative — *l'attività «a) sia limitata a compiti procedurali; b) migliori il risultato di un'attività umana già completata; c) rilevi schemi o deviazioni senza sostituire il giudizio umano; d) prepari un'attività valutativa da svolgersi con supervisione umana»* — e ne trae la nozione, destinata a governare tutto il seguito, di una *«zona grigia tra attività propriamente giudiziarie e attività organizzative o accessorie, rispetto alle quali l'utilizzo dell'IA può essere considerato compatibile con l'ordinamento vigente»* [delib. 2025, par. 3]. Va segnalato che il documento del 2025 individua altresì un secondo ambito ad alto rischio *«che, indirettamente, può intendersi riferito anche all'autorità giudiziaria»,* ossia i sistemi *«destinati ad essere utilizzati per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento dei reati, o per determinare il rischio di recidiva»* [delib. 2025, par. 2]; un rilievo di grande portata per il settore penale, che nessuno dei due documenti sviluppa oltre l'enunciazione.

Le fonti di cornice richiamate da entrambi i documenti comprendono la *«Carta etica europea sull'uso dell'Intelligenza Artificiale nei sistemi giudiziari e nel loro ambiente»* adottata dalla CEPEJ il 3 dicembre 2018, il regolamento generale sulla protezione dei dati (reg. UE 2016/679) e la Carta dei diritti fondamentali dell'Unione europea [delib. 2025, *«Richiamati»*; delib. agg. 2026, par. 2]. La sola delibera del 2025 richiama inoltre, fra l'altro, le *«Linee Guida per l'adozione dei sistemi di Intelligenza Artificiale nella Pubblica Amministrazione»*, pubblicate con Determinazione n. 17 del 17 febbraio 2025, il regolamento sui dati (UE) 2023/2854, il regolamento sulla governance dei dati (UE) 2022/868, la direttiva NIS2 (UE) 2022/2555, il d.lgs. n. 196 del 2003 e il codice dell'amministrazione digitale.

Quanto al termine per l'obbligo di certificazione, la delibera del 2025 individuava nell'agosto 2026 la data «dalla quale gli unici sistemi di intelligenza artificiale che potranno essere utilizzati dai magistrati nell'esercizio dell'attività giudiziaria (ovvero “nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti”), conformemente al diritto UE, saranno solo quelli a marcatura CE, ovvero quelli che avranno ottenuto una positiva valutazione di conformità e saranno iscritti nella relativa banca dati dell'Unione Europea» [delib. 2025, par. 2]. L'aggiornamento dà atto che, «in data 7 maggio 2026, il Consiglio dell'Unione Europea e il Parlamento europeo hanno raggiunto un accordo provvisorio nell'ambito del cd. Digital Omnibus on AI, che posticipa di 16 mesi — dal 2 agosto 2026 al 2 dicembre 2027 — l'entrata in vigore degli obblighi per i sistemi ad alto rischio autonomi classificati nell'allegato III (categoria che ricomprende espressamente i sistemi destinati all'amministrazione della giustizia)», precisando che «l'accordo è provvisorio e deve ancora essere formalmente adottato dalle istituzioni europee competenti» [delib. agg. 2026, par. 6]³.

La motivazione del rinvio è di natura tecnica: «le specifiche tecniche armonizzate su cui i fornitori avrebbero dovuto basarsi per dimostrare la conformità dei propri sistemi non sono state completate e la Commissione europea deve ancora provvedere all'emanazione delle linee guida di classificazione ai sensi dell'art. 6 dell'AI Act (originariamente previste per febbraio 2026)», sicché «imporre gli obblighi di conformità alla data originaria avrebbe significato richiedere agli operatori di costruire un'architettura di conformità rispetto a standard non ancora esistenti» [delib. agg. 2026, par. 6]. Il Consiglio ne trae tre conseguenze concorrenti, che vale la pena riportare perché ne definiscono la postura complessiva: «in primo luogo, i principi di legalità, trasparenza, autonomia decisionale e protezione dei dati che governano l'uso dell'intelligenza artificiale in ambito giudiziario trovano il loro fondamento nei principi costituzionali e nelle garanzie del giusto processo, indipendentemente dalle scadenze regolamentari europee; in secondo luogo, la nuova scadenza del 2 dicembre 2027 è stata indicata come definitiva (avendo le istituzioni europee segnalato con chiarezza che non sarà oggetto di ulteriori proroghe); in terzo luogo, il tempo aggiuntivo deve essere utilizzato produttivamente per costruire l'infrastruttura tecnica e organizzativa necessaria, non per differire gli sforzi di adeguamento» [delib. agg. 2026, par. 6].

È un passaggio importante, perché sottrae le cautele consiliari alla loro origine regolamentare e le ancora a un fondamento costituzionale: se i principi valgono «indipendentemente dalle scadenze regolamentari europee», la proroga non libera alcuno spazio operativo. Il che rende tanto più necessario verificare se l'ampliamento del perimetro disposto dallo stesso documento sia coerente con quella premessa.

³ Successivamente alla delibera qui commentata l'accordo è stato formalizzato: il regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio dell'8 luglio 2026, recante modifica dei regolamenti (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (Omnibus digitale sull'IA), è stato pubblicato nella Gazzetta ufficiale dell'Unione europea del 24 luglio 2026 ed è entrato in vigore il 27 luglio 2026. Il nuovo art. 113, terzo comma, lett. c), del regolamento (UE) 2024/1689 conferma la data indicata dal Consiglio, disponendo che il capo III, sezioni 1, 2 e 3, «si applica a decorrere dal: i) 2 dicembre 2027 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III; e ii) 2 agosto 2028 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, e dell'allegato I». L'art. 6, par. 3, sul quale poggia l'impianto delle raccomandazioni del CSM, non è stato modificato.

3. Da ottobre 2025 a luglio 2026: gli sviluppi e le garanzie tecniche

L'aggiornamento individua espressamente «quattro ordini di sviluppi» che ne giustificano l'adozione.

Il primo è «l'avvio, dal 1° gennaio 2026, della sperimentazione di Microsoft 365 Copilot negli uffici giudiziari, disposta dal Dipartimento per l'innovazione tecnologica della giustizia, che ha reso urgente un chiarimento sui confini dell'uso consentito dello strumento, con particolare riferimento al trattamento degli atti giudiziari».

Il secondo è «l'acquisizione, a seguito delle richieste formulate dal Comitato Paritetico tra il Consiglio superiore della magistratura e il Ministero della giustizia nella seduta del 20 gennaio 2026, delle rassicurazioni tecniche di Microsoft in ordine alla riservatezza dei dati, all'assenza di addestramento dei modelli sui dati giudiziari e all'architettura di sistema adottata per il dominio giustizia».

Il terzo è «la ricognizione svolta dalla struttura tecnica per l'organizzazione del Consiglio superiore (STO) sugli usi dell'intelligenza artificiale negli uffici giudiziari (trasmessa alla settima commissione e al coordinatore del Comitato Paritetico il 29 aprile 2026), che ha dato conto tanto delle criticità strutturali dello strumento quanto delle sperimentazioni più avanzate condotte da alcuni uffici giudiziari».

Il quarto è «il riscontro del Dipartimento per l'innovazione tecnologica della giustizia del 10 maggio 2026, con cui il Capo del Dipartimento ha condiviso alcune delle valutazioni della STO e comunicato l'avvio di un approccio “multimodello”, con l'istituzione di uno sportello tecnico dedicato agli utenti della sperimentazione» [delib. agg. 2026, par. 1].

Le garanzie tecniche comunicate dal Ministero «con comunicazione formale del 12 febbraio 2026» riguardano quattro profili.

La «residenza dei dati in Italia», assicurata dal componente Advanced Data Residency (acquisito dal Ministero della Giustizia), che «garantisce la memorizzazione dei dati, inclusi i contenuti delle interazioni con Copilot, nei datacenter localizzati in Italia; la posizione dei dati è verificabile direttamente dal tenant attraverso il Microsoft 365 Admin Center».

L'«isolamento del tenant»: quello ministeriale «costituisce un'istanza logicamente separata da tutti gli altri tenant Microsoft 365, con dati protetti sulla base delle politiche di sicurezza, conformità e privacy proprie dell'organizzazione».

L'«assenza di addestramento sui dati giudiziari»: «i dati dei clienti – compresi i prompt inseriti dagli utenti, le risposte generate e i dati accessibili tramite Microsoft Graph – non vengono utilizzati per l'addestramento o il miglioramento dei modelli linguistici di Copilot; tali dati restano confinati all'interno del tenant e sono trattati esclusivamente per l'erogazione del servizio».

Il «controllo sulla classificazione dei documenti»: il Ministero «può classificare i documenti sensibili tramite etichette di riservatezza (Microsoft Purview) al fine di limitare o inibire l'elaborazione dei contenuti da parte di Copilot, e può configurare o disabilitare la funzionalità di ricerca web» [delib. agg. 2026, par. 3].

La formula con cui il Consiglio registra tali garanzie merita attenzione per la sua cautela sintattica: «*Il Consiglio non può che prendere atto di tali garanzie, le quali modificano il quadro di valutazione rispetto a quello disponibile al momento dell'adozione delle raccomandazioni dell'8 ottobre 2025*» [delib. agg. 2026, par. 3]. «Non può che prendere atto» non è «valuta», né «verifica»: è la constatazione di un dato acquisito da altri, coerente con il riconoscimento — reso nel periodo immediatamente successivo — che l'individuazione e l'autorizzazione dei sistemi spettano «*esclusivamente al Ministero della giustizia*». Il Consiglio, in altri termini, dichiara di non disporre né del titolo né degli strumenti per un accertamento autonomo delle assicurazioni fornite dal fornitore. È una premessa che pesa su tutto ciò che segue.

Va aggiunto un elemento che l'aggiornamento riporta e che ne attenua il tono rassicurante: la nota del Dipartimento del 10 maggio 2026 è quella con cui il Capo del Dipartimento «*ha riconosciuto che un impiego non accompagnato di Copilot in ambito giudiziario presenta margini di rischio che devono essere governati con misure mirate, e ha comunicato che il Ministero sta recependo le segnalazioni emerse nel corso della sperimentazione, apportando i correttivi tecnici e organizzativi necessari*» [delib. agg. 2026, par. 3]. L'ammissione proviene dall'organo che ha disposto la sperimentazione e che, secondo la stessa delibera, è l'unico titolare del potere di autorizzazione: la sperimentazione, dunque, procede mentre il suo promotore ne riconosce i «margini di rischio» e ne annuncia i «correttivi».

4. La riscrittura del perimetro: dodici voci, sette conferme, cinque aggiunte (e tre sparizioni)

La delibera del 2025 aveva individuato un elenco di impieghi ammissibili nella fase transitoria, «*purché in modalità tracciata, sicura e con revisione umana e nell'ambito degli applicativi forniti all'interno del dominio giustizia*», e ne aveva espressamente dichiarato la natura aperta: «*si tratta di un'elencazione non esaustiva*» [delib. 2025, par. 3]. Le voci erano dodici. L'aggiornamento del 2026, nel paragrafo dedicato al «*raccordo con le raccomandazioni consiliari dell'8 ottobre 2025*», dispone che «*l'elenco di cui al paragrafo 4 delle raccomandazioni è confermato e ampliato*», e ne offre una nuova redazione in dodici punti, chiusa dalla precisazione: «*I punti da 1 a 7 erano già previsti dalle raccomandazioni dell'8 ottobre 2025; i punti da 8 a 12 costituiscono le nuove attività ammesse dal presente aggiornamento in ragione delle garanzie tecniche acquisite*» [delib. agg. 2026, par. 8].

L'operazione è, dunque, duplice: dodici voci del 2025 sono riportate a sette, e a queste se ne aggiungono cinque nuove. La prima parte dell'operazione — la compressione — non è dichiarata, e merita di essere verificata voce per voce, perché non si risolve in una mera riscrittura sintetica.

Sono confermate, in forma accorpata, le seguenti voci del 2025: le «*ricerche dottrinali*» (n. 1), la «*sintesi di provvedimenti ostensibili e contributi dottrinali*» (n. 2), l'«*organizzazione del lavoro giudiziario*» (n. 3, che assorbe anche la «*predisposizione di calendari d'udienza*» già autonoma al n. 11), il «*supporto agli uffici c.d. "affari semplici"*» (n. 4), la «*revisione linguistica e stilistica di testi*» (n. 9), la «*produzione di tabelle e grafici*» (n. 8, che assorbe la «*generazione automatica di presentazioni (slides)*» di cui al n. 7, ora ricompresa nella formula «*materiali illustrativi*») e la «*traduzione assistita*» (n. 12).

Non compaiono più, invece, tre voci del 2025: il n. 5, ossia il «*Supporto ad attività giurisdizionali gestionali attraverso il controllo della documentazione (soprattutto contabile nonché delle certificazioni) prodotta in atti ove opportunamente anonimizzata*»; il n. 6, ossia il «*Confronto tra soluzioni tecniche per la gestione fascicoli: comparazione automatizzata di pratiche e prassi organizzative, anche tra diversi uffici, per*

individuare criticità o buone pratiche replicabili»; e il n. 10, ossia la «Catalogazione e archiviazione per materia dei quesiti ai CTU: organizzazione delle richieste per parola chiave o categoria tematica per facilitarne la consultazione e il riuso». Cade inoltre, all'interno della voce sull'organizzazione del lavoro giudiziario, la «comparazione automatizzata di documenti» che il 2025 vi includeva espressamente.

Come vadano intese tali omissioni è questione che il testo non risolve. Esistono, però, alcuni elementi utili a delineare una traccia interpretativa. Da un lato, l'elenco è dichiarato *«confermato e ampliato»*, il che esclude un intento abrogativo; dall'altro, la clausola di chiusura dispone che *«per ogni profilo non espressamente modificato dal presente documento, continuano ad applicarsi integralmente le raccomandazioni consiliari dell'8 ottobre 2025»* [delib. agg. 2026, par. 8], e la natura dell'elenco resta, in entrambe le versioni, dichiaratamente aperta (*«si tratta di un'elencazione non esaustiva»*, nel 2025; *«a titolo esemplificativo e non esaustivo»*, nel 2026). La lettura corretta è dunque che le tre voci sopravvivano. Ma la tecnica redazionale prescelta — la riscrittura integrale dell'elenco in luogo dell'integrazione per aggiunta — genera un'incertezza evitabile in un documento la cui funzione dichiarata è precisamente quella di *«chiarimento sui confini dell'uso consentito dello strumento»* [delib. agg. 2026, par. 1].

Un dettaglio, in questa vicenda, non è privo di significato: fra le voci scomparse, il n. 5 del 2025 era l'unica che subordinasse espressamente l'ammissibilità dell'impiego alla condizione che la documentazione fosse *«opportunamente anonimizzata»*. Ne riparleremo al par. 6.

Le cinque voci nuove sono invece dichiarate come tali: *«8. classificazione e categorizzazione degli atti processuali per tipologia e funzione; 9. analisi strutturata del contenuto degli atti delle parti ai fini della ricostruzione delle posizioni processuali; 10. sintesi documentale di atti giudiziari, per finalità di classificazione e archiviazione tematica; 11. confronto tra posizioni processuali delle parti, ai fini della individuazione del thema decidendum e del thema probandum; 12. compilazione assistita di atti standardizzati e di moduli (quali i mandati di arresto europeo), con supervisione e completamento obbligatori da parte del magistrato»* [delib. agg. 2026, par. 8].

Che tali voci non siano ipotesi di scuola risulta dallo stesso documento, che indica la propria base empirica nelle *«sperimentazioni più avanzate – in particolare quelle condotte dal Tribunale civile di Catania e dalla Procura generale di Perugia»* [delib. agg. 2026, par. 5], e che di esse dà una valutazione favorevole, *«quale fattivo contributo al migliore adattamento dell'applicativo Copilot alle esigenze della funzione giudiziaria, auspicando che ne siano presto autorizzate altre e che i risultati vengano messi a disposizione di tutti gli uffici giudiziari come modelli replicabili e base per la progettazione della suite dedicata»* [delib. agg. 2026, par. 7]. Il richiamo esplicito all'esperienza catanese come modello dei *«flussi di lavoro strutturati»* [delib. agg. 2026, par. 4] e la menzione dei *«mandati di arresto europeo»* quale esempio di atto standardizzato al nuovo n. 12 consentono di ricondurre le nuove voci, rispettivamente, alle due sperimentazioni citate. L'aggiornamento, in altri termini, non innova in astratto: codifica e generalizza prassi già in corso, di cui la ricognizione della STO ha potuto verificare — come si vedrà al par. 10 — tanto le potenzialità quanto i limiti.

Tavola 1 - L'elenco degli usi consentiti: corrispondenze, accorpamenti, sparizioni e aggiunte

Delibera 8 ottobre 2025 (par. 4)	Delibera 22 luglio 2026, aggiornamento (par. 8)
1. «Ricerche dottrinali: assistenza nella consultazione di banche dati e nella costruzione di stringhe di ricerca finalizzate all'individuazione di dottrina pertinente.»	1. «ricerche dottrinali e supporto alla consultazione di banche dati;»
2. «Sintesi di provvedimenti ostensibili e contributi dottrinali: creazione di abstract per la classificazione e l'archiviazione tematica di decisioni e saggi, anche in vista dell'elaborazione di banche dati giurisprudenziali interne all'ufficio.»	2. «sintesi di provvedimenti ostensibili e contributi dottrinali per finalità di classificazione e archiviazione tematica;»
3. «Organizzazione del lavoro giudiziario: supporto nella redazione di report statistici sull'andamento dell'ufficio; analisi di conformità tra programmi di gestione e dati di registro; comparazione automatizzata di documenti; redazione di bozze di relazioni o pareri su incarichi direttivi e semidirettivi; gestione dei calendari d'udienza sulla base di carichi e scadenze.» 11. «Predisposizione di calendari d'udienza: generazione automatizzata degli orari e dell'agenda sulla base dei criteri predefiniti e dei carichi di lavoro.»	3. «supporto all'organizzazione e alla gestione degli uffici giudiziari: report statistici, analisi di conformità tra programmi di gestione e dati di registro, redazione di bozze di relazioni su incarichi direttivi e semidirettivi, gestione dei calendari d'udienza;» [la voce assorbe la n. 11 del 2025; cade la «comparazione automatizzata di documenti»]
4. «Supporto agli uffici c.d. “affari semplici”: ausilio nelle attività seriali e a bassa complessità giuridica con la redazione di bozze standardizzate da adattare poi al caso specifico dal magistrato o dai suoi collaboratori.»	4. «supporto agli uffici cd. “affari semplici” per attività seriali e a bassa complessità giuridica;»
5. «Supporto ad attività giurisdizionali gestionali attraverso il controllo della documentazione (soprattutto contabile nonché delle certificazioni) prodotta in atti ove opportunamente anonimizzata.»	— voce non riprodotta
6. «Confronto tra soluzioni tecniche per la gestione fascicoli: comparazione automatizzata di pratiche e prassi organizzative, anche tra diversi uffici, per individuare criticità o buone pratiche replicabili.»	— voce non riprodotta
9. «Revisione linguistica e stilistica di testi: rilettura di bozze per verificarne la coerenza sintattica, ortografica e la chiarezza espositiva.»	5. «revisione linguistica e stilistica di testi;»
7. «Generazione automatica di presentazioni (slides): creazione di materiali illustrativi a partire da documenti giuridici o relazioni, per attività formative o divulgative.» 8. «Produzione di tabelle e grafici: estrazione di dati dai registri, organizzazione in tabelle, analisi comparativa e rappresentazione grafica per fini organizzativi o conoscitivi.»	6. «produzione di tabelle, grafici e materiali illustrativi;» [la voce assorbe la n. 7 del 2025 nella formula «materiali illustrativi»]
10. «Catalogazione e archiviazione per materia dei quesiti ai CTU: organizzazione delle richieste per parola chiave o categoria tematica per facilitarne la consultazione e il riuso.»	— voce non riprodotta
12. «Traduzione assistita: uso dell'IA per traduzioni preliminari di testi giuridici, da sottoporre sempre a verifica umana.»	7. «traduzione assistita di testi giuridici, con verifica umana obbligatoria;»
—	8. «classificazione e categorizzazione degli atti processuali per tipologia e funzione;» [nuova]
—	9. «analisi strutturata del contenuto degli atti delle parti ai fini della ricostruzione delle posizioni processuali;» [nuova]
—	10. «sintesi documentale di atti giudiziari, per finalità di classificazione e archiviazione tematica;» [nuova]
—	11. «confronto tra posizioni processuali delle parti, ai fini della individuazione del thema decidendum e del thema probandum;» [nuova]
—	12. «compilazione assistita di atti standardizzati e di moduli (quali i mandati di arresto europeo), con supervisione e completamento obbligatori da parte del magistrato.» [nuova]

Simmetricamente, l'aggiornamento isola per la prima volta gli usi vietati in un elenco autonomo: «*Con riferimento agli usi non consentiti, rimangono in ogni caso esclusi dall'uso di strumenti di intelligenza artificiale: 1. la formulazione del dispositivo e l'affidamento della redazione dei provvedimenti giurisdizionali; 2. l'uso di sistemi di intelligenza artificiale generativa non autorizzati dal Ministero della giustizia e al di fuori del sistema giustizia*» [delib. agg. 2026, par. 8]. È, sul piano redazionale, un irrigidimento: nel 2025 il divieto era desumibile dal contesto, ora è enunciato. Ma è anche un elenco assai più breve del catalogo degli usi ammessi, e formulato per fattispecie: le due voci descrivono condotte determinate — far redigere il provvedimento alla macchina, ricorrere a sistemi non autorizzati — mentre il divieto di principio resta quello enunciato al par. 2, dove «*rimane in ogni caso escluso qualsiasi uso dell'intelligenza artificiale che si traduca nell'adozione o nella predisposizione di provvedimenti giurisdizionali, nella valutazione autonoma delle prove o nella formazione del convincimento del giudice*». Fra i due poli — il nucleo giurisdizionale, in ogni caso precluso, e le dodici attività espressamente consentite — resta però una zona intermedia che nessuno dei due elenchi copre: quella delle attività strumentali non nominate, che quel nucleo non toccano ma possono avvicinarvisi. A governarla l'aggiornamento pone un criterio soltanto, la riconducibilità dell'impiego alla «*fase analitica e ricostruttiva del processo*»; ed è su questa formula che conviene ora soffermarsi.

5. Il nodo: «*fase analitica e ricostruttiva*» o attività valutativa?

Il criterio esiste, ed è enunciato nel paragrafo che apre l'ampliamento. Il Consiglio ritiene che l'uso di Copilot possa essere esteso «*in via sperimentale e nel rispetto delle condizioni indicate al paragrafo seguente, anche ad attività che coinvolgono atti giudiziari, nella misura in cui tali attività siano riconducibili alla fase analitica e ricostruttiva del processo e non incidano sulle valutazioni giuridiche, interpretative o decisionali*» [delib. agg. 2026, par. 4]. La distinzione fra «*fase analitica e ricostruttiva*» e «*valutazioni giuridiche, interpretative o decisionali*» è dunque il perno dell'intera operazione: è essa a stabilire quali attività restino nella «*zona grigia*» dell'art. 6, par. 3, e quali ricadano invece nel regime dei sistemi ad alto rischio.

Il dubbio si concentra sul nuovo n. 11: il «*confronto tra posizioni processuali delle parti, ai fini della individuazione del thema decidendum e del thema probandum*». L'individuazione del *thema decidendum* non è operazione descrittiva: è l'atto con cui il giudice determina l'oggetto del giudizio, seleziona le questioni rilevanti, qualifica giuridicamente le domande e le eccezioni. È, per definizione, «*interpretazione dei fatti e del diritto*», ossia esattamente ciò che l'Allegato III, comma 8, dell'AI Act descrive quando qualifica come ad alto rischio «*i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti*» [delib. 2025, nota 14]. Considerazioni analoghe, ancorché meno stringenti, valgono per il nuovo n. 9, ossia l'«*analisi strutturata del contenuto degli atti delle parti ai fini della ricostruzione delle posizioni processuali*».

Che il rilievo non sia estraneo alla logica dei documenti del CSM lo dimostra il fatto che la delibera del 2025 aveva già affrontato un problema strutturalmente identico, e lo aveva risolto in senso opposto. A proposito delle ricerche sulle banche dati giurisprudenziali, essa aveva distinto con precisione: l'intelligenza artificiale «*può validamente assistere il magistrato nella consultazione delle banche dati istituzionali e commerciali, nella costruzione di stringhe di ricerca complesse e nella classificazione tematica del materiale reperito. In questo caso, l'attività si configura come supporto tecnico-organizzativo,*

riconducibile ai compiti procedurali limitati ai sensi dell'art. 6, par. 3, lett. a) del Regolamento UE 1689/2024. Tuttavia, laddove i sistemi siano progettati per selezionare automaticamente la giurisprudenza "più rilevante", per suggerire orientamenti interpretativi prevalenti o per generare schemi motivazionali basati su pattern ricorrenti, si configura un impiego che incide potenzialmente sull'attività valutativa e sull'indirizzo giuridico, e dunque si esce dall'ambito dell'art. 6, par. 3» [delib. 2025, par. 3].

Il confronto fra i due passaggi è istruttivo. Nel 2025, la selezione automatica del precedente «più rilevante» esce dall'ambito della deroga perché *«incide potenzialmente sull'attività valutativa»*; e la ragione è enunciata in termini generali: *«L'automazione della ricerca non può sostituire la sensibilità giuridica necessaria alla contestualizzazione del precedente»* [delib. 2025, par. 3]. Nel 2026, l'individuazione automatizzata del *thema decidendum* — operazione che incide sull'oggetto stesso del giudizio, non sul materiale di supporto — resta invece dentro la deroga, perché appartiene alla *«fase analitica e ricostruttiva»*. Il criterio del 2025 è più severo di quello applicato nel 2026 a un'attività situata più vicino alla decisione.

Né vale obiettare che il rischio sia neutralizzato dalla riserva del nucleo giurisdizionale. Quella riserva è formulata dalla delibera del 2026 nei termini più netti — *«Rimane in ogni caso escluso qualsiasi uso dell'intelligenza artificiale che si traduca nell'adozione o nella predisposizione di provvedimenti giurisdizionali, nella valutazione autonoma delle prove o nella formazione del convincimento del giudice: tali attività – che costituiscono il nucleo della funzione giurisdizionale – sono e restano di esclusiva competenza del magistrato»* [delib. agg. 2026, par. 2] —, ma opera su un piano diverso. Il divieto colpisce la sostituzione; il problema posto dal n. 11 è invece quello dell'ancoraggio: un magistrato che riceva dal sistema una ricostruzione strutturata del *thema decidendum* non delega la decisione, ma parte da un perimetro che non ha costruito. È il fenomeno che la stessa delibera del 2025 aveva nominato, quando raccomandava di preservare *«la possibilità di resistere alla macchina (riconoscendone gli errori ed evitando il c.d. automation bias)»* [delib. 2025, par. 5].

Vi è, infine, un argomento testuale che rende la questione ineludibile. La delibera del 2026 afferma che *«l'eventuale futura estensione dell'intelligenza artificiale a fasi più prossime alla decisione sarà possibile esclusivamente mediante sistemi certificati ai sensi dell'AI Act, la cui scadenza per i sistemi dell'allegato III è ora fissata al 2 dicembre 2027»* [delib. agg. 2026, par. 2]. Il Consiglio, dunque, sa che l'avvicinamento alla decisione richiede la certificazione, e la rinvia al futuro. La domanda che il documento non si pone è se il nuovo n. 11 non rientri già, esso stesso, fra quelle *«fasi più prossime alla decisione»*.

6. La parabola dell'anonimizzazione

Il secondo nodo riguarda il regime dei dati, ed è quello in cui la distanza fra i due documenti è massima — pur essendo, formalmente, quello in cui il 2026 dichiara di non innovare, avendo affermato che le raccomandazioni del 2025 *«conservano piena validità nei principi, nel perimetro normativo e nelle cautele operative ivi indicate»* [delib. agg. 2026, par. 1].

La cautela operativa del 2025 in materia di protezione dei dati era formulata come divieto: *«nei sistemi IA non vanno immessi dati sensibili, riservati o soggetti a segreto investigativo, anche in forma indiretta. È importante, in particolare, considerare il rischio di reidentificazione dei dati, ancorché anonimizzati o pseudonimizzati, ad opera dell'IA attraverso l'incrocio di dataset. Occorre, in ogni caso, immettere nei sistemi di IA solo le informazioni necessarie»* [delib. 2025, par. 4]. Coerentemente, il documento

concludeva che «*pur dovendosi escludere l'immissione di dati sensibili di atti processuali su dispositivi di IA generalista occorre fornire per tempo un'alternativa: progettare un sistema interno di IA che possa essere gradualmente utilizzato a partire da agosto 2026*» [delib. 2025, par. 4].

La regola del 2026 è di segno opposto: «*l'immissione di atti giudiziari contenenti dati personali nel sistema Copilot è consentita all'interno del tenant istituzionale del Ministero della giustizia, in ragione delle garanzie tecniche acquisite in ordine alla residenza dei dati in Italia, all'isolamento del tenant e all'assenza di addestramento dei modelli sui dati giudiziari. L'anonimizzazione preventiva degli atti è raccomandata quale buona pratica, in particolare quando non sia strettamente necessario che il sistema operi su dati identificativi per il conseguimento della finalità perseguita; in quest'ottica appare urgente la diffusione di adeguato software per l'anonimizzazione degli atti*» [delib. agg. 2026, par. 4].

Tre osservazioni si impongono. La prima è che l'anonimizzazione passa da presupposto a «*buona pratica*», e dunque cessa di essere condizione di ammissibilità: fra le cinque condizioni cumulative enumerate dal paragrafo 4, essa non figura. La seconda è che il periodo si chiude con un'ammissione notevole — «*appare urgente la diffusione di adeguato software per l'anonimizzazione degli atti*» —, la quale spiega, senza dirlo, perché l'anonimizzazione non possa essere imposta: lo strumento tecnico per praticarla su larga scala non è ancora disponibile. Il Consiglio, cioè, degrada a raccomandazione una cautela la cui attuazione risulta oggi materialmente impraticabile, e nel farlo consente proprio ciò che, in mancanza di quello strumento, la cautela mirava a evitare. La terza è che la questione della reidentificazione — il rischio, evocato dal 2025, che l'incrocio di dataset vanifichi anonimizzazione e pseudonimizzazione — scompare del tutto dal documento del 2026: non è superata, non è discussa, semplicemente non è più menzionata.

Vi è, poi, un'antinomia più radicale, e anch'essa interamente ricavabile dai testi. La delibera del 2025 aveva escluso in via di principio che garanzie di fonte negoziale potessero risolvere il problema: «*L'adozione di misure contrattuali ritenute idonee a garantire la riservatezza dei dati con operatori commerciali non appare soluzione soddisfacente. Occorre, infatti, garantire la sicurezza della rete, valutando l'utilizzo di modelli residenti su server sotto il controllo del ministero o l'uso di modelli (anche) open source in locale su hardware in dotazione ai magistrati*» [delib. 2025, par. 4]. L'apertura del 2026 poggia invece, per intero, su un insieme di assicurazioni provenienti dal fornitore e trasmesse dal Ministero: le «*rassicurazioni tecniche di Microsoft*» [delib. agg. 2026, par. 1], di cui il Consiglio «*non può che prendere atto*» [delib. agg. 2026, par. 3]. Non si tratta di rilevare una contraddizione formale — le garanzie del 2026 sono di natura architeturale, non solo negoziale, e riguardano la residenza dei dati e l'isolamento del *tenant*, non la sola riservatezza —, ma di osservare che il criterio enunciato nel 2025 (non fidarsi delle garanzie dell'operatore commerciale, ma controllare l'infrastruttura) non è stato né soddisfatto né espressamente abbandonato.

Manca infine, in entrambi i documenti, ogni riferimento alla disciplina eurounitaria della protezione dei dati sul piano procedimentale. Il GDPR è richiamato quale fonte di cornice — l'uso dell'intelligenza artificiale deve avvenire nel rispetto «*del GDPR (regolamento generale sulla protezione dei dati, Reg. UE 2016/679)*» [delib. agg. 2026, par. 2] —, ma nulla è detto sulla base giuridica del trattamento consistente nell'immissione di atti giudiziari in un sistema generativo, sul regime dei dati di cui agli artt. 9 e 10 del regolamento, sulla valutazione d'impatto ex art. 35 e sulla eventuale consultazione preventiva dell'autorità di controllo.

7. RAG, profilazione e indipendenza interna

Fra i «*principi irrinunciabili che governano l'uso dell'intelligenza artificiale in ambito giudiziario*», l'aggiornamento del 2026 include, accanto all'autonomia decisionale e alla supervisione umana, il «*divieto di profilazione*», così formulato: «*va escluso il rischio che tecniche di retrieval augmented generation (RAG) applicate ad archivi digitali della giustizia si traducano nella creazione di repository idonei a consentire forme di profilazione dell'attività giudiziaria e dei singoli magistrati*» [delib. agg. 2026, par. 2]. Il principio riprende, quasi alla lettera, il corrispondente passaggio del 2025: «*Si deve, inoltre, escludere il rischio che con la tecnica del retrieval augmented generation (RAG) su archivi digitali della giustizia possa tradursi nella creazione di repository idonei a consentire forme di invasiva profilazione dell'attività giudiziaria e dei singoli magistrati*» [delib. 2025, par. 4].

È il passaggio di maggiore spessore costituzionale dei due documenti, e insieme il meno sviluppato. La profilazione qui evocata non è quella dell'utente-cittadino, ma quella del magistrato: la costruzione, a partire dagli archivi della giustizia, di rappresentazioni statistiche degli orientamenti individuali. Il bene protetto non è la riservatezza, ma l'indipendenza.

Il principio, tuttavia, resta allo stato di enunciazione. Nessuno dei due documenti indica chi debba accertarne il rispetto, con quali strumenti, né quali misure tecniche o organizzative valgano a impedire che l'archiviazione degli output — che la delibera del 2026 anzi presuppone, quando fra le nuove attività ammesse elenca la «*sintesi documentale di atti giudiziari, per finalità di classificazione e archiviazione tematica*» [delib. agg. 2026, par. 8] — si traduca proprio nella formazione di quei repository. Vi è, anzi, una tensione interna: le voci nn. 8, 9, 10 e 11 del nuovo elenco descrivono attività che producono, per loro natura, materiale strutturato e indicizzabile sugli atti e sulle posizioni processuali; la garanzia contro il loro uso profilante è affidata a un divieto di risultato, non a un vincolo di architettura.

Il paradosso è che proprio la richiesta di una piattaforma dedicata — su cui il Consiglio insiste in entrambi i documenti (par. 12) — offrirebbe la sede naturale per tradurre il divieto in requisito tecnico, secondo il modello che il documento del 2026 evoca quando chiede sistemi «*dotati di governance specifica, tracciabilità delle fonti, verificabilità degli output e possibilità di controllo ex post delle elaborazioni effettuate*» [delib. agg. 2026, par. 5]. Ma la «*possibilità di controllo ex post delle elaborazioni effettuate*» è essa stessa, se non presidiata, una capacità di sorveglianza: la stessa funzione che garantisce la verificabilità dell'operato del sistema consente di ricostruire l'operato del magistrato che lo ha interrogato. Chi controlla i log, e per quali finalità, è questione che nessuno dei due documenti pone.

8. Il contraddittorio: il convitato di pietra

Fra le condizioni di compatibilità dell'intelligenza artificiale con la funzione giurisdizionale, la delibera del 2025 ne enunciava quattro, in un passaggio delle premesse che vale la pena riportare per intero: «*l'introduzione di sistemi di intelligenza artificiale in ambito giudiziario può essere considerata compatibile con la funzione giurisdizionale soltanto nella misura in cui tali strumenti siano integrati nel rispetto dei principi fondamentali del diritto processuale. In particolare, devono essere garantiti la trasparenza dell'elaborazione algoritmica, la possibilità di verifica e contestazione degli output, la subordinazione all'autonomia valutativa del giudice, e la parità informativa tra le parti. Solo un utilizzo conforme a tali requisiti potrà risultare coerente con i principi di legalità, giusto processo e tutela effettiva, su cui si fonda la giurisdizione in uno Stato di diritto*» [delib. 2025, premessa].

Delle quattro condizioni, l'aggiornamento del 2026 sviluppa esclusivamente la terza. La «*subordinazione all'autonomia valutativa del giudice*» è ribadita e rafforzata; la trasparenza dell'elaborazione algoritmica è degradata a problema tecnico dello strumento («*carenza di grounding documentale*»); la «*possibilità di verifica e contestazione degli output*» e la «*parità informativa tra le parti*» scompaiono.

La scomparsa non è indolore, perché è proprio l'aggiornamento a rendere quelle due condizioni attuali. Fintanto che l'intelligenza artificiale era confinata ad attività organizzative — report statistici, calendari d'udienza, revisione linguistica —, la questione del contraddittorio non si poneva. Dal momento in cui il sistema è ammesso ad operare sugli «*atti delle parti*» «*ai fini della ricostruzione delle posizioni processuali*» e «*ai fini della individuazione del thema decidendum e del thema probandum*» [delib. agg. 2026, par. 8], la questione diventa ineludibile: le parti hanno diritto di sapere che le loro difese sono state elaborate da un sistema generativo? Il magistrato deve darne atto? Come si esercita la «*possibilità di verifica e contestazione degli output*» su un output che non è mai reso ostensibile? E come si assicura la «*parità informativa*» fra un giudice che dispone dello strumento e parti che, secondo lo stesso Consiglio, dispongono di strumenti diversi e migliori — poiché «*i professionisti del diritto dispongono spesso di sistemi specificamente dedicati al settore giuridico, con adeguate garanzie di tracciabilità e ancoraggio alle fonti*» [delib. agg. 2026, par. 5]?

Che il Consiglio fosse consapevole della dimensione bilaterale del problema risulta dal 2025, dove fra gli impegni auspicati per il Ministero figurava «*l'avvio delle necessarie interlocuzioni con l'avvocatura per una valutazione e una disciplina uniforme delle ricadute dell'utilizzo dell'IA in ambito processuale*» [delib. 2025, par. 6]. Il paragrafo 7 dell'aggiornamento, che enumera ciò che «*rimane necessario*» — la suite dedicata, la *sandbox* regolatoria, la condivisione delle sperimentazioni —, non riprende quella richiesta. Il tema del contraddittorio esce così dai documenti del CSM nel momento esatto in cui l'ampliamento del perimetro lo rende urgente.

9. Lo strumento e il criterio della sua scelta: Copilot come modello GPAI

Un dato resta sullo sfondo di entrambi i documenti senza essere mai tematizzato: la scelta di Copilot quale strumento della sperimentazione ministeriale non nasce da una valutazione comparativa fra sistemi, ma dalla disponibilità pregressa della licenza. Lo dice, in nota, la delibera del 2025: «*Allo stato è disponibile per i magistrati la funzionalità “copilot” fornita di default dal pacchetto office messo a disposizione degli utenti del “dominio giustizia”*» [delib. 2025, nota 1]. E lo conferma, nel 2026, la formula con cui il Consiglio ne registra la presenza: «*Il Consiglio prende atto che Microsoft 365 Copilot rappresenta lo strumento messo a disposizione dal Ministero in assenza di un sistema di intelligenza artificiale progettato specificamente per le esigenze della funzione giudiziaria*» [delib. agg. 2026, par. 7].

Non si tratta di un dettaglio di cronaca amministrativa. La scelta di uno strumento destinato a operare su atti giudiziari in un settore che l'Allegato III dell'AI Act qualifica ad alto rischio è, essa stessa, un atto che dovrebbe reggersi su un criterio dichiarato. Che quel criterio sia stato, di fatto, la disponibilità della licenza — soluzione comprensibile sul piano dell'economia amministrativa, perché evita procedure di approvvigionamento e integrazioni infrastrutturali — condiziona a monte la lettura delle criticità documentate dalla STO: non si tratta dei difetti di un prodotto giudicato inadeguato all'esito di un confronto, ma dei limiti di un prodotto generalista adottato per ragioni di disponibilità e valutato solo in seguito.

È il Consiglio stesso a offrire la qualificazione normativa che l'argomento richiede, e che ne accresce la portata: «*Microsoft 365 Copilot è un modello di intelligenza artificiale per finalità generali (General purpose AI – GPAI) ai sensi dell'art. 3, punto 63, dell'AI Act: non è progettato per operare nell'ambito specifico della funzione giudiziaria e non soddisfa in modo nativo i requisiti che tale funzione richiede*» [delib. agg. 2026, par. 5]. La delibera del 2025 aveva già riportato per esteso quella definizione, descrivendo il modello per finalità generali come quello «*caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle*» [delib. 2025, nota 2].

Da questa qualificazione discendono conseguenze che i documenti non traggono. Un modello per finalità generali integrato «*in una varietà di sistemi o applicazioni a valle*» e destinato, nel dominio giustizia, ad attività che coinvolgono atti giudiziari, solleva la questione della qualificazione del *deployer*: chi configura il *tenant*, definisce le etichette di riservatezza, disegna i flussi di lavoro con i «*checkpoint di supervisione umana*» e autorizza gli usi, esercita un potere di modellazione del sistema che l'AI Act, agli artt. 25 e 26, non tratta come indifferente. Il punto è tanto più rilevante alla luce del rinvio disposto dal Digital Omnibus: se l'obbligo di certificazione per i sistemi dell'Allegato III slitta al 2 dicembre 2027, il regime dei modelli per finalità generali segue tempi propri, e la sperimentazione in corso si colloca in un interstizio di cui i documenti non discutono le implicazioni.

Quanto alle alternative, il Consiglio ne registra l'esistenza in termini generali, quando lamenta che, «*a fronte di un modello generalista come quello fornito dal Ministero, i professionisti del diritto dispongono spesso di sistemi specificamente dedicati al settore giuridico, con adeguate garanzie di tracciabilità e ancoraggio alle fonti*» [delib. agg. 2026, par. 5]. La constatazione è esatta: il mercato offre strumenti verticali costruiti sul dominio giuridico e ancorati a corpora giurisprudenziali proprietari, dotati nativamente di meccanismi di *grounding* e di verifica delle citazioni⁴. Ma la comparazione non deve arrestarsi ad essi. Copilot è, per ammissione consiliare, un modello per finalità generali, e come tale si confronta anzitutto con gli altri modelli generalisti disponibili. Nulla, nell'impianto delle raccomandazioni, esclude che anche questi possano essere oggetto di sperimentazione, purché ricorrano le medesime garanzie richieste per Copilot: residenza dei dati, isolamento del *tenant*, assenza di addestramento, operatività confinata al dominio giustizia. L'«*approccio “multimodello”*» annunciato dal Dipartimento il 10 maggio 2026 [delib. agg. 2026, par. 1] sembra muoversi in questa direzione, pur senza che l'aggiornamento ne tragga conseguenze operative.

Resta aperta, dunque, la domanda se la «*posizione di sistematico svantaggio rispetto agli altri operatori del diritto*» [delib. agg. 2026, par. 7] derivi da un limite intrinseco dei modelli generalisti in quanto tali, oppure dal fatto che, fra i generalisti disponibili, la magistratura sta sperimentando soltanto quello già incluso nella licenza in uso.

Una terza via, evocata dalla delibera del 2025 e non ripresa nell'aggiornamento, è quella dei modelli eseguiti in locale: «*l'evoluzione tecnologica sta permettendo la realizzazione di sistemi di IA (spesso Open-source) progettati per eseguire modelli di linguaggio di grandi dimensioni localmente, ossia attraverso una*

⁴ Per un inventario aggiornato delle piattaforme di intelligenza artificiale generalista e di quelle verticali progettate specificamente per i giuristi si veda la pagina curata dall'autore a questo indirizzo <https://www.giovannipascuzzi.eu/2026/05/03/intelligenza-artificiale-generativa/>

installazione sul pc dell'utente e senza dipendere dal cloud. Tali sistemi, destinati prossimamente ad evolvere e diventare di largo consumo, devono, al pari degli altri, essere gestiti dai magistrati con una particolare attenzione ed essere oggetto di adeguata sperimentazione» [delib. 2025, par. 3]. La soluzione azzererebbe per definizione i rischi connessi alla trasmissione dei dati verso server esterni, ma il documento stesso ne segnala i limiti: essa richiede il *«previo adeguamento tecnologico delle macchine»*, e sconta l'incompatibilità con applicativi ministeriali — *«i nuovi applicativi ministeriali (Desk Cassazione, APP) sono concepiti per lavorare on line»* — che rappresenta, per il Consiglio, *«ulteriore ragione per cui la soluzione più efficace appare la costruzione di un sistema di IA interno al sistema giustizia»* [delib. 2025, par. 4].

10. Il contrappunto tecnico: la ricognizione della STO e il monito della prassi

All'apertura del paragrafo 4 l'aggiornamento fa seguire, immediatamente, il proprio contrappeso, e con una premessa che ne rovescia il tono: *«L'utilizzo di Copilot con gli atti giudiziari deve essere, comunque, ponderato dal singolo magistrato anche alla luce della ricognizione della STO del 29 aprile 2026»* [delib. agg. 2026, par. 5]. La ponderazione è dunque rimessa al singolo, sulla base di un documento istruttorio che elenca le criticità dello strumento appena autorizzato.

Le criticità enunciate sono quattro. La prima è la *«carezza di grounding documentale»*: il sistema *«tende a inserire dati non verificati nella costruzione di informazioni riepilogative, senza garantire il corretto collegamento tra il contenuto prodotto e le fonti effettivamente disponibili; nel contesto giudiziario, ciò compromette l'affidabilità complessiva del prodotto informativo»*.

La seconda, e la più grave, sono le *«allucinazioni»*: *«il sistema può generare contenuti presentati come reali pur non fondati su riscontri documentali, anche quando operante su un corpus documentale chiuso e predefinito»*. La precisazione è decisiva, perché smentisce l'assunto — diffuso anche fra gli operatori del diritto — secondo cui vincolare un sistema generativo a un insieme chiuso di documenti, anziché al web aperto, basti a eliminare il rischio di invenzione. L'esempio riportato è emblematico proprio per la ridondanza delle cautele adottate: *«l'inserimento da parte di Copilot di un riferimento a un Comune inesistente nel corso di una attività di catalogazione di elenchi di beni immobili svolta in ambiente istituzionale protetto, su documentazione previamente trattata con OCR: il sistema aveva ricevuto istruzioni esplicite di limitarsi ai soli documenti messi a disposizione, e ciononostante ha prodotto il riferimento errato senza segnalarlo come incerto»*. Alla medesima criticità la ricognizione riconduce, *«quale criticità strutturale generale di Copilot», «l'inserimento di collegamenti ipertestuali fittizi in luogo di riferimenti effettivamente verificabili»* [delib. agg. 2026, par. 5].

La terza è la *«mancata segnalazione dei limiti informativi»*: lo strumento *«tende a fornire risposte conclusive anziché segnalare esplicitamente i limiti incontrati nella fase di acquisizione dei dati, colmando automaticamente le lacune attraverso inferenze non supportate da evidenze documentali»*.

La quarta — che il documento colloca fra le criticità tecniche, benché non sia un difetto del prodotto ma una carezza di sistema — è la già ricordata *«posizione di svantaggio della magistratura»* [delib. agg. 2026, par. 5].

Vale la pena osservare che le prime tre criticità non sono, in realtà, scoperte del 2026: sono l'esatta verifica sul campo di ciò che il documento del 2025 aveva descritto in via teorica. *«L'output prodotto dai sistemi di*

IA generativa non è costante, poiché il loro funzionamento non segue logiche deterministiche ma probabilistiche: a ogni interrogazione il sistema seleziona, tra molte opzioni possibili, la risposta ritenuta più verosimile. Questa dinamica introduce una variabilità intrinseca, per cui la stessa domanda può generare risposte differenti»; e ancora: «Non è garantito un livello uniforme di qualità, coerenza o affidabilità delle risposte prodotte, anche in relazione a quesiti simili o ripetuti»; donde la conseguenza: «È sempre necessaria una verifica umana sull'accuratezza, la completezza e la pertinenza delle risposte, con riferimento a fonti attendibili e normative aggiornate, al fine di evitare che contenuti generati automaticamente assumano valore probatorio o decisionale senza adeguato controllo» [delib. 2025, par. 1, punti A, C e D]. La delibera del 2025 aveva distinto, con precisione lessicale, le «cd. allucinazioni (generazioni di contenuti non basati sulla realtà oggettiva)» dalle «cd. sycophancies (generazioni di contenuti compiacenti)» [delib. 2025, par. 1]: quest'ultima categoria non ricompare nella delibera del 2026, benché sia quella più insidiosa in un contesto in cui il sistema è interrogato su atti di parte.

Il monito, peraltro, non proviene soltanto dall'istruttoria consiliare. L'esperienza giudiziaria degli ultimi anni ha già registrato, in Italia e all'estero, casi di atti processuali contenenti riferimenti giurisprudenziali inesistenti, generati da sistemi conversazionali e non verificati da chi li ha depositati. L'episodio riferito dalla STO ne costituisce l'omologo interno: la stessa patologia — l'invenzione presentata come dato —, prodotta questa volta all'interno del dominio giustizia, «in ambiente istituzionale protetto», su un corpus chiuso e con istruzioni restrittive. Se il presidio contro l'allucinazione è la verifica umana, e se la verifica umana è tanto più difficile quanto più l'output è plausibile e privo di segnali di incertezza — il sistema, si ricorderà, ha prodotto il dato errato «senza segnalarlo come incerto» —, allora il rischio non è governato dalla sola prescrizione di controllare: è governato dal tempo e dalle competenze di cui il controllore dispone. È esattamente il punto che il documento del 2025 aveva colto sotto la formula della tutela del tempo della decisione (par. 13).

Da questo quadro il Consiglio trae una conclusione che ridimensiona, nella sostanza, la portata dell'apertura appena concessa: «Microsoft 365 Copilot, nella sua configurazione standard, non costituisce la soluzione strutturale adeguata per l'uso dell'intelligenza artificiale nella giustizia e [...] la funzione giudiziaria richiede sistemi di intelligenza artificiale dedicati, progettati ab origine per il dominio giuridico, dotati di governance specifica, tracciabilità delle fonti, verificabilità degli output e possibilità di controllo ex post delle elaborazioni effettuate» [delib. agg. 2026, par. 5]. Il documento amplia il perimetro degli usi consentiti nello stesso atto in cui certifica, sulla base della propria istruttoria, l'inadeguatezza strutturale dello strumento con cui quegli usi dovranno essere realizzati. L'ambivalenza non è contraddizione: è la fotografia di una fase di transizione. Ma essa impone di leggere l'ampliamento del paragrafo 8 non come un giudizio di affidabilità su Copilot, bensì come la presa d'atto che, nell'attesa di una suite dedicata, le condizioni cumulative del paragrafo 4 sono l'unico argine disponibile contro rischi che il Consiglio stesso considera non superati, ma soltanto governabili.

Tavola 2 - I rischi: previsione teorica (2025) e verifica sul campo (2026)

Delibera 8 ottobre 2025	Delibera 22 luglio 2026 (aggiornamento)
«A. L'output prodotto dai sistemi di IA generativa non è costante, poiché il loro funzionamento non segue logiche deterministiche ma probabilistiche: a ogni interrogazione il sistema seleziona, tra molte opzioni possibili, la risposta ritenuta più verosimile. Questa dinamica introduce una variabilità intrinseca, per cui la stessa domanda può generare risposte differenti» [par. 1]	«carezza di grounding documentale: il sistema tende a inserire dati non verificati nella costruzione di informazioni riepilogative, senza garantire il corretto collegamento tra il contenuto prodotto e le fonti effettivamente disponibili; nel contesto giudiziario, ciò compromette l'affidabilità complessiva del prodotto informativo» [par. 5]

Delibera 8 ottobre 2025	Delibera 22 luglio 2026 (aggiornamento)
«Rischi significativi riguardano, inoltre, gli output generati dai sistemi di IA che possono contenere errori e distorsioni, quali cd. allucinazioni (generazioni di contenuti non basati sulla realtà oggettiva), o cd. sycophancies (generazioni di contenuti compiacenti)» [par. 1]	«“allucinazioni”: il sistema può generare contenuti presentati come reali pur non fondati su riscontri documentali, anche quando operante su un corpus documentale chiuso e predefinito. La ricognizione della STO del 29 aprile 2026 documenta, quale esempio emblematico, l'inserimento da parte di Copilot di un riferimento a un Comune inesistente nel corso di una attività di catalogazione di elenchi di beni immobili svolta in ambiente istituzionale protetto, su documentazione previamente trattata con OCR: il sistema aveva ricevuto istruzioni esplicite di limitarsi ai soli documenti messi a disposizione, e ciononostante ha prodotto il riferimento errato senza segnalarlo come incerto. La medesima ricognizione documenta inoltre - quale criticità strutturale generale di Copilot - l'inserimento di collegamenti ipertestuali fittizi in luogo di riferimenti effettivamente verificabili» [par. 5] [la categoria delle sycophancies non è ripresa]
«B. Le risposte fornite possono variare anche in funzione della formulazione del quesito (cd. prompting), della lunghezza, della precisione linguistica o del contesto implicito nella richiesta, influenzando sensibilmente la qualità e la direzione dell'output generato. C. Non è garantito un livello uniforme di qualità, coerenza o affidabilità delle risposte prodotte, anche in relazione a quesiti simili o ripetuti. L'output può contenere imprecisioni, omissioni, o risultare non pertinente rispetto al dominio di applicazione» [par. 1]	«mancata segnalazione dei limiti informativi: lo strumento tende a fornire risposte conclusive anziché segnalare esplicitamente i limiti incontrati nella fase di acquisizione dei dati, colmando automaticamente le lacune attraverso inferenze non supportate da evidenze documentali» [par. 5]
«D. È sempre necessaria una verifica umana sull'accuratezza, la completezza e la pertinenza delle risposte, con riferimento a fonti attendibili e normative aggiornate, al fine di evitare che contenuti generati automaticamente assumano valore probatorio o decisionale senza adeguato controllo» [par. 1]	«Il Consiglio ribadisce, pertanto, che Microsoft 365 Copilot, nella sua configurazione standard, non costituisce la soluzione strutturale adeguata per l'uso dell'intelligenza artificiale nella giustizia e che la funzione giudiziaria richiede sistemi di intelligenza artificiale dedicati, progettati ab origine per il dominio giuridico, dotati di governance specifica, tracciabilità delle fonti, verificabilità degli output e possibilità di controllo ex post delle elaborazioni effettuate» [par. 5]
— nessuna disposizione corrispondente	«posizione di svantaggio della magistratura: a fronte di un modello generalista come quello fornito dal Ministero, i professionisti del diritto dispongono spesso di sistemi specificamente dedicati al settore giuridico, con adeguate garanzie di tracciabilità e ancoraggio alle fonti» [par. 5]

11. Le condizioni cumulative e i loro corollari: formazione, supervisione bloccante, responsabilità

L'uso di Copilot con atti giudiziari è ammesso «esclusivamente nel rispetto cumulativo» di cinque condizioni [delib. agg. 2026, par. 4].

La prima riguarda il trattamento dei dati personali contenuti negli atti, di cui si è detto al paragrafo 6.

La seconda è l'«operatività esclusiva all'interno del dominio giustizia»: «l'uso di Copilot è consentito unicamente attraverso il tenant istituzionale del Ministero della giustizia [...]; è vietato l'uso di versioni consumer o di altri sistemi di intelligenza artificiale generativa non autorizzati dal Ministero».

La terza è la «supervisione umana obbligatoria e bloccante»: «ogni output prodotto da Copilot deve essere verificato dal magistrato prima di qualsiasi utilizzo; nei flussi di lavoro strutturati (come quelli modellati sull'esperienza del Tribunale di Catania), i checkpoint di supervisione

umana devono essere obbligatori e bloccanti, impedendo la prosecuzione automatica del flusso in assenza di esplicita validazione».

La quarta è l'«utilizzo di prompt strutturati»: *«ove possibile, il magistrato o l'ufficio dovranno adottare un linguaggio di interrogazione strutturato che limiti lo spazio interpretativo del sistema e vincoli gli output ai soli documenti del fascicolo, riducendo il rischio di “allucinazioni”».*

La quinta è l'«adeguata formazione»: *«il magistrato che utilizzi Copilot con atti giudiziari deve aver ricevuto adeguata formazione tecnica sulle caratteristiche del sistema, sui suoi limiti strutturali – in particolare sul fenomeno delle “allucinazioni” – e sulle tecniche di verifica degli output; la formazione è presupposto essenziale dell'uso corretto dello strumento».*

Tre corollari, che i documenti non esplicitano, discendono da questa costruzione.

Il primo riguarda la formazione. Essa non è raccomandata: è condizione cumulativa di ammissibilità, e il testo la qualifica come «*presupposto essenziale*». Ne segue che l'uso di Copilot su atti giudiziari da parte del magistrato che non abbia ricevuto formazione non è un uso imprudente: è un uso non consentito dalle raccomandazioni. Il che apre interrogativi che il documento lascia intatti — quale formazione soddisfi il requisito, quale soggetto la eroghi e la attesti, quali conseguenze si producano in caso di inosservanza — e che assumono peso ulteriore ove si consideri che la quarta condizione, i *prompt* strutturati, presuppone una competenza tecnica specifica («*un linguaggio di interrogazione strutturato*»), la cui acquisizione non è oggetto di alcun percorso definito. Il Consiglio, nel 2025, aveva del resto già ricondotto la questione alla responsabilità individuale: *«il magistrato è tenuto all'utilizzo consapevole e conforme degli strumenti IA a partire dall'obbligo di informazione e partecipazione alla formazione che sul tema sarà erogata»* [delib. 2025, par. 4].

Il secondo riguarda la supervisione bloccante. La prescrizione per cui i *checkpoint* «*devono essere obbligatori e bloccanti*» non è una regola di condotta rivolta al magistrato: è una caratteristica del flusso di lavoro, e dunque un vincolo inscritto nell'architettura applicativa. Ma il disegno dell'architettura applicativa appartiene, per l'art. 15, comma 2, della l. n. 132 del 2025, alla competenza ministeriale. Ne risulta una configurazione singolare: l'autonomia del magistrato è presidiata mediante un vincolo tecnico progettato dall'amministrazione. Il presidio è opportuno, e la sua ratio evidente; ma la stessa leva che impone la validazione umana in un punto del flusso può, se diversamente calibrata, determinare la sequenza delle operazioni, i tempi, i punti di ingresso e di uscita del giudice dal procedimento automatizzato. Che il disegno dei *workflow* giudiziari sia materia neutra, il documento lo presuppone senza dimostrarlo.

Il terzo riguarda la responsabilità. Il documento del 2025 pone fra le cautele operative «*la responsabilità individuale*» e ne precisa il contenuto in termini di verificabilità: *«Occorre sempre verificare di poter replicare autonomamente le conclusioni fornite dall'IA»* [delib. 2025, par. 4]. La formula è esigente, e definisce uno standard di diligenza: la conclusione dell'IA è utilizzabile solo se il magistrato è in grado di raggiungerla autonomamente. Ma i documenti si arrestano qui. Che cosa accada quando un'allucinazione superi indenne la supervisione e raggiunga un provvedimento — se ne derivi una questione di responsabilità disciplinare, se e a quali condizioni possa configurarsi la colpa grave rilevante ai fini della responsabilità civile per l'esercizio della funzione giudiziaria, come si combinino tali profili con l'obbligo di formazione elevato a condizione di ammissibilità — è materia che esula dalle competenze del Consiglio in sede di

raccomandazione, ma che l'ampliamento del perimetro rende attuale e che nessuna fonte, allo stato, disciplina.

12. Il piano istituzionale: piattaforma dedicata, *sandbox*, gruppo tecnico

Un filo conduttore attraversa senza soluzione di continuità entrambi i documenti: la convinzione che la soluzione non possa essere, a regime, uno strumento generalista adattato al contesto giudiziario, ma debba essere un sistema costruito per esso. Già nel 2025 il Consiglio auspicava che il Ministero, *«dopo aver messo a disposizione degli uffici giudiziari i risultati delle sperimentazioni in corso con la rete dei RID e dei MAGRIF sotto la supervisione della STO»*, valutasse *«la possibilità di commissionare la realizzazione di un sistema di IA interno al sistema giustizia auspicabilmente pronto prima di agosto 2026 per essere fruito da tutti i magistrati ordinari»* [delib. 2025, par. 3]. Il termine indicato è trascorso senza esito, e l'aggiornamento non ne dà conto.

La richiesta è ribadita e rafforzata con un argomento comparativo: l'assenza di un sistema dedicato *«pone, tuttavia, la magistratura in una posizione di sistematico svantaggio rispetto agli altri operatori del diritto, i quali dispongono già di strumenti dedicati al settore giuridico»*; si auspica pertanto *«che l'approccio “multimodello” avviato dal Ministero evolva, prima dell'entrata in vigore delle disposizioni europee sui sistemi ad alto rischio, verso l'adozione di una suite di intelligenza artificiale progettata ab origine per operare all'interno di workflow giuridici formalizzati, con regole stringenti in materia di gestione e protezione dei dati, tracciabilità delle fonti, possibilità di controllo e verifica ex post»* [delib. agg. 2026, par. 7].

Alla richiesta di piattaforma si affiancano due strumenti istituzionali. Il primo è la *sandbox* regolatoria congiunta, già prevista nel 2025 come *«definizione, con il coinvolgimento del Consiglio Superiore della Magistratura, di una sandbox regolatoria congiunta per la sperimentazione controllata di sistemi di IA destinati all'uso giudiziario o organizzativo»*, ambiente destinato a consentire *«la verifica preventiva dell'impatto tecnologico, giuridico e costituzionale, con particolare riferimento alla protezione dei diritti fondamentali, all'imparzialità del trattamento e all'autonomia della funzione giurisdizionale»* [delib. 2025, par. 6]; e nel 2026 sollecitata di nuovo, *«in attuazione di quanto previsto dalle raccomandazioni dell'8 ottobre 2025»* [delib. agg. 2026, par. 7]. La reiterazione, a nove mesi di distanza e nei medesimi termini, è essa stessa una notizia: la *sandbox* non è stata istituita, e la sperimentazione di Copilot su atti giudiziari procede al di fuori di quell'ambiente controllato che avrebbe dovuto precederla.

Il secondo strumento riguarda l'organizzazione consiliare: il Consiglio *«anche eventualmente intervenendo sul suo regolamento»* potrà *«avvalersi di un gruppo tecnico multidisciplinare permanente, eventualmente anche con esperti esterni, incaricato di svolgere attività di valutazione indipendente dei sistemi, di elaborare criteri metodologici condivisi per il controllo degli impieghi di IA»* [delib. agg. 2026, par. 7; già delib. 2025, par. 6]. È la risposta, sul piano organizzativo, al deficit istruttorio di cui si è detto al paragrafo 3: se il Consiglio *«non può che prendere atto»* delle garanzie fornite dal fornitore, la costituzione di un organismo stabile di *«valutazione indipendente dei sistemi»* è la condizione perché quella formula, in futuro, possa essere sostituita da una verifica. L'ipotesi di un intervento sul regolamento consiliare segnala che il passaggio è avvertito come strutturale, e non contingente.

Va infine ricordato che il piano strategico auspicato nel 2025 comprendeva altri due elementi che l'aggiornamento non riprende: *«la verifica della adesione formale o sostanziale al Codice di Condotta per*

i modelli generativi da parte dei fornitori, quale presupposto di trasparenza, affidabilità, protezione dei dati e rispetto dei diritti fondamentali» e «l'istituzione di un sistema di audit periodico sull'impatto dei sistemi IA nell'attività giudiziaria e organizzativa» [delib. 2025, par. 6]. Il primo avrebbe offerto un criterio esterno di valutazione del fornitore; il secondo, uno strumento di controllo continuo sugli effetti. Nessuno dei due compare fra ciò che, nel 2026, «rimane necessario».

Tavola 3 - Gli impegni chiesti al Ministero: reiterazioni e abbandoni

Delibera 8 ottobre 2025	Delibera 22 luglio 2026 (aggiornamento)
«Da questo punto di vista sarebbe utile che il Ministero - dopo aver messo a disposizione degli uffici giudiziari i risultati delle sperimentazioni in corso con la rete dei RID e dei MAGRIF sotto la supervisione della STO (diretta articolazione consiliare) - valuti la possibilità di commissionare la realizzazione di un sistema di IA interno al sistema giustizia auspicabilmente pronto prima di agosto 2026 per essere fruito da tutti i magistrati ordinari» [par. 3]	«l'adozione di una suite di intelligenza artificiale dedicata alla funzione giudiziaria: si auspica che l'approccio “multimodello” avviato dal Ministero evolva, prima dell'entrata in vigore delle disposizioni europee sui sistemi ad alto rischio, verso l'adozione di una suite di intelligenza artificiale progettata ab origine per operare all'interno di workflow giuridici formalizzati, con regole stringenti in materia di gestione e protezione dei dati, tracciabilità delle fonti, possibilità di controllo e verifica ex post» [par. 7] [reiterato, senza indicazione di termine]
«la definizione, con il coinvolgimento del Consiglio Superiore della Magistratura, di una sandbox regolatoria congiunta per la sperimentazione controllata di sistemi di IA destinati all'uso giudiziario o organizzativo. Tale ambiente sperimentale, fondato su un approccio paritetico e trasparente, consentirà la verifica preventiva dell'impatto tecnologico, giuridico e costituzionale, con particolare riferimento alla protezione dei diritti fondamentali, all'imparzialità del trattamento e all'autonomia della funzione giurisdizionale» [par. 6]	«l'istituzione della sandbox regolatoria congiunta: il Consiglio chiede di procedere all'istituzione, d'intesa con il Consiglio stesso, della sandbox regolatoria congiunta per la sperimentazione controllata di sistemi di intelligenza artificiale destinati all'uso giudiziario, in attuazione di quanto previsto dalle raccomandazioni dell'8 ottobre 2025» [par. 7] [reiterato nei medesimi termini]
«Il Consiglio, potrà, inoltre avvalersi di un gruppo tecnico multidisciplinare permanente, costituito eventualmente anche da esperti esterni, con l'incarico di svolgere attività di valutazione indipendente dei sistemi, di elaborare criteri metodologici condivisi per il controllo degli impieghi di IA» [par. 6]	«Si ribadisce, inoltre, che il Consiglio - anche eventualmente intervenendo sul suo regolamento - potrà “avvalersi di un gruppo tecnico multidisciplinare permanente, eventualmente anche con esperti esterni, incaricato di svolgere attività di valutazione indipendente dei sistemi, di elaborare criteri metodologici condivisi per il controllo degli impieghi di IA”» [par. 7] [reiterato, con l'ipotesi di un intervento sul regolamento consiliare]
— nessuna disposizione corrispondente	«la condivisione e la capitalizzazione delle sperimentazioni avanzate: il Consiglio valuta favorevolmente le sperimentazioni in atto presso il Tribunale di Catania e la Procura generale di Perugia, quale fattivo contributo al migliore adattamento dell'applicativo Copilot alle esigenze della funzione giudiziaria, auspicando che ne siano presto autorizzate altre e che i risultati vengano messi a disposizione di tutti gli uffici giudiziari come modelli replicabili e base per la progettazione della suite dedicata» [par. 7] [impegno nuovo]
«l'istituzione di un sistema di audit periodico sull'impatto dei sistemi IA nell'attività giudiziaria e organizzativa» [par. 6]	— non ripreso
«la verifica della adesione formale o sostanziale al Codice di Condotta per i modelli generativi da parte dei fornitori, quale presupposto di trasparenza, affidabilità, protezione dei dati e rispetto dei diritti fondamentali» [par. 6]	— non ripreso
«la definizione di criteri condivisi per l'autorizzazione e la tracciabilità dei sistemi impiegati negli uffici giudiziari» [par. 6]	— non ripreso
«la predisposizione di protocolli tecnici e organizzativi per la tutela dei dati, la cybersicurezza e la prevenzione della profilazione indebita» [par. 6]	— non ripreso
«l'avvio delle necessarie interlocuzioni con l'avvocatura per una valutazione e una disciplina uniforme delle ricadute dell'utilizzo dell'IA in ambito processuale» [par. 6]	— non ripreso

13. Ciò che l'aggiornamento lascia cadere

Il confronto fra i due documenti restituisce, oltre alle differenze di regola, una differenza di registro. La delibera del 2025 dedicava un intero paragrafo al ruolo del Consiglio, e vi svolgeva un discorso che eccede la gestione del rischio per toccare la natura della funzione giurisdizionale. Vi si legge che «è *fondamentale che l'IA non sostituisca mai il pensiero libero e critico del magistrato, né pregiudichi l'originale contributo personale alla riflessione in campo giuridico, ma lo supporti in modo trasparente e ricostruibile*» [delib. 2025, par. 5].

Da questa premessa discendevano tre impegni. Il primo era rendere i magistrati consapevoli «che i sistemi di IA producono output probabilistici, non deterministici», diffondendo buone prassi «sui fondamenti dell'IA (natura probabilistica, soglie di confidenza, errore, bias, model drift), sulle cautele d'uso (minimizzazione degli input, divieto di trattare atti o dati di procedimento) e sulle tecniche di verifica dell'output (replicabilità su fonti ufficiali, triangolazione delle fonti, controllo di coerenza)» [delib. 2025, par. 5]. Si noti, per inciso, che fra le cautele d'uso allora indicate figurava il «divieto di trattare atti o dati di procedimento»: la formula più netta, in tutto il corpus consiliare, di ciò che l'aggiornamento ha poi consentito.

Il secondo impegno era «*tutelare il tempo della decisione*», ed è il passaggio teoricamente più denso dei due documenti: «L'uso dell'IA deve essere prevalentemente orientato a liberare tempo per la decisione e non solo a un incremento dell'efficienza e della produttività. Poiché realisticamente in futuro non sarà consentito al singolo magistrato di vagliare in autonomia gli algoritmi che governano i sistemi, la verifica umana dovrà concentrarsi sull'output: pertinenza rispetto al caso, coerenza giuridica, replicabilità su fonti ufficiali e assenza di errori o distorsioni rilevanti. Il giudice potrà mantenere l'autonomia critica solo se disporrà del tempo necessario per controllare gli esiti, farli propri oppure discostarsene motivatamente quando non convincenti. Ciò implica anche la possibilità di resistere alla macchina (riconoscendone gli errori ed evitando il c.d. automation bias) e di non cedere all'attrazione dell'efficienza numerica quando questa mette a rischio la qualità della decisione e i presidi del giusto processo» [delib. 2025, par. 5].

Il terzo era «*riaffermare la centralità dell'esperienza processuale*»: «Il processo e la valutazione giudiziale sono un'esperienza umana insostituibile, fondata su presenza, oralità, immediatezza percettiva e contraddittorio in uno spazio condiviso. Il Consiglio si adopererà, pertanto, per impedire la “despazializzazione del giudizio”, ossia la riduzione del processo a mera interazione digitale, riaffermando che la decisione nasce da una relazione viva tra giudice, parti e prove, in un tempo e in uno spazio che ne garantiscano serietà, pubblicità e responsabilità» [delib. 2025, par. 5].

Nulla di tutto questo ricompare nell'aggiornamento del 2026, che è documento interamente tecnico-operativo: garanzie, condizioni, elenchi, criticità. Si può leggere l'omissione come fisiologica — il documento del 2026 dichiara di integrare, non di sostituire, e i principi del 2025 «conservano piena validità» — e la lettura è formalmente ineccepibile. Ma l'omissione non è indifferente, perché i tre impegni del 2025 erano precisamente gli argomenti che consentivano di misurare l'ampliamento del 2026. La supervisione «obbligatoria e bloccante» del 2026 è la traduzione procedurale della verifica umana; ma la delibera del 2025 aveva avvertito che la verifica è effettiva solo se il giudice «disporrà del tempo necessario per controllare gli esiti», e il 2026 non si interroga sul costo temporale delle cinque condizioni cumulative che impone. Analogamente, l'*automation bias* è la ragione per cui l'ancoraggio a un *thema decidendum*

precostituito dalla macchina è problematico anche quando la decisione resta umana; e il 2026, che quel rischio rende attuale, non lo nomina.

Se dunque il documento dell'ottobre 2025 conteneva, accanto alle regole, una teoria della funzione giurisdizionale nell'età dell'automazione, quello del luglio 2026 contiene un manuale di condizioni d'uso. È forse un esito inevitabile della specializzazione progressiva degli interventi; ma è anche la ragione per cui l'aggiornamento, letto da solo, appare più permissivo di quanto la sua lettera non dica.

14. La natura delle raccomandazioni e il perimetro soggettivo

Resta da chiarire che cosa siano, sul piano delle fonti, i documenti qui esaminati. La domanda non è oziosa, perché è lo stesso Consiglio a riconoscere che il potere di individuare e autorizzare i sistemi appartiene *«esclusivamente al Ministero della giustizia, ai sensi dell'art. 15, comma 2, della legge 23 settembre 2025, n. 132»* [delib. agg. 2026, par. 3], e che il proprio intervento si colloca su un piano diverso: *«in tale quadro, le presenti raccomandazioni ribadiscono, sulla base delle garanzie acquisite, le condizioni e i limiti entro cui l'uso di Microsoft 365 Copilot può ritenersi compatibile con i principi fondamentali della funzione giudiziaria»* [delib. agg. 2026, par. 3].

Il titolo dell'intervento consiliare non è dunque la disciplina degli impieghi, ma la tutela dei principi che governano l'esercizio della funzione: le raccomandazioni del 2025 sono dichiaratamente *«ispirate ai principi di legalità, trasparenza, proporzionalità e autonomia decisionale, al fine di garantire i diritti fondamentali nonché l'indipendenza e l'imparzialità dell'azione giudiziaria»* [delib. 2025, premessa]. È la ragione per cui il Consiglio, mentre riconosce la competenza ministeriale, invita il Ministero a esercitare le proprie prerogative costituzionali: *«è poi auspicabile che allo stato [...] il Ministero della Giustizia italiano eserciti le prerogative previste dall'art. 110 della Costituzione»* [delib. 2025, par. 3].

Ne discende che si tratta di atti di indirizzo, non di regolamentazione. Ma il lessico dei due documenti oscilla, e l'oscillazione non è priva di conseguenze. Accanto al registro raccomandatorio (*«si auspica», «sarebbe utile», «è opportuno»*) compaiono formule prescrittive: *«è vietato l'uso di versioni consumer», i checkpoint «devono essere obbligatori e bloccanti», la formazione «è presupposto essenziale», l'uso è ammesso «esclusivamente nel rispetto cumulativo delle seguenti condizioni», taluni usi «rimangono in ogni caso esclusi»* [delib. agg. 2026, parr. 4 e 8]. Quale sia l'effetto dell'inosservanza — se essa rilevi soltanto sul piano dell'utilizzo consapevole di cui alla *«responsabilità individuale»* enunciata nel 2025, o se possa assumere rilievo ulteriore — è questione che i documenti non affrontano, e che la progressiva prescrittività del linguaggio rende meno teorica di quanto fosse nel 2025.

Va infine segnalato il perimetro soggettivo. Entrambe le delibere si rivolgono ai magistrati ordinari e agli uffici giudiziari del *«dominio giustizia»*: il sistema interno auspicato nel 2025 deve essere *«fruito da tutti i magistrati ordinari»* [delib. 2025, par. 3], e l'operatività consentita è quella *«all'interno del tenant istituzionale del Ministero della giustizia»* [delib. agg. 2026, par. 4]. Restano fuori le altre magistrature — la giustizia amministrativa, quella contabile, quella tributaria —, che operano su domini informatici distinti, rispondono a organi di autogoverno diversi e, allo stato, non dispongono di un atto di indirizzo equivalente. La lacuna è tanto più significativa in quanto i principi invocati dal Consiglio non hanno nulla di specificamente ordinario: l'autonomia decisionale, il divieto di profilazione, la supervisione umana, la parità informativa fra le parti valgono per ogni giurisdizione. Che a essi si sia data forma soltanto nel circuito della magistratura ordinaria è un dato dell'organizzazione dell'autogoverno, non della materia.

15. Conclusioni: le questioni aperte

Il percorso ricostruito restituisce l'immagine di un aggiornamento che si dichiara prudente e che, sul piano dei principi, lo è davvero. Il nucleo della funzione giurisdizionale resta *«di esclusiva competenza del magistrato, che non può delegarla ad alcun sistema di intelligenza artificiale»* [delib. agg. 2026, par. 2], e il documento del 2026 lo ribadisce con maggiore nettezza redazionale del testo che integra, isolando per la prima volta in elenco autonomo gli usi non consentiti.

Ciò che muta è il perimetro delle attività strumentali: dall'esclusione dell'immissione *«di dati sensibili di atti processuali su dispositivi di IA generalista»* [delib. 2025, par. 4] si passa a un'apertura ancorata a garanzie tecniche verificate da altri e a cinque condizioni cumulative che delineano un modello di supervisione particolarmente esigente — *«obbligatoria e bloccante»*, non meramente successiva. Ma è un'apertura che il Consiglio accompagna con una dichiarazione di sfiducia tecnica verso lo strumento concretamente disponibile, riconoscendo che Copilot *«non costituisce la soluzione strutturale adeguata»* [delib. agg. 2026, par. 5]: ambivalenza che non è contraddizione, ma fotografia onesta di una transizione in cui la magistratura è chiamata a usare uno strumento che i propri organi di garanzia giudicano, insieme, utilizzabile sotto condizioni e strutturalmente inadeguato.

Il punto critico, però, non sta nell'ambivalenza: sta nella qualificazione. L'aggiornamento estende l'uso ad attività che coinvolgono atti giudiziari *«nella misura in cui tali attività siano riconducibili alla fase analitica e ricostruttiva del processo e non incidano sulle valutazioni giuridiche, interpretative o decisionali»* [delib. agg. 2026, par. 4], ma non dimostra che l'individuazione del *thema decidendum* e del *thema probandum* soddisfi quella condizione, né la riconduce ad alcuna delle quattro ipotesi dell'art. 6, par. 3, dell'AI Act. E il criterio che il documento del 2025 aveva impiegato per un problema analogo — l'uscita dalla deroga ogni volta che l'impiego *«incide potenzialmente sull'attività valutativa e sull'indirizzo giuridico»* [delib. 2025, par. 3] — condurrebbe, se applicato, a conclusione diversa. È qui che l'aggiornamento avrebbe dovuto motivare, e non lo ha fatto.

Restano, per il prossimo intervento consiliare — che lo stesso aggiornamento si riserva di adottare *«all'esito dell'iter legislativo europeo relativo al Digital Omnibus on AI e in ragione dei progressi registrati nell'attuazione degli impegni ministeriali»* [delib. agg. 2026, par. 7] —, sei questioni aperte.

– La qualificazione delle nuove attività ammesse rispetto all'art. 6, par. 3, dell'AI Act, e in particolare la compatibilità del confronto automatizzato fra posizioni processuali con l'esclusione dalla categoria dei sistemi ad alto rischio.

– Il regime dei dati: se l'anonimizzazione debba tornare condizione di ammissibilità una volta disponibile quel *«software per l'anonimizzazione degli atti»* di cui il Consiglio dichiara *«urgente»* la diffusione, e come il trattamento consistente nell'immissione di atti giudiziari in un sistema generativo si collochi rispetto agli obblighi del regolamento (UE) 2016/679.

– La traduzione del divieto di profilazione da enunciazione di principio a requisito di architettura, con l'individuazione di chi acceda ai log delle elaborazioni e a quali fini.

– Il contraddittorio: se e come le parti debbano essere informate dell'impiego di sistemi generativi sugli atti del proprio fascicolo, e come si eserciti quella *«possibilità di verifica e contestazione degli output»* che la delibera del 2025 poneva fra le condizioni di compatibilità con il giusto processo.

– La scelta dello strumento: se la sperimentazione ministeriale si aprirà a un confronto sistematico fra più modelli — generalisti e verticali — anziché restare ancorata a quello reso disponibile dalla licenza in uso, e con quali criteri dichiarati.

– L'attuazione degli impegni istituzionali reiterati da due delibere consecutive: la suite dedicata, la *sandbox* regolatoria congiunta e il gruppo tecnico multidisciplinare permanente, senza i quali la formula secondo cui il Consiglio «non può che prendere atto» delle garanzie altrui è destinata a ripetersi.

Alla fine, il criterio di valutazione che i documenti offrono di sé è quello enunciato dal Consiglio a proposito del rinvio europeo, e vale anche per l'ampliamento che l'aggiornamento dispone: «*il tempo aggiuntivo deve essere utilizzato produttivamente per costruire l'infrastruttura tecnica e organizzativa necessaria, non per differire gli sforzi di adeguamento*» [delib. agg. 2026, par. 6]. I sedici mesi guadagnati sul calendario europeo sono esattamente il tempo entro cui le sei questioni elencate dovrebbero trovare risposta.

Per approfondimenti

CESARE PARODI, [*Le nuove Raccomandazioni del CSM sull'intelligenza artificiale nella giustizia. Dalla cautela difensiva alla governance del rischio*](#), in Sistema penale, 24 luglio 2026

AGOSTINO CLEMENTE, [*Intelligenza artificiale e processo civile: dal se al come, senza ulteriori indugi*](#), in Questione giustizia, 24 luglio 2026

MARIANO SCIACCA, [*Integrare senza sostituire. L'aggiornamento 2026 delle raccomandazioni del CSM sull'intelligenza artificiale nella giustizia, tra continuità regolatoria e tutela dell'integrità cognitiva*](#), in Diritto, giustizia e Costituzione del 23 luglio 2026.

GIOVANNI PASCUZZI, [*Sulle sentenze “allucinate” dall'intelligenza artificiale*](#), Il Dubbio, 9 luglio 2026

CLAUDIA MORELLI, [*AI nei tribunali italiani tra sperimentazioni e guardrail. Duemila agenti Copilot creati dai magistrati, i progetti autorizzati a Perugia e Catania*](#), Altalex, 29 giugno 2026.

GIOVANNI PASCUZZI, [*Intelligenza artificiale generativa e giustizia amministrativa*](#), 22 giugno 2026 [<https://www.giovannipascuzzi.eu/2026/06/22/intelligenza-artificiale-generativa-e-giustizia-amministrativa/>].

Giovanni Pascuzzi, Consigliere di Stato

Le opinioni di cui al presente contributo sono espresse dall'Autore a titolo personale; esse non impegnano l'Ufficio studi della Giustizia amministrativa, né quest'ultima quale Istituzione.