

Ia, banche dati giurisprudenziali, anonimizzazione e tutela del dato: un modello multilivello

Raccolta giurisprudenziale, anonimizzazione, strumenti Ai generativi e proprietà intellettuale del dato giudiziario



di *Fernanda Iannone*

Consigliere Corte d'Appello di Napoli
RID giudicante penale Napoli
EJTN Digital Ambassador 2025-2026

It

Il contributo esamina le principali questioni giuridiche sollevate dall'integrazione dell'intelligenza artificiale nella gestione della giurisprudenza. Muovendo dalla qualificazione della sentenza come «dato strutturato», lo scritto analizza il quadro normativo multilivello applicabile – dall'AI Act alle Linee guida UNESCO 2025 e al documento AI Essentials for Judges 2026, dalla L. 132/2025 alle Raccomandazioni CSM del 2025 e al loro aggiornamento del 22 luglio 2026, nonché alle Guidelines CEPEJ 2025 – per poi affrontare i temi dell'anonimizzazione delle decisioni, dell'utilizzo di strumenti generativi (Copilot e analoghi) nel dominio della giustizia e della proprietà intellettuale sulle banche dati giurisprudenziali. La riflessione si conclude con la proposta di un modello integrato di governo del dato giudiziario, nel segno del magistrato quale «garante umano» della sua qualità.



intelligenza artificiale – banche dati giurisprudenziali – anonimizzazione – AI Act – proprietà intellettuale.

Eng

This article examines the main legal issues raised by the integration of artificial intelligence into the management of case law. Starting from the characterisation of judicial decisions as «structured data», the paper analyses the applicable multi-level regulatory framework – from the AI Act to the UNESCO Guidelines 2025 and AI Essentials for Judges 2026, from Italian Law 132/2025 to the 2025 CSM Recommendations and their update of 22 July 2026, as well as the 2025 CEPEJ Guidelines – before addressing the anonymisation of decisions, the use of generative AI tools (Copilot and analogous systems) in the justice domain, and intellectual property rights over case law databases. The analysis concludes by proposing an integrated institutional framework for judicial data, centred on the judge as the «human guarantor» of data quality.



artificial intelligence – case law databases – anonymisation – AI Act – intellectual property.

Sommario

1. Premessa: la giurisprudenza come «dato». – 2. Il quadro normativo multilivello: 2.1. Le Linee guida UNESCO 2025 per l'uso dei sistemi IA nei tribunali; 2.2. Il documento «AI Essentials for Judges» (UNESCO 2026); 2.3. Il Regolamento sull'intelligenza artificiale (AI Act); 2.4. Il quadro del Consiglio d'Europa e le Guidelines CEPEJ 2025; 2.5. La legge italiana n. 132/2025 e le Raccomandazioni CSM; 2.6. Il ruolo dell'EJTN e del programma Digital Ambassador; 2.7. L'aggiornamento CSM del 22 luglio 2026: l'apertura controllata agli atti giudiziari e il governo del rischio: 2.7.1. Continuità dei principi e riserva della funzione giurisdizionale; 2.7.2. Le garanzie tecniche e la delimitazione dell'ambiente autorizzato; 2.7.3. L'apertura sperimentale al trattamento degli atti giudiziari; 2.7.4. La linea di confine tra attività ricostruttiva e attività valutativa; 2.7.5. Il coordinamento con la disciplina europea dei sistemi ad alto rischio; 2.7.6. I limiti del modello generalista e la prospettiva di una suite dedicata; 2.7.7. Sperimentazione, formazione e regolazione evolutiva; 2.7.8. Grounding, supervisione e integrità del processo cognitivo: la prima traduzione giurisprudenziale. – 3. Anonimizzazione e pubblicità delle decisioni: un equilibrio instabile: 3.1. La sentenza TAR Lazio n. 7625/2025; 3.2. Il sistema delle fonti applicabile; 3.3. La sentenza CGUE «Deloitte» e la pseudonimizzazione; 3.4. Chiosa: pubblicità controllata e dato personale relativo. – 4. Copilot e strumenti IA generativi: il nodo della tutela del dato: 4.1. Il problema dell'accesso ai dati; 4.2. Il perimetro UE e le eccezioni; 4.3. Machine unlearning e diritto all'oblio; 4.4. Prompt injection e rischi per l'integrità processuale. – 5. La proprietà intellettuale del dato giurisprudenziale: 5.1. Le sentenze come opere dell'ingegno; 5.2. Il diritto sui generis del costituente della banca dati; 5.3. Text and data mining dopo la L. 132/2025. – 6. Verso un modello integrato di governo del dato giudiziario: 6.1. Il modello delle linee guida distrettuali; 6.2. La massimazione assistita da IA; 6.3. La sfida dell'interoperabilità; 6.4. Il magistrato come «garante umano». – 7. Conclusioni. – Riferimenti bibliografici.

1. Premessa: la giurisprudenza come «dato»

La trasformazione digitale ha operato una silenziosa ma profonda metamorfosi sulla natura stessa del precedente giudiziario. Ciò che per secoli era stato un testo cartaceo custodito negli archivi dei tribunali – accessibile con difficoltà, consultabile fisicamente, spesso noto soltanto agli addetti ai lavori – è divenuto oggi un dato strutturato, ricercabile per chiavi semantiche, estraibile mediante algoritmi, aggregabile in corpus di milioni di provvedimenti, riproducibile, vendibile e persino addestrabile come set di training per modelli di linguaggio di grandi dimensioni (c.d. LLM, Large Language Models)¹.

Questa metamorfosi non è meramente tecnologica. Essa ridefinisce il perimetro concettuale entro cui si collocano istituti classici del diritto pubblico e privato: la pubblicità delle decisioni, il diritto alla privacy delle parti processuali, la riservatezza dei terzi menzionati negli atti, la titolarità dei diritti sulle raccolte sistematiche, la responsabilità per l'uso distorto delle informazioni estratte. La sentenza, una volta digitalizzata, smette di essere soltanto un atto autoritativo che risolve una controversia: diventa un oggetto informativo dotato di vita autonoma, capace di circolare in contesti radicalmente diversi da quello in cui è stato prodotto.

Il fenomeno pone interrogativi inediti su tre grandi assi tematici, che questo contributo intende percorrere sistematicamente: (i) la raccolta, la diffusione e l'anonimizzazione dei dati giurisprudenziali; (ii) l'utilizzo di strumenti di intelligenza artificiale generativa – in primis Microsoft Copilot – nell'ecosistema della giustizia e i relativi rischi per l'integrità del dato processuale; (iii) la proprietà intellettuale sulle banche dati giurisprudenziali, con il paradosso tutto italiano di dati pubblici custoditi in banche dati proprietarie.

La specificità del dato giudiziario rispetto ad altri dati pubblici impone una riflessione metodologica preliminare. Il provvedimento del giudice non è un documento amministrativo qualunque: esso è il prodotto di una funzione costituzionale, è destinato strutturalmente alla pubblicità (artt. 101 e 111 Cost.; art. 6 CEDU), e al contempo contiene informazioni sensibilissime su persone fisiche che sono state coinvolte – spesso loro malgrado – in vicende processuali. Il bilanciamento tra questi valori è l'alfa e l'omega di ogni discorso serio sull'IA applicata alla giustizia.

L'approccio metodologico seguito in queste pagine combina l'analisi normativa, la casistica giurisprudenziale italiana ed europea e la riflessione critica sulla specificità del dato giudiziario. Il contributo si propone non soltanto di mappare il quadro regolatorio vigente, ma di identificare le tensioni strutturali che esso non riesce ancora a risolvere e di formulare proposte operative per un modello integrato di governo del dato giudiziario nell'era dell'intelligenza artificiale.

2. Il quadro normativo multilivello

Chi si accosti oggi alla materia si trova a navigare un arcipelago normativo di straordinaria complessità, nel quale si sovrappongono – non sempre coerentemente – fonti di diverso livello gerarchico e di diversa provenienza geografica: documenti internazionali di soft law, regolamenti europei direttamente applicabili, leggi nazionali di attuazione, linee guida di organismi di autogoverno della magistratura. Questa stratificazione normativa rispecchia la natura intrinsecamente trasversale del fenomeno IA applicato alla giustizia, che incide simultaneamente su tutela dei dati personali, diritti fondamentali, organizzazione dell'amministrazione della giustizia e disciplina della proprietà intellettuale.

2.1. Le Linee guida UNESCO 2025 per l'uso dei sistemi IA nei tribunali

Le Guidelines for the Use of AI Systems in Courts and Tribunals, pubblicate dall'UNESCO nel 2025 con il finanziamento della Commissione europea nell'ambito del progetto «*Supporting Member States in Implementing UNESCO's Recommendation on the Ethics of AI through Innovative Tools*», costituiscono il primo quadro etico e operativo globale specificamente dedicato all'impiego dell'intelligenza artificiale nel settore giudiziario (UNESCO, 2025)². Il documento è stato elaborato sulla base di un'attività decennale di formazione di oltre 36.000 operatori giudiziari in più di 160 Paesi, di un'ampia consultazione pubblica svolta nell'agosto-settembre 2024 che ha prodotto oltre cento contributi da 41 Paesi, e di una revisione da parte di venti esperti internazionali.

Le Linee guida articolano i propri contenuti intorno a quindici principi universali, pensati per orientare le organizzazioni e gli individui che fanno parte del sistema giudiziario lungo l'intero ciclo di vita dei sistemi IA: (1) protezione dei diritti umani; (2) proporzionalità; (3) fattibilità dei benefici; (4) sicurezza; (5) sicurezza delle informazioni; (6) accuratezza e affidabilità; (7) spiegabilità; (8) auditabilità; (9) giustizia trasparente e aperta; (10) consapevolezza e uso informato; (11) responsabilità; (12) responsabilizzazione e contestabilità; (13) supervisione umana e processo decisionale; (14) progettazione umanocentrica e partecipativa; (15) governance e collaborazione multi-stakeholder.

Il principio 1 merita un esame specifico nell'ottica del presente contributo. Le Linee guida distinguono quattro diritti fondamentali di rilievo peculiare nel contesto dei procedimenti giudiziari: non discriminazione, eguaglianza, equità procedurale e diritto alla privacy e alla protezione dei dati personali. Su quest'ultimo profilo, il documento afferma che le organizzazioni giudiziarie devono evitare sistemi IA che generino rischi di divulgazione di dati personali o consentano accessi non autorizzati da parte di terzi, e che «*techniques d'anonymisation des données doivent être employées lorsque les systèmes d'IA traitent des données personnelles, en particulier lors de la création de bases de données utilisées à des fins d'analyse juridique ou d'étude des précédents*» (principio 1.1d), precisando che tale anonimizzazione deve essere bilanciata con l'esigenza di open data e con il diritto alla libertà di espressione.

Sul tema specifico dei sistemi IA generativi, le Linee guida contengono un'apposita sezione (2.3) rivolta alle organizzazioni giudiziarie, che si articola in tre raccomandazioni operative: (a) garantire che i membri della magistratura che utilizzeranno strumenti di IA generativa siano consapevoli degli usi adeguati, delle limitazioni e dei rischi associati, con particolare riguardo agli output distorti o errati; (b) assicurare l'autenticità e l'integrità dei contenuti prodotti, segnalando chiaramente i documenti prodotti con il

supporto dell'IA e istituendo sistemi di tracciamento delle modifiche; (c) adottare specifiche restrizioni d'uso, vietando in particolare le applicazioni che prevalgano come probabilità di comportare gravi violazioni dei diritti umani e quelle i cui termini di servizio prevedano l'utilizzo dei prompt degli utenti per addestrare i propri modelli o che consentano a terzi l'accesso ai relativi prompt.

Di notevole interesse pratico è la sezione 3 delle Linee guida, dedicata alle raccomandazioni per i singoli membri della magistratura. Prima di utilizzare uno strumento IA, il magistrato deve: verificare le policy istituzionali dell'ufficio; esaminare se sia stata condotta una valutazione di impatto etico; comprendere il funzionamento dello strumento, incluse le sue impostazioni di protezione dei dati; chiarire il regime di responsabilità in caso di errori; investire nella formazione continua. Durante l'utilizzo, il magistrato deve evitare l'eccessivo affidamento ai sistemi IA per decisioni di merito, aderire ai termini di servizio, garantire trasparenza nei confronti delle parti e responsabilizzarsi per gli output prodotti. Per i sistemi di IA generativa è inoltre richiesto di non inserire dati personali o riservati nei prompt, verificare sempre gli output prima di utilizzarli in atti giudiziari, e non sostituire le testimonianze di periti con output degli LLM.

Le Linee guida sottolineano infine un aspetto di grande rilievo metodologico: l'elenco dei dieci usi raccomandabili degli strumenti generativi per i magistrati – tra cui la correzione di bozze amministrative, la riorganizzazione dei riferimenti bibliografici, la comparazione di testi, la predisposizione di presentazioni, la generazione di codice informatico, l'esplorazione iniziale di argomenti, il brainstorming, la strutturazione delle argomentazioni, l'esame di spiegazioni alternative su questioni di diritto e la generazione di riassunti – non include in alcun modo la redazione autonoma di sentenze o motivazioni, confermando il ruolo rigorosamente ausiliario che questi strumenti devono svolgere nel processo giurisdizionale (UNESCO, 2025, pp. 29-30).

2.2. Il documento «AI Essentials for Judges» (UNESCO 2026)

Complementare alle Linee guida è il documento *AI Essentials for Judges*, pubblicato dall'UNESCO nel 2026 nell'ambito dello stesso programma *AI & Rule of Law*, specificamente concepito per fornire risposte rapide alle domande più frequenti dei magistrati sull'intelligenza artificiale, senza presupporre competenze tecniche pregresse (UNESCO, 2026)³. Il documento nasce dalle rilevazioni del sondaggio UNESCO del 2023 condotto su operatori giudiziari di 96 Paesi⁴, che ha accertato come il 44% dei professionisti legali integrasse già l'IA nel proprio lavoro, mentre soltanto il 9% dei rispondenti avesse ricevuto formazione o linee guida istituzionali in materia: un divario allarmante tra adozione spontanea e regolazione strutturata.

Il documento è organizzato in sei aree tematiche: definizioni di IA e IA generativa; sviluppo e uso dell'IA nel settore giudiziario; uso dell'IA da parte dei giudici; benefici potenziali per le parti; rischi; azioni preventive e correttive. Tra i contenuti di maggiore interesse per il tema del presente contributo, si segnalano le risposte alle domande sui rischi per la riservatezza dei dati giudiziari e sulla cybersicurezza (domanda 11), sul rischio di profilazione dei giudici da parte di sistemi di predizione delle decisioni (domanda 12), e sui meccanismi di impugnazione delle decisioni assunte con il supporto dell'IA (domanda 17). Sul primo punto, il documento avverte che una violazione dei dati potrebbe esporre informazioni sensibili su giudici, parti e fascicoli, minacciando la sicurezza personale e minando la fiducia nel sistema giudiziario, e che i giudici devono anche tutelare la propria privacy intellettuale professionale, poiché la profilazione algoritmica dei loro ragionamenti o delle loro preferenze potrebbe compromettere l'indipendenza giudiziaria orientando o anticipando le loro decisioni.

Sul meccanismo di impugnazione, *AI Essentials for Judges* richiama espressamente l'art. 22 GDPR sul diritto all'intervento umano nelle decisioni automatizzate e l'art. 86 AI Act,

che riconosce ai soggetti interessati da decisioni assunte con il supporto dell'IA il diritto di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema IA nel procedimento decisionale e sugli elementi principali della decisione adottata. Questa disciplina è applicabile nei tribunali per gli strumenti IA classificati come ad alto rischio ai sensi dell'Allegato III dell'AI Act, categoria che – come si è già osservato – include i sistemi IA destinati all'amministrazione della giustizia.

2.3. Il Regolamento sull'intelligenza artificiale (AI Act)

Il Regolamento (UE) 2024/1689 – comunemente noto come *AI Act*⁵ – classifica i sistemi IA destinati all'amministrazione della giustizia e alla gestione dei procedimenti come sistemi «ad alto rischio» ai sensi dell'Allegato III (Sartor – Lagioia, 2024, p. 891)¹⁴. Questa classificazione, che copre specificatamente i sistemi «*intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution*» (punto 8(a) dell'Allegato III), implica obblighi stringenti di conformità: valutazione del rischio ex ante, registrazione in appositi database europei, trasparenza nei confronti degli utenti, meccanismi di sorveglianza umana, test di robustezza e sicurezza.

Particolarmente rilevante per il tema in esame è l'art. 10 AI Act, che impone requisiti severi in materia di qualità dei dati di addestramento, validazione e test: i sistemi IA utilizzati in ambito giudiziario devono essere alimentati da dati rappresentativi, privi di distorsioni sistematiche e adeguatamente documentati. L'AI Act crea, peraltro, una tensione strutturale con la realtà delle banche dati giurisprudenziali italiane ed europee: questi archivi – che costituiscono la materia prima per l'addestramento dei modelli IA applicati alla giustizia – sono costruiti su anni di oscuramento selettivo, eterogeneità dei criteri di massimazione, lacune documentali. Il rischio di «garbage in, garbage out» è tutt'altro che teorico.

Le disposizioni sulla contestabilità delle decisioni assunte con il supporto dell'IA (art. 86 AI Act, già richiamato da AI Essentials for Judges) si inseriscono in un quadro più ampio di garanzie procedurali che l'AI Act pone a carico dei deployers di sistemi ad alto rischio. Sul piano processuale, esse aprono uno scenario nuovo per la pratica giudiziaria italiana: la parte di un procedimento che ritenga che una decisione sia stata influenzata in modo determinante dall'output di un sistema IA potrà invocare queste disposizioni per ottenere informazioni sul funzionamento del sistema e contestarne le conclusioni.

2.4. Il quadro del Consiglio d'Europa e le Guidelines CEPEJ 2025

Il quadro multilivello è completato dagli strumenti elaborati dal Consiglio d'Europa. La Carta etica europea della CEPEJ del 2018 ha posto cinque principi – rispetto dei diritti fondamentali, non discriminazione, qualità e sicurezza, trasparenza e controllo dell'utilizzatore – successivamente tradotti in criteri operativi di valutazione. Le Guidelines on the use of generative AI for courts, adottate dalla CEPEJ nel dicembre 2025¹⁹, muovono da un criterio di proporzionalità tecnologica: individuare anzitutto il problema organizzativo, verificare se possa essere risolto con strumenti meno complessi e ricorrere all'IA generativa soltanto quando il beneficio atteso sia concreto e misurabile.

Le Guidelines richiedono sperimentazioni controllate, metriche preventive, tracciabilità, sicurezza giuridica, indipendenza del giudice e sorveglianza umana effettiva. Particolare rilievo assume il principio di reversibilità: l'introduzione del sistema deve poter essere sospesa o corretta quando gli esiti non raggiungano le soglie attese o emergano rischi non previsti. La supervisione non è considerata una semplice approvazione finale, ma una funzione organizzativa sostenuta da formazione, accesso alle fonti, tempi adeguati per la verifica e possibilità reale di discostarsi dall'output.

UNESCO e CEPEJ convergono così su una medesima architettura: IA assistiva e non sostitutiva, valutazione preventiva degli impatti, governo dell'intero ciclo di vita, controllo umano significativo e responsabilità istituzionale. Questi standard di soft law non sostituiscono l'AI Act, ma ne orientano l'applicazione nel settore giudiziario, dove l'efficienza non può essere separata dalla qualità del processo e dalla fiducia degli utenti.

2.5. La legge italiana n. 132/2025 e le Raccomandazioni CSM

Sul versante nazionale, la L. 9 agosto 2025, n. 132, recante «Disposizioni in materia di intelligenza artificiale»¹⁵, ha introdotto nell'ordinamento italiano un complesso di norme specificamente dedicate all'IA nel settore pubblico, con disposizioni di particolare rilievo per l'amministrazione della giustizia. Tra queste, meritano speciale attenzione: la disciplina del «machine unlearning» (art. 17), che riconosce il diritto alla cancellazione dei propri dati dai modelli IA già addestrati; le norme sull'opt-out per il text and data mining nel settore della ricerca scientifica (art. 24, che modifica gli artt. 70-ter e 70-quater della legge sul diritto d'autore); le disposizioni sulla trasparenza algoritmica nelle decisioni amministrative (art. 31). L'art. 15 riserva al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti; attribuisce al Ministero della giustizia la disciplina degli impieghi destinati all'organizzazione dei servizi, alla semplificazione del lavoro giudiziario e alle attività amministrative accessorie, nonché – nella fase transitoria – l'individuazione dei sistemi autorizzati. La legge prevede inoltre la formazione specifica dei magistrati e del personale e affida ai decreti attuativi il raccordo pieno con l'AI Act. Le Raccomandazioni del CSM dell'8 ottobre 2025 sull'utilizzo dell'IA da parte dei magistrati¹⁶ completano il quadro interno. Il documento consiliare si articola in linee guida operative che, pur non avendo forza di legge, esprimono l'interpretazione autentica dell'organo di autogoverno della magistratura italiana in ordine ai limiti e alle cautele nell'impiego degli strumenti algoritmici, posizionandosi nel solco delle Linee guida UNESCO e anticipandone in parte i contenuti nel contesto ordinamentale italiano. In particolare, le Raccomandazioni insistono sulla necessità che il magistrato mantenga la piena responsabilità dell'atto decisorio, utilizzi gli strumenti IA soltanto come supporto nella ricerca di precedenti e nella redazione delle minute, e verifichi criticamente gli output prima di recepirli nei provvedimenti.

2.6. Il ruolo dell'EJTN e del programma Digital Ambassador

La dimensione europea della formazione digitale dei magistrati si sviluppa principalmente attraverso la Rete Europea di Formazione Giudiziaria (EJTN) e il suo programma Digital Ambassador. Questo percorso si inserisce coerentemente nella visione espressa dall'UNESCO in AI Essentials for Judges: il documento UNESCO del 2026 sottolinea che i programmi di formazione continua, i laboratori pratici e le risorse educative online sono essenziali per consentire ai giudici e al personale dei tribunali di comprendere e utilizzare efficacemente gli strumenti IA, e che queste sessioni devono tenersi a intervalli regolari per consolidare le competenze e favorire lo scambio di buone pratiche (UNESCO, 2026, p. 9).

La coerenza tra le iniziative formative dell'EJTN e le indicazioni UNESCO è confermata dal fatto che le Linee guida del 2025 raccomandano esplicitamente (punto 2.2.1) di incorporare i temi dell'IA nei curricula permanenti delle scuole di formazione giudiziaria, includendo le basi dell'IA, le applicazioni delle tecnologie AI nei sistemi giudiziari e l'impatto dell'IA sull'indipendenza dei giudici, sull'amministrazione della giustizia e in particolare sulle questioni relative ai diritti umani, all'etica e ai modelli di governo. L'istruzione giudiziaria in materia di IA cessa così di essere un optional e diventa una componente strutturale della professionalità del giudice contemporaneo, da garantire attraverso programmi istituzionali e non lasciata all'iniziativa individuale del singolo magistrato.

2.7. L'aggiornamento CSM del 22 luglio 2026: l'apertura controllata agli atti giudiziari e il governo del rischio

L'aggiornamento delle Raccomandazioni approvato dal Consiglio superiore della magistratura nella seduta del 22 luglio 2026²⁰ segna il passaggio da una disciplina prevalentemente prudenziale a un assetto di regolazione operativa dell'impiego dell'intelligenza artificiale negli uffici giudiziari. Il documento non dismette le cautele elaborate nel 2025, ma le ricolloca in un contesto mutato: la sperimentazione di Microsoft 365 Copilot, l'acquisizione di specifiche garanzie tecniche e le prime risultanze maturate negli uffici consentono di affrontare non più soltanto l'eventualità dell'uso, bensì le condizioni concrete della sua ammissibilità. La stessa delibera dichiara, in premessa, che le raccomandazioni dell'8 ottobre 2025

«costituiscono il quadro di riferimento vigente e conservano piena validità nei principi, nel perimetro normativo e nelle cautele operative ivi indicate. 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».

Il rapporto tra i due documenti è, pertanto, di continuità nei principi e di progressione sul piano applicativo. La precedente cautela non viene superata in nome di una generica fiducia nella tecnologia, ma trasformata in un insieme più analitico di condizioni, limiti e responsabilità: il mutamento investe il presupposto tecnico e organizzativo dell'impiego, non già la titolarità umana della funzione né la qualità delle garanzie che devono accompagnarla.

2.7.1. Continuità dei principi e riserva della funzione giurisdizionale

Restano fermi, quali principi irrinunciabili, l'autonomia decisionale del magistrato e la supervisione umana obbligatoria. Quanto alla prima, la delibera ribadisce che «ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti è e rimane di esclusiva competenza del magistrato, che non può delegarla ad alcun sistema di intelligenza artificiale»; quanto alla seconda, che «ogni output prodotto da sistemi di intelligenza artificiale deve essere oggetto di verifica, valutazione critica e validazione da parte del magistrato prima di qualsiasi utilizzo».

La riserva della decisione costituisce il nucleo indisponibile dell'intero impianto. L'aggiornamento non si limita a esigere che il provvedimento sia formalmente imputabile al magistrato, ma pretende che rimangano effettivamente umane la comprensione del fascicolo, la qualificazione giuridica, la valutazione probatoria e la scelta decisoria. Ne consegue che la supervisione non può esaurirsi nella sottoscrizione finale: essa deve intervenire nel corso dell'elaborazione, consentire il ritorno alle fonti e rendere possibile la correzione, l'integrazione o il rigetto dell'output. La previsione di checkpoint obbligatori e bloccanti traduce tale esigenza in una regola di processo, impeditiva della prosecuzione automatica del flusso in assenza di un atto espresso di validazione; affinché il presidio non degradi a formalità, la validazione deve corrispondere a un controllo intelligibile e documentabile sul contenuto elaborato.

2.7.2. Le garanzie tecniche e la delimitazione dell'ambiente autorizzato

Il mutamento del quadro di valutazione riposa sulle garanzie tecniche comunicate dal Ministero della giustizia in ordine al servizio operante nel dominio giustizia: «residenza dei dati in Italia: il Ministero della giustizia ha acquisito il componente Advanced Data Residency (ADR), che garantisce la memorizzazione dei dati, inclusi i contenuti delle interazioni con Copilot, nei datacenter localizzati in Italia [...]; isolamento del tenant: il tenant del Ministero della giustizia costituisce un'istanza logicamente

separata da tutti gli altri tenant Microsoft 365 [...]; 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 [...]; controllo sulla classificazione dei documenti: il Ministero può classificare i documenti sensibili tramite etichette di riservatezza (Microsoft Purview) [...], e può configurare o disabilitare la funzionalità di ricerca web».

Tali garanzie consentono di distinguere nettamente l'impiego istituzionale dalle forme di uso informale di applicazioni consumer: il dato giudiziario non è affidato a un ambiente aperto e indifferenziato, ma trattato entro un dominio autorizzato, dotato di separazione logica, regole di accesso e misure di protezione configurabili dall'amministrazione. La delimitazione dell'ambiente costituisce, dunque, una condizione preliminare di ammissibilità, non una mera preferenza tecnica. La sicurezza, nondimeno, non coincide con una qualità immutabile del prodotto: essa dipende dalla configurazione concreta delle autorizzazioni, dall'impiego delle etichette di riservatezza, dalla minimizzazione dei dati, dalla disciplina dei log, dalla gestione degli aggiornamenti e dalla verifica periodica delle condizioni dichiarate. Le garanzie tecniche vanno pertanto intese come un processo continuativo di controllo e adeguamento, e non come un attributo acquisito una volta per tutte.

2.7.3. L'apertura sperimentale al trattamento degli atti giudiziari

Il cuore dispositivo dell'aggiornamento risiede nell'estensione del perimetro degli usi consentiti. Il Consiglio ritiene infatti che «l'uso di Microsoft 365 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».

L'apertura è circoscritta e subordinata al concorso di condizioni cumulative: trattamento dei dati nel solo tenant istituzionale, con anonimizzazione preventiva raccomandata quale buona pratica quando l'identificazione dei soggetti non sia necessaria alla finalità perseguita; operatività esclusiva nel dominio giustizia, con divieto delle versioni consumer e degli altri sistemi non autorizzati; supervisione umana obbligatoria e bloccante; impiego di prompt strutturati; adeguata formazione tecnica dell'utilizzatore. Il carattere cumulativo delle condizioni impedisce che una singola garanzia sia assunta a equivalente dell'intero sistema di protezione. In coerenza con quanto sopra osservato in tema di anonimizzazione (§§ 3.3 e 3.4), la scelta consigliare di raccomandare — e non imporre — l'anonimizzazione preventiva conferma la preferenza per una minimizzazione ragionata del dato, calibrata sullo scopo e sul rischio concreto, anziché per un automatismo indistinto.

Sul piano applicativo, l'elenco degli usi consentiti dalle Raccomandazioni del 2025 è confermato e ampliato: ai sette impieghi già previsti si aggiungono cinque nuove attività, ammesse «nel rispetto delle condizioni di cui al paragrafo 4 del presente documento [...], a titolo esemplificativo e non esaustivo»:

«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».

L'elenco descrive una progressione che muove dalle attività di ordinamento documentale verso operazioni più prossime alla ricostruzione del caso. Proprio per questo, il

nomen dell'attività non basta a determinarne il regime: una classificazione ristretta a categorie predeterminate non equivale a una selezione di rilevanza; una sintesi meramente estrattiva non coincide con una ricostruzione che risolva contraddizioni o attribuisca peso agli elementi; la compilazione di dati anagrafici in un modulo non è assimilabile alla formulazione di campi che richiedano qualificazioni giuridiche o apprezzamenti di proporzionalità. Restano in ogni caso esclusi, per espressa previsione, «la formulazione del dispositivo e l'affidamento della redazione dei provvedimenti giurisdizionali», nonché l'uso di sistemi generativi non autorizzati dal Ministero e al di fuori del sistema giustizia.

2.7.4. La linea di confine tra attività ricostruttiva e attività valutativa

La distinzione accolta dalla delibera offre un criterio operativo fecondo: l'intelligenza artificiale può concorrere a estrarre domande, eccezioni, date, documenti citati e relazioni già rappresentate nel fascicolo; non può, invece, attribuire credibilità, stabilire autonomamente la decisività di un elemento, colmare lacune, suggerire la soluzione o predisporre il percorso motivazionale. La verificabilità documentale diviene, così, la prima misura della legittimità dell'ausilio: ogni affermazione rilevante deve poter essere ricondotta senza ambiguità alla fonte da cui è tratta²¹.

La fase ricostruttiva non è, tuttavia, cognitivamente indifferente. Ordinare gli atti, selezionare categorie e rappresentare le posizioni delle parti può influire sulla salienza delle informazioni e sulla cornice iniziale del ragionamento. Il rilievo non impone di escludere l'ausilio, ma di incorporare la cautela nella progettazione del caso d'uso: tassonomie predeterminate, indicazione puntuale delle fonti, esplicitazione delle omissioni e delle incertezze, possibilità di visualizzare versioni alternative e checkpoint che richiedano un contributo effettivo del magistrato²². Ne deriva una posizione di equilibrio: l'analisi può rimanere ausiliaria anche quando riduca il costo cognitivo della prima ricognizione, purché il sistema non definisca autonomamente la cornice giuridica del caso e il magistrato conservi il dominio della selezione, della qualificazione e della verifica. Il rischio di condizionamento va, così, assunto come elemento da prevenire e misurare, non come ragione per assimilare ogni attività ricostruttiva alla decisione.

2.7.5. Il coordinamento con la disciplina europea dei sistemi ad alto rischio

Il catalogo consiliare deve essere coordinato con l'art. 6 e con l'Allegato III, punto 8, dell'AI Act. Il regolamento qualifica ad alto rischio i sistemi destinati ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a un insieme concreto di fatti; al tempo stesso, sottrae a tale qualificazione le attività meramente procedurali o preparatorie che non incidano materialmente sull'esito della valutazione umana. La classificazione va dunque condotta sul singolo caso d'uso: la catalogazione documentale secondo classi prestabilite può mantenersi nell'area dei compiti procedurali ristretti, mentre un sistema che individui autonomamente questioni giuridicamente rilevanti, lacune probatorie o rapporti tra fatti e fattispecie normativa si avvicina all'assistenza giudiziaria ad alto rischio; tra i due poli si colloca una fascia intermedia, che esige la descrizione della finalità, dell'output, del grado di autonomia e della concreta capacità di influenzare il giudizio.

Sul piano temporale, il Regolamento (UE) 2026/1744 ha fissato al 2 dicembre 2027 l'applicazione dei requisiti e degli obblighi relativi ai sistemi ad alto rischio dell'Allegato III²³. Il differimento non sospende i principi costituzionali, processuali e di protezione dei dati; offre, piuttosto, uno spazio nel quale predisporre registri dei casi d'uso, valutazioni d'impatto sui diritti fondamentali, metriche di accuratezza e completezza, protocolli di supervisione e procedure di gestione degli incidenti. La stessa delibera consiliare ribadisce, del resto, che i principi 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».

2.7.6. I limiti del modello generalista e la prospettiva di una suite dedicata

L'apertura sperimentale non oblitera i limiti strutturali dello strumento, che la delibera enuncia con inusuale nettezza. Essa riconosce, in particolare, che «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», e ne documenta le criticità rilevate in sede di sperimentazione — carenza di grounding documentale; «allucinazioni» anche su corpus documentale chiuso, come attesta l'inserimento di un riferimento a un Comune inesistente in un'attività di catalogazione svolta in ambiente protetto e su documentazione trattata con OCR, nonostante l'istruzione esplicita di attenersi ai soli documenti forniti; inserimento di collegamenti ipertestuali fittizi; tendenza a fornire risposte conclusive anziché segnalare i limiti informativi incontrati.

Il riconoscimento di tali limiti non contraddice l'apertura, ma ne delimita il significato: la scelta consiste nel sottoporre lo strumento disponibile a impieghi circoscritti, verificabili e reversibili, utilizzando la sperimentazione anche per individuare i requisiti della soluzione futura. La delibera afferma, in termini conclusivi, 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». La prospettiva di una suite dedicata trasferisce, così, parte del peso dal controllo individuale alla responsabilità infrastrutturale: il magistrato resta responsabile dell'uso concreto del risultato, ma non può essere chiamato a supplire, da solo e caso per caso, a difetti che devono essere prevenuti in sede di progettazione — tracciabilità nativa delle fonti, gestione del corpus documentale, controllo delle versioni, verificabilità *ex post*, sicurezza, valutazione indipendente e possibilità di arrestare o correggere il sistema.

2.7.7. Sperimentazione, formazione e regolazione evolutiva

Il Consiglio colloca il singolo impiego all'interno di un ciclo istituzionale più ampio, reputando necessari 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», l'istituzione di una sandbox regolatoria congiunta per la sperimentazione controllata e la condivisione delle sperimentazioni avanzate — segnatamente quelle del Tribunale di Catania e della Procura generale di Perugia — affinché i risultati siano messi a disposizione degli uffici come modelli replicabili. La sandbox non dovrebbe risolversi in un ambiente di mera permissività, ma costituire la sede nella quale rendere espliciti criteri, metriche, responsabilità e condizioni di arresto della sperimentazione; sul piano attuativo, converrà chiarirne il raccordo con la sandbox a regime prevista dall'art. 20, comma 1, lett. c), l. n. 132/2025, onde evitare la moltiplicazione di sedi sperimentali concorrenti.

La formazione assume, in tale prospettiva, natura strutturale: essa deve comprendere non soltanto il fenomeno delle allucinazioni e le tecniche di verifica, ma altresì l'eccessivo affidamento nell'automazione, la tutela dei log, la gestione delle fonti, la classificazione del rischio e la capacità di riconoscere quando una funzione apparentemente ausiliaria si avvicini alla valutazione. Preservare l'integrità cognitiva del magistrato significa, in termini operativi, far sì che egli continui a esercitare le operazioni che fondano il giudizio — formulare le questioni, confrontare le alternative, verificare le fonti e motivare la scelta: l'intelligenza artificiale può alleggerire le attività ripetitive, non già rendere passivo il controllo che ne giustifica l'impiego.

2.7.8. Grounding, supervisione e integrità del processo cognitivo: la prima tradu-

zione giurisprudenziale

Alle carenze di grounding, alle allucinazioni, ai collegamenti fittizi e alla tendenza del modello a colmare le lacune informative la risposta più coerente non risiede in formule generiche del prompt, bensì nella progettazione di output verificabili: per ciascuna informazione devono essere indicati il documento e il passaggio di origine; le inferenze devono essere tenute distinte dai dati estratti; le contraddizioni e le informazioni mancanti devono essere segnalate; il sistema deve poter dichiarare che il fascicolo non consente una conclusione affidabile.

L'esigenza di un controllo effettivo ha ricevuto una prima, netta traduzione giurisprudenziale in Cass. pen., Sez. III, 11 giugno 2026, dep. 22 giugno 2026, n. 23006²⁴. La Corte, dopo aver riscontrato nel ricorso la citazione di precedenti inesistenti o alterati, ricondotti a un fenomeno di «allucinazione informatica», afferma che

«il richiamo, nel ricorso per cassazione, di precedenti giurisprudenziali inesistenti o “allucinati” da sistemi di intelligenza artificiale costituisce un indice particolarmente significativo di colpa qualificata nella determinazione della causa di inammissibilità e, proprio per questo, giustifica l'irrogazione di una sanzione più elevata ai sensi dell'art. 616 cod. proc. pen. quando la Corte, come nel caso di specie, ravvisi che il ricorso è stato proposto senza il minimo controllo professionale sulla veridicità e pertinenza delle fonti invocate».

Il punto decisivo — prosegue la Corte — è che «l'utilizzo di strumenti di intelligenza artificiale non vale di per sé a escludere la colpa, perché il professionista che redige e sottoscrive il ricorso conserva integralmente il controllo dell'atto e la responsabilità della sua conformità ai canoni di verità, pertinenza e specificità»; né può sostenersi che l'impiego dell'intelligenza artificiale introduca «una zona franca di deresponsabilizzazione», poiché l'errore non è inevitabile, bensì «prevenibile con l'ordinaria diligenza professionale: sarebbe bastato verificare la reale esistenza delle decisioni, il loro numero, la sezione, la data e la massima pertinente».

La pronuncia riguarda direttamente l'atto difensivo e la colpa processuale ai sensi dell'art. 616 c.p.p., ma esprime un criterio suscettibile di proiezione sull'intero ecosistema giudiziario: l'impiego di uno strumento generativo non trasferisce alla macchina la responsabilità del contenuto, né riduce il livello di diligenza esigibile. La supervisione umana non è, quindi, una formula organizzativa o un controllo meramente finale, ma un dovere professionale concretamente misurabile nella verifica dell'esistenza, dell'esattezza e della pertinenza delle fonti e nella piena riconducibilità dell'atto alla persona che lo assume. Il principio si raccorda alla delibera del Consiglio, che prescrive una verifica obbligatoria e bloccante degli output, e ne rivela la dimensione sostanziale: quanto maggiore è la capacità dello strumento di produrre testi plausibili, tanto più rigoroso deve essere il controllo sulle informazioni che ne costituiscono il fondamento.

Il prompt strutturato riduce lo spazio interpretativo della macchina; il checkpoint bloccante assicura che il flusso non proceda senza un atto umano. Perché la supervisione sia sostanziale, il checkpoint deve richiedere un'attività verificabile — confronto con la fonte, correzione, integrazione o esplicita conferma delle categorie estratte — e non un mero comando di prosecuzione. In questa dimensione, la tutela dell'integrità cognitiva completa il modello della supervisione: il controllo deve proteggere tanto la correttezza dell'output quanto la capacità del magistrato di costruire autonomamente la cornice giuridica e probatoria. La tracciabilità, infine, deve essere proporzionata: è opportuno conservare, per gli usi significativi, il sistema e la versione, la finalità, i documenti elaborati, i prompt rilevanti, gli output e le verifiche effettuate, impedendo al tempo stesso che i log siano riutilizzati per profilare orientamenti, produttività o stile decisionale del singolo magistrato. Auditabilità del sistema e divieto di profilazione non sono principi opposti, ma esigono regole di accesso, tempi di conservazione e finalità rigidamente predeterminati.

3. Anonimizzazione e pubblicità delle decisioni: un equilibrio instabile

Il nodo dell'anonimizzazione delle sentenze è forse il punto di massima tensione nell'intera materia. Esso concentra, come in un prisma, le contraddizioni di un sistema che aspira simultaneamente alla trasparenza della giustizia e alla protezione dei dati personali, alla libera circolazione delle informazioni e alla tutela della riservatezza, all'efficienza della ricerca giuridica e al rispetto della dignità delle persone coinvolte nei procedimenti. Le Linee guida UNESCO del 2025 colgono puntualmente questa tensione quando affermano che l'anonimizzazione «*doit être mise en balance avec la nécessité d'avoir des ensembles de données ouverts ainsi que du droit à la liberté d'expression et d'accès à l'information afin de ne pas entraver le développement des systèmes de justice numérique*», e che «*la manière dont ces droits sont mis en balance dans la pratique dépend de la façon dont chaque juridiction régit le droit d'accès aux documents judiciaires et les règles d'anonymisation découlant des lois sur la protection des données et la vie privée*» (punto 2.1.16).

3.1. La sentenza TAR Lazio n. 7625/2025

La sentenza TAR Lazio, Roma, Sez. I, 17 aprile 2025, n. 7625⁷ ha aperto una breccia significativa in un assetto che si era consolidato negli anni. La decisione non afferma un diritto indiscriminato alla pubblicazione integrale di ogni dato contenuto nei provvedimenti giudiziari, né contesta in sé la creazione della nuova banca dati di merito o l'adozione di sistemi di accesso tracciato. Il suo nucleo è più preciso: è illegittima la scelta amministrativa di oscurare in modo generalizzato e automatico tutti i dati personali contenuti nelle decisioni pubblicate nella banca dati pubblica, quando tale scelta impedisca la piena intelligibilità del precedente e sostituisca al bilanciamento concreto una regola uniforme di anonimizzazione massiva.

Il TAR valorizza, in particolare, gli artt. 51 e 52 del Codice privacy: le decisioni depositate in cancelleria o segreteria sono rese accessibili anche tramite sistemi informativi e siti istituzionali, ma osservando le cautele previste per la tutela dei dati. La clausola di cautela non autorizza però un oscuramento indistinto; impone, al contrario, un giudizio proporzionato, ragionevole e necessario. La protezione della riservatezza resta essenziale, specie nei procedimenti che coinvolgono minori, salute, famiglia, vittime di reati o dati particolari, ma deve essere calibrata dall'autorità giudiziaria procedente caso per caso, non decisa una volta per tutte dal gestore della banca dati. La decisione va dunque letta come arresto contro l'anonimizzazione amministrativa seriale, non contro l'anonimizzazione selettiva e motivata. La sentenza è significativa anche perché collega la pubblicità della giurisprudenza alla funzione pratica del precedente: senza una sufficiente comprensione del fatto, il ragionamento giuridico diviene astratto e non consente all'operatore di valutare analogia, differenza e distinguishing. In questo senso, la pubblicità non è mera esposizione del documento, ma accessibilità sostanziale del contenuto giuridicamente rilevante.

3.2. Il sistema delle fonti applicabile

Il quadro normativo rilevante è particolarmente stratificato. L'art. 6 CEDU, come interpretato dalla giurisprudenza di Strasburgo, esige che la giustizia sia resa in condizioni di conoscibilità pubblica, anche quando la forma concreta della pubblicità della decisione possa essere diversa dalla lettura integrale in udienza¹⁷. Tale principio non è assoluto: convive con l'art. 8 CEDU e con la tutela della vita privata, familiare e dei dati sensibili, che possono giustificare limitazioni, anonimizzazioni o forme selettive di pubblicazione¹⁸. Il GDPR - e in particolare l'art. 9, relativo ai dati particolari - impone restrizioni al

trattamento dei dati sensibili (stato di salute, orientamento sessuale, convinzioni religiose o politiche) che frequentemente compaiono nei testi delle sentenze. Gli artt. 51 e 52 del D.lgs. 196/2003, come modificati dal D.lgs. 101/2018, prevedono un regime speciale per il trattamento dei dati effettuato nell'esercizio della funzione giurisdizionale, sottratto in larga misura alle disposizioni ordinarie del Codice privacy. Le Linee guida del Garante del 2010, ormai superate dagli sviluppi tecnologici ma mai formalmente abrogate, continuano a fornire un riferimento operativo per gli uffici giudiziari.

L'intreccio tra queste fonti produce un quadro interpretativo di notevole complessità. La giurisprudenza del Garante per la protezione dei dati personali ha cercato di fornire criteri operativi per la redazione delle sentenze destinate alla pubblicazione, fondati sulla rimozione dei dati identificativi quando la loro ostensione non sia necessaria alla comprensione della decisione. Questo criterio, tuttavia, si rivela insufficiente in presenza di strumenti IA capaci di inferire l'identità delle persone da informazioni apparentemente neutre. La lezione che si ricava dalla giurisprudenza convenzionale è dunque duplice: la pubblicità della decisione garantisce controllo democratico sulla giurisdizione; la pubblicazione non può però trasformarsi in esposizione sproporzionata della sfera personale delle parti o dei terzi.

3.3. La sentenza CGUE «Deloitte» e la pseudonimizzazione

Di notevole interesse è la sentenza della Corte di Giustizia dell'Unione Europea del 4 settembre 2025 (C-413/23 P, European Data Protection Supervisor c. Single Resolution Board, cd. sentenza «Deloitte»)⁸, che ha affrontato il problema della pseudonimizzazione in un contesto diverso da quello giudiziario ma con implicazioni dirette per la materia in esame. La Corte ha chiarito che il dato pseudonimizzato non è automaticamente anonimo, ma ha anche confermato una concezione relativa del dato personale: occorre verificare, rispetto al soggetto che tratta o riceve l'informazione, se esistano mezzi ragionevolmente utilizzabili per re-identificare l'interessato. Al tempo stesso, quando si valuta l'obbligo informativo del titolare, la prospettiva rilevante resta quella del titolare al momento della raccolta, non soltanto quella del destinatario successivo.

Questa precisazione ha implicazioni dirette per le banche dati giurisprudenziali e introduce una distinzione analitica che la dottrina e la prassi hanno finora trascurato: quella tra anonimizzazione dei metadati, pseudonimizzazione del testo e anonimizzazione effettiva del contenuto narrativo della sentenza.

L'anonimizzazione dei metadati – la soppressione del nome delle parti, del numero di ruolo, della data dell'udienza e degli altri elementi formali di identificazione del fascicolo – costituisce, nella prassi corrente degli uffici giudiziari italiani, l'unica misura sistematicamente adottata prima della pubblicazione delle sentenze nelle banche dati ministeriali. Essa risponde a una logica di semplicità operativa, ed è quella che il TAR Lazio ha ritenuto insufficiente con la sentenza n. 7625/2025. Ma il problema è più profondo: un testo di sentenza può rivelare un caso specifico – e quindi identificare le persone coinvolte – anche in assenza di qualunque metadato, per il solo fatto della sua struttura narrativa. Si tratta di ciò che potremmo definire il 'paradosso dell'anonimizzazione per rimozione': non basta cancellare i nomi se la storia che il testo racconta è di per sé unica e identificante.

Il contenuto di una sentenza, per assolvere alla propria funzione di motivazione del provvedimento, deve descrivere i fatti in modo sufficientemente specifico da consentire la verifica della correttezza del ragionamento giuridico. Questa specificità narrativa è strutturalmente incompatibile con l'anonimizzazione piena: una sentenza in materia familiare che descriva un'adozione internazionale avvenuta in un determinato Paese nel corso di un anno preciso, con la menzione dell'età dei minori e della loro cittadinanza, il numero e il sesso dei figli, la professione dei genitori adottivi e il tribunale

minorile che ha rilasciato l'autorizzazione, è di per sé identificante, quand'anche tutti i nomi siano stati oscurati. Analogamente, una sentenza penale che descriva un reato tributario commesso attraverso una specifica operazione finanziaria, con l'indicazione del settore merceologico, della localizzazione geografica dell'impresa, dell'anno fiscale contestato e dell'importo evaso, consente a un operatore del settore – e a maggior ragione a un sistema IA dotato di capacità di ricerca incrociata – di risalire all'identità del soggetto con relativa facilità. Questo fenomeno, che la letteratura anglosassone denomina “*narrative re-identification*”, è strutturalmente diverso dal classico *re-identification risk* basato sulla combinazione di metadati: non richiede set di dati esterni, non necessita di algoritmi di matching, ma si produce per effetto della sola lettura attenta del testo.

L'impiego su larga scala di strumenti IA aggrava questo rischio in modo esponenziale. Un sistema LLM addestrato su un corpus di sentenze anonimizzate può: (i) ricordare frammenti narrativi sufficientemente specifici da ricostituire casi concreti in risposta a query mirate; (ii) collegare la descrizione fattuale contenuta in una sentenza con altre fonti pubbliche (articoli di stampa, atti amministrativi accessibili, registri pubblici) per completare il profilo dell'individuo; (iii) generare sintesi che, pur non citando esplicitamente le parti, ne riproducono la vicenda in modo tale da renderle riconoscibili per chiunque conosca il contesto. Questi rischi non sono meramente teorici: ricercatori nel campo della sicurezza informatica hanno dimostrato che modelli di linguaggio addestrati su testi giuridici sono capaci di recuperare informazioni specifiche su individui, anche quando il training set era stato formalmente depurato dei dati identificativi diretti (c.d. ‘memorizzazione involontaria’, fenomeno analizzato da Carlini et al., 2021, con riferimento ai grandi modelli linguistici)¹⁶. Le Linee guida UNESCO del 2025 recepiscono questa consapevolezza nella raccomandazione 2.1.16, imponendo alle organizzazioni giudiziarie di adottare tecniche di anonimizzazione che tengano conto dei rischi di re-identificazione attraverso l'analisi combinata dei dati, e di bilanciare tale tutela con le esigenze di open data e libertà di informazione. Ne consegue che la sfida dell'anonimizzazione nel settore giudiziario non può essere risolta con strumenti esclusivamente formali – la soppressione di nomi e date – ma richiede una revisione profonda delle tecniche redazionali delle sentenze destinate alla pubblicazione, una riflessione sulla granularità del dettaglio fattuale necessario e, sul versante tecnologico, l'adozione di approcci come la *differential privacy* o la generalizzazione semantica controllata, allo stato ancora lontani da una diffusione sistematica negli uffici giudiziari italiani.

Una questione specifica, oggi particolarmente rilevante per gli uffici giudiziari, è se l'anonimizzazione eseguita in locale mediante un modello linguistico di grandi dimensioni possa essere considerata una forma di anonimizzazione «via LLM» e se essa sia consentita. La risposta deve essere articolata. Sul piano tecnico, un LLM impiegato per riconoscere nomi, luoghi, dati anagrafici, riferimenti familiari, professionali o fattuali idonei alla re-identificazione opera effettivamente come motore di supporto all'anonimizzazione; sul piano giuridico, tuttavia, l'operazione resta trattamento di dati personali sino a quando il risultato non renda ragionevolmente impossibile l'identificazione dell'interessato. L'elaborazione locale riduce drasticamente il rischio di trasferimento a terzi, di riuso dei prompt, di addestramento non controllato e di accesso cloud, ma non trasforma automaticamente il trattamento in trattamento anonimo.

Ne deriva che l'uso locale di un LLM per anonimizzare provvedimenti giudiziari può ritenersi ammissibile soltanto a condizioni rigorose: il modello deve operare all'interno del perimetro infrastrutturale dell'amministrazione o comunque in un ambiente approvato dall'ufficio competente; i dati non devono essere trasmessi a fornitori esterni né utilizzati per addestrare o migliorare il modello senza una base giuridica specifica; devono essere esclusi o fortemente limitati log contenenti testo processuale; devono essere previste misure di cifratura, controllo degli accessi, versionamento del modello, tracciabilità delle operazioni e verifica umana dell'output. In questa prospettiva, il punto non è se lo strumento sia «locale» in senso fisico, ma se l'intera catena di trattamen-

to sia governata, documentata e verificabile.

La qualificazione regolatoria proposta da DigitalJustice@2030 conferma tale impostazione: la pseudonimizzazione di decisioni, documenti o dati giudiziari, quando non incide sull'attività decisoria, non è di per sé un sistema ad alto rischio ai sensi dell'AI Act, ma rimane un'attività sensibile, soggetta a trasparenza, sicurezza informatica e responsabilità organizzativa. Pertanto non può essere equiparata all'uso libero di un chatbot generalista, né può essere rimessa all'iniziativa individuale del singolo magistrato o funzionario. Occorre una soluzione istituzionale, preferibilmente validata dall'amministrazione, con parametri noti, controlli periodici e criteri uniformi di oscuramento selettivo.

Quanto al consenso delle parti, esso non costituisce normalmente il fondamento giuridico dell'anonimizzazione delle decisioni giudiziarie destinate alla pubblicazione o alla consultazione istituzionale: il trattamento si radica nella funzione pubblica della giurisdizione, negli obblighi di pubblicità e trasparenza e nelle esigenze di protezione dei dati personali. Ciò non significa, però, che l'interessato sia privo di garanzie. Restano centrali i principi di minimizzazione, proporzionalità, limitazione della finalità, sicurezza e controllo del rischio di re-identificazione. Se l'output del modello conserva elementi indirettamente identificativi – ad esempio una combinazione di luogo, professione, data, patologia, relazione familiare o circostanze del fatto – il documento non è realmente anonimizzato, ma soltanto pseudonimizzato, e deve continuare a essere trattato come dato personale.

3.4. Chiosa: pubblicità controllata e dato personale relativo

La combinazione tra il filone TAR Lazio e il filone CGUE «Deloitte» suggerisce una soluzione di equilibrio: non anonimizzazione cieca e generalizzata, ma pubblicità controllata; non presunzione assoluta di anonimato, ma verifica concreta del rischio di re-identificazione. Il primo filone ricorda che la giurisprudenza deve restare comprensibile e riutilizzabile come infrastruttura pubblica del diritto vivente; il secondo avverte che la rimozione dei nomi non basta, se il contesto o il destinatario consentono comunque l'identificazione. Il corretto governo delle banche dati giudiziarie dovrà quindi muoversi su tre piani: selezione giudiziale degli oscuramenti, valutazione tecnica del rischio residuo e tracciabilità istituzionale degli accessi e degli usi.

Da tale impostazione discende un corollario che merita di essere reso esplicito: l'anonimizzazione non può essere concepita come uno snaturamento dell'atto, imposto in via meccanica e a prescindere da ogni riflessione sulla sua concreta utilità. Per un verso, il provvedimento giudiziario si autoqualifica sovente attraverso il fatto storico che ricostruisce — la specifica vicenda, la sequenza degli eventi, le circostanze di tempo e di luogo — sì che l'identità delle persone coinvolte traspare dalla stessa struttura narrativa, indipendentemente dalla soppressione dei nomi, dei metadati e dei dati anagrafici: in simili ipotesi l'oscuramento nominativo si rivela, ad un tempo, insufficiente a proteggere la riservatezza e idoneo soltanto a impoverire l'intelligibilità del precedente. Per altro verso, vi sono fasi e materie nelle quali la conoscenza del nome risponde a un'esigenza di pubblicità intrinseca alla funzione: si pensi al procedimento di prevenzione, ove la pubblicità collegata alle diverse fasi del giudizio e la stessa conoscibilità della vicenda nella sua interezza possono richiedere che l'identità del proposto rimanga ostensibile, quale elemento costitutivo della trasparenza del controllo giurisdizionale e della comprensione dei presupposti applicativi della misura.

Ne consegue che la scelta sull'anonimizzazione — lungi dal potersi risolvere in un automatismo — postula un giudizio di proporzionalità calibrato sulla finalità perseguita, sulla fase processuale e sulla natura del procedimento: né soppressione indistinta, che tradisce la comprensibilità del precedente e ne dissolve la funzione euristica, né osten-

sione indiscriminata, che sacrifica la riservatezza oltre il necessario. È la medesima logica che, sul piano dell'impiego degli strumenti generativi, ispira la scelta consigliare di raccomandare — e non già di imporre — l'anonimizzazione preventiva degli atti (cfr. *infra*, § 2.7.3), rimettendola a una valutazione di necessità in concreto anziché a un precetto indifferenziato.

4. Copilot e strumenti IA generativi: il nodo della tutela del dato

L'adozione di strumenti di intelligenza artificiale generativa negli uffici giudiziari – in primis Microsoft Copilot, ma anche sistemi analoghi basati su modelli di linguaggio di grandi dimensioni – pone una serie di criticità specifiche che meritano un esame approfondito. Si tratta di un fenomeno già in atto, che non attende l'approvazione di linee guida o l'emanazione di circolari: i magistrati e il personale amministrativo stanno già utilizzando questi strumenti, spesso in modo informale e senza piena consapevolezza dei rischi connessi. Il sondaggio UNESCO del 2023 ha rilevato che il 44% dei professionisti legali integra già l'IA nel proprio lavoro, ma solo il 9% ha ricevuto formazione istituzionale: dati che rendono urgente la definizione di regole operative chiare (UNESCO, 2026, p. 5).

4.1. Il problema dell'accesso ai dati

Il Data Risk Report 2025, pubblicato dalla società di sicurezza informatica Varonis, ha rilevato che il 57% dei dati aziendali accessibili attraverso Microsoft Copilot sono informazioni riservate o sensibili (Varonis, 2025, p. 23)⁹. Nel contesto degli uffici giudiziari, questa percentuale è destinata ad essere ancora più elevata: i sistemi documentali dei tribunali contengono informazioni di straordinaria delicatezza – atti processuali, bozze di sentenze, comunicazioni tra colleghi, note riservate sui fascicoli – che per loro natura non dovrebbero essere oggetto di elaborazione da parte di sistemi IA collegati a infrastrutture cloud esterne al perimetro istituzionale.

Il rischio specifico di Copilot è quello che i tecnici definiscono «*oversharing*»: lo strumento, per rispondere ai prompt dell'utente, accede a tutti i documenti cui l'utente è autorizzato e li utilizza come contesto, senza che l'utente sia sempre consapevole di questa operazione. Le Linee guida UNESCO affrontano direttamente questa criticità nella raccomandazione 2.3.3 («*Usage restrictions*»), specificando che le organizzazioni giudiziarie devono vietare o limitare l'uso di strumenti generativi i cui termini di servizio prevedano l'utilizzo dei prompt degli utenti per addestrare i propri modelli o consentano a terzi l'accesso a tali prompt – ipotesi che ricorrono frequentemente nelle versioni gratuite o semi-professionali degli strumenti più diffusi.

4.2. Il perimetro UE e le eccezioni

Microsoft ha istituito per i propri clienti europei una c.d. *EU Data Boundary*, una garanzia contrattuale secondo la quale i dati degli utenti europei vengono elaborati esclusivamente all'interno del territorio dell'Unione Europea (Microsoft, 2025)¹⁰. Questa garanzia è tuttavia soggetta a importanti eccezioni che ne limitano significativamente la portata pratica. In primo luogo, le query effettuate attraverso il motore di ricerca Bing – che Copilot utilizza per la ricerca in tempo reale su internet – transitano per server ubicati negli Stati Uniti. In secondo luogo, Microsoft si avvale di *subprocessor* che possono operare al di fuori dell'UE, inclusi fornitori di componenti o servizi tecnici del modello sottostante. In terzo luogo, le istanze relative alla sicurezza e alla prevenzione degli abusi vengono gestite da team operanti globalmente.

Queste eccezioni non sono prive di rilevanza giuridica. Il trasferimento di dati personali

verso paesi terzi richiede, ai sensi degli artt. 44-49 GDPR, l'adozione di misure supplementari specifiche. Nel contesto della giustizia, la questione si fa ancora più delicata perché i dati processuali possono essere soggetti a obblighi di riservatezza previsti anche da disposizioni procedurali (segreto istruttorio, divieto di pubblicazione degli atti coperti da segreto). Le Linee guida UNESCO affrontano questo aspetto nella raccomandazione 2.1.15 («*Security and cybersecurity-enhancing measures*»), stabilendo che, quando il sistema IA implica l'accesso a servizi cloud, l'organizzazione deve assicurarsi che il livello di protezione offerto dal fornitore corrisponda agli standard legali locali e agli standard di sicurezza organizzativi.

4.3. Machine unlearning e diritto all'oblio

L'art. 17 della L. 132/2025 introduce nell'ordinamento italiano una disciplina del «*machine unlearning*» che, pur non essendo priva di profili di incertezza applicativa, rappresenta un importante passo in avanti nel riconoscimento del diritto all'oblio in relazione ai dati di addestramento dei modelli IA (Thaler – Domingo-Ferrer, 2024, p. 54789)¹³. La norma prevede che il soggetto i cui dati personali siano stati utilizzati per addestrare un sistema IA possa richiedere la loro rimozione dal modello, con la conseguente necessità per il titolare del trattamento di procedere al re-addestramento del sistema in modo da eliminare l'influenza di quei dati sul comportamento del modello.

L'applicazione di questo istituto al contesto giudiziario è tutt'altro che semplice. Le sentenze sono pubblici ed ufficiali documenti, destinati strutturalmente alla pubblicità: il fatto che esse contengano dati personali non le trasforma in dati il cui trattamento richiede il consenso dell'interessato. La questione che si pone è dunque se l'utilizzo del testo di una sentenza come dato di addestramento per un modello IA costituisca un trattamento autonomo – distinto dalla mera pubblicazione della sentenza stessa – soggetto ai principi generali del GDPR e, quindi, potenzialmente suscettibile di opposizione da parte delle persone coinvolte.

Il tema del machine unlearning conserva rilievo¹³, ma deve essere distinto dall'uso di Copilot nel tenant descritto dalla delibera. Se i prompt e i dati giudiziari non sono utilizzati per addestrare o migliorare il modello, il problema immediato è soprattutto quello della conservazione e della cancellazione delle interazioni e dei log, e non della rimozione del dato dai pesi del modello.

La questione tornerà centrale per le future suite dedicate, qualora esse siano addestrate o adattate su corpora giurisprudenziali o su documenti giudiziari. In tale scenario occorrerà distinguere tra base giuridica della pubblicazione della decisione, ulteriore trattamento per addestramento, diritto alla cancellazione, obblighi di conservazione e fattibilità tecnica della rimozione dell'influenza del dato. Il principio di limitazione della finalità impone, in ogni caso, che la disponibilità pubblica di una sentenza non sia automaticamente equiparata alla libertà di utilizzarla per qualsiasi forma di addestramento.

4.4. Prompt injection e rischi per l'integrità processuale

Un rischio ulteriore, di natura più strettamente informatica ma con dirette implicazioni giuridiche, è quello della *prompt injection*: istruzioni occulte inserite in un documento depositato possono tentare di alterare il comportamento del sistema che lo elabora. Nel processo, la possibilità che una parte introduca contenuti destinati non al giudice, ma al modello, trasforma la sicurezza informatica in garanzia dell'integrità del contraddittorio: un atto potrebbe essere confezionato per orientare surrettiziamente l'analisi automatizzata svolta dall'ufficio.

Il rischio esige una separazione rigorosa tra il testo del documento e le istruzioni di sistema, la neutralizzazione dei contenuti attivi, l'analisi preventiva degli allegati, test

avversariali e la registrazione degli eventi anomali. I documenti delle parti devono essere trattati come dati non affidabili rispetto alle istruzioni: possono fornire contenuti da analizzare, ma non modificare le regole del *workflow*. Le indicazioni UNESCO sulla resilienza dei sistemi lungo l'intero ciclo di vita (punto 2.1.15) e le Guidelines CEPEJ sulla sperimentazione controllata trovano, in questa sede, una traduzione immediatamente operativa.

5. La proprietà intellettuale del dato giurisprudenziale

Il tema della proprietà intellettuale applicata alle banche dati giurisprudenziali è probabilmente il più affascinante e il più controverso dell'intera materia, perché mette a nudo un paradosso strutturale del nostro ordinamento: i dati giurisprudenziali sono pubblici per definizione, in quanto prodotti dall'esercizio di una funzione statale finanziata dalla collettività, ma le banche dati che li raccolgono, li organizzano e li rendono consultabili sono spesso di proprietà privata e oggetto di tutela sulla base del diritto sui generis.

5.1. Le sentenze come opere dell'ingegno

La prima questione che si pone è se le singole sentenze – intese come testi redatti da magistrati nell'esercizio delle loro funzioni – possano essere considerate «opere dell'ingegno» ai sensi dell'art. 1 della legge sul diritto d'autore (L. 633/1941) e godere della relativa protezione. La risposta è tendenzialmente negativa, per una ragione di principio che affonda le radici nella teoria del «lavoro per conto» applicata alla funzione pubblica: il magistrato che redige una sentenza non lo fa in qualità di autore creativo che esprime la propria personalità artistica, ma come funzionario dello Stato che esercita una competenza istituzionale.

La questione diventa più complessa quando si considerano elementi quali le massime giurisprudenziali: brevi sintesi del principio di diritto enunciato da una sentenza, la cui redazione richiede un'elaborazione intellettuale significativa. Le massime sono prodotte, nella tradizione italiana, dalla Corte di Cassazione attraverso l'Ufficio del Massimario, e da alcuni tribunali di merito: si tratta di testi che, pur derivando da un atto autoritativo, presentano caratteri di originalità sufficienti a porsi il problema della loro tutela autorale (Bertani, 2023, p. 145)¹². Le stesse Linee guida UNESCO segnalano peraltro che le organizzazioni giudiziarie devono prestare «*special consideration to intellectual property rights compliance*» anche in relazione ai contenuti prodotti dai sistemi IA generativi, assicurando che tali contenuti rispettino la proprietà intellettuale dei testi originali (punto 2.3.3).

Il riferimento decisivo, nel diritto italiano, è anche l'art. 5 della legge n. 633/1941, secondo cui le disposizioni sul diritto d'autore non si applicano ai testi degli atti ufficiali dello Stato e delle amministrazioni pubbliche, italiane o straniere. La sentenza, in quanto atto ufficiale della giurisdizione, deve dunque essere distinta dalle opere dell'ingegno in senso proprio: essa può essere scritta con stile elevato, rigore argomentativo e originalità espositiva, ma non è appropriabile come opera privata, perché appartiene alla funzione pubblica che la genera. Questa esclusione, tuttavia, riguarda il testo ufficiale del provvedimento, non necessariamente gli apparati redazionali, le note, le massime, gli abstract, le classificazioni tematiche e le elaborazioni editoriali che si innestano su di esso.

5.2. Il diritto sui generis del costituente della banca dati

Il terreno più fertile per la tutela delle banche dati giurisprudenziali è quello del diritto sui generis del costituente introdotto dalla Direttiva 96/9/CE e recepito nell'ordinamen-

to italiano dagli artt. 102-bis e 102-ter della legge sul diritto d'autore. Questo istituto – che non richiede l'originalità creativa ma solo un investimento sostanziale nella raccolta, nella verifica o nella presentazione del contenuto – protegge il costituente della banca dati contro le estrazioni sistematiche e il riutilizzo di parti sostanziali del contenuto.

Le grandi banche dati giurisprudenziali private (DeJure, Il Foro Italiano, Leggi d'Italia, Ius Explorer) sono costruite su investimenti enormi in termini di raccolta, selezione, massimazione e indicizzazione delle sentenze: investimenti che giustificano pienamente la tutela sui generis. Il paradosso emerge però chiaramente: l'oggetto di questo investimento – le sentenze – è un bene pubblico prodotto con denaro pubblico. La privatizzazione dell'accesso a questo bene attraverso lo strumento del diritto sui generis solleva interrogativi di legittimità costituzionale che non sono mai stati affrontati in modo risolutivo dalla giurisprudenza italiana.

Occorre quindi distinguere tre piani. Il primo è il piano del documento giudiziario in sé, che tende a sottrarsi alla logica proprietaria del diritto d'autore. Il secondo è il piano della banca dati, che può essere protetta non perché «possieda» le sentenze, ma perché incorpora un investimento sostanziale nella raccolta, verifica, normalizzazione, classificazione e presentazione dei materiali. Il terzo è il piano degli arricchimenti informativi: massime, titoletti, parole chiave, collegamenti ipertestuali, note di commento, classificazioni redazionali e grafi di citazioni possono, a seconda dei casi, presentare una tutela autonoma. Questa tripartizione è essenziale anche per l'addestramento dei sistemi IA: usare il testo pubblico di una decisione non equivale a estrarre sistematicamente il contenuto qualificato di una banca dati protetta, né a riutilizzare gli apparati editoriali che ne costituiscono il valore aggiunto.

5.3. Text and data mining dopo la L. 132/2025

La L. 132/2025, modificando gli artt. 70-ter e 70-quater della legge sul diritto d'autore, ha ridisegnato il quadro delle eccezioni al diritto d'autore e al diritto sui generis applicabili al text and data mining. La nuova disciplina distingue tra TDM per ricerca scientifica (eccezione obbligatoria, non derogabile contrattualmente) e TDM per altri scopi (eccezione facoltativa, soggetta all'opt-out del titolare dei diritti). Il meccanismo dell'opt-out consente alle banche dati giurisprudenziali private di escludere i propri contenuti dall'utilizzo per l'addestramento di sistemi IA, attraverso appositi metadati tecnici (come il file robots.txt o il tag «ai-notraining»).

Le implicazioni di questo regime per l'ecosistema delle banche dati giurisprudenziali sono profonde. Se le principali banche dati private esercitassero il proprio diritto di opt-out, i sistemi IA destinati al settore legale potrebbero essere addestrati soltanto su dati pubblici – le sentenze pubblicate sui siti istituzionali dei tribunali e della Cassazione – che presentano qualità e completezza assai inferiori rispetto ai dataset curati dai soggetti privati. Il risultato sarebbe un'IA giuridica di qualità strutturalmente inferiore, con evidenti ricadute sulla qualità dell'assistenza legale e, in ultima analisi, sull'accesso alla giustizia. Si tratta di un effetto perverso che il legislatore del 2025 non sembra aver adeguatamente valutato.

In questa materia il text and data mining non può essere affrontato come una questione meramente proprietaria. Le sentenze sono il materiale primario per la conoscibilità del diritto vivente e per la costruzione di strumenti di supporto all'accesso alla giustizia; tuttavia l'estrazione massiva da banche dati private può incidere sul diritto sui generis del costituente e sugli eventuali diritti relativi agli apparati redazionali. La soluzione di equilibrio dovrebbe muovere da un principio semplice: piena apertura, in formato machine-readable, dei testi ufficiali delle decisioni pubbliche, previa anonimizzazione proporzionata; rispetto delle riserve tecniche e contrattuali quando l'estrazione riguar-

di contenuti editoriali ulteriori o raccolte curate da soggetti privati; promozione di dataset istituzionali di qualità, in modo da evitare che l'innovazione giuridica dipenda esclusivamente da archivi proprietari.

6. Verso un modello integrato di governo del dato giudiziario

I temi affrontati nelle sezioni precedenti convergono verso un'esigenza di fondo: la costruzione di un modello integrato di governo del dato giudiziario che sappia coniugare le esigenze di trasparenza, di protezione dei dati, di innovazione tecnologica e di tutela dei diritti di proprietà intellettuale in un quadro coerente e operativamente praticabile. I singoli strumenti normativi esistenti sono necessari ma non sufficienti: senza coordinamento, essi rischiano di moltiplicare i vincoli senza produrre un sistema coerente di incentivi per l'innovazione responsabile.

6.1. Il modello delle linee guida distrettuali

Un'esperienza di rilievo è quella delle linee guida distrettuali sull'utilizzo dell'IA, adottate da alcuni Consigli Giudiziari nell'arco del 2024-2025. Questi documenti – emanati nel solco delle Raccomandazioni CSM e, successivamente, delle Linee guida UNESCO – offrono un modello di regolazione «dal basso» particolarmente prezioso perché calato nella realtà operativa degli uffici giudiziari locali. Il documento UNESCO del 2025 propone esplicitamente (conclusioni, p. 32) che le sue linee guida possano essere utilizzate *«as a template for developing context-specific national and subnational guidelines»*: un approccio che legittima e valorizza il pluralismo delle esperienze distrettuali, purché esse si sviluppino entro un quadro di principi nazionali vincolanti.

Il rischio principale di questo modello è la frammentazione: la coesistenza di discipline distrettuali significativamente diverse potrebbe creare zone d'ombra e disparità di trattamento che finiscono per ledere il principio di uguaglianza. È dunque necessario che le linee guida locali si sviluppino entro un quadro di principi nazionali vincolanti, definiti dal CSM in coordinamento con il Garante per la protezione dei dati personali e l'Agenzia per la cybersicurezza nazionale.

6.2. La massimazione assistita da IA

Un dominio in cui l'IA può offrire vantaggi concreti e misurabili è quello della massimazione delle sentenze: l'attività di estrazione e sintesi del principio di diritto enunciato da un provvedimento, tradizionalmente svolta dall'Ufficio del Massimario della Cassazione e dagli uffici analoghi dei tribunali di merito. I modelli LLM mostrano capacità promettenti in questo ambito. L'integrazione umano-macchina in questo campo – con il magistrato che verifica, corregge e valida la bozza prodotta dall'algoritmo – sembra uno dei percorsi più promettenti, coerente con la lista degli usi raccomandabili dei sistemi generativi indicata dalle Linee guida UNESCO (punto 3.3.2, che include la generazione di riassunti, con la raccomandazione di verificarne sempre l'accuratezza).

È tuttavia essenziale che la massimazione assistita da IA sia accompagnata da garanzie metodologiche rigorose: validazione empirica della qualità degli output, audit periodici sull'assenza di distorsioni sistematiche, tracciabilità della catena umano-macchina nella produzione di ogni massima. L'esperienza della Cour de Cassation francese, che ha avviato un progetto pilota in questa direzione, offre spunti preziosi per la progettazione di sistemi analoghi in Italia.

Un esempio particolarmente significativo è offerto da OLGA, l'assistente IA sviluppato in Germania per supportare i giudici nella gestione dei procedimenti seriali nati dal contenzioso Dieselgate. Secondo DigitalJustice@2030, OLGA analizza le sentenze di primo grado, estrae parametri ricorrenti – quali tipo di veicolo, motore, standard emissivo e ragioni del richiamo – raggruppa automaticamente casi simili e compila modelli individuali predisposti dai giudici. Il valore dello strumento non consiste nel decidere la controversia, ma nel ridurre attività ripetitive, migliorare la programmazione delle udienze e consentire al giudice di concentrare il proprio lavoro sul controllo dei fatti e sulla decisione. Proprio per questo OLGA rappresenta un paradigma utile: IA come infrastruttura organizzativa, non come sostituto del giudizio.

L'esperienza OLGA mostra anche il criterio che dovrebbe guidare la progettazione degli strumenti: partire da compiti ad alta ripetitività e basso contenuto discrezionale, costruire template di controllo giudiziario, mantenere verificabilità e modificabilità dell'output, impedire che l'automazione trasformi in opacità decisionale. In tal modo l'IA può contribuire a ridurre l'arretrato e a razionalizzare i flussi senza intaccare il principio secondo cui la decisione resta personale, responsabile e motivata dal magistrato.

6.3. La sfida dell'interoperabilità

La dimensione europea della questione impone di affrontare il tema dell'interoperabilità tra le banche dati giurisprudenziali nazionali ed europee. Il progetto e-Justice Portal della Commissione europea e la base dati EUR-Lex coprono ormai gran parte della giurisprudenza delle corti di giustizia dell'Unione, ma restano largamente insufficienti per quanto riguarda la giurisprudenza dei tribunali nazionali. La costruzione di un'infrastruttura condivisa di banche dati giurisprudenziali europee, fondata su standard comuni di metadatazione, anonimizzazione e accessibilità, è una necessità non più rinviabile se si vuole che i sistemi IA applicati alla giustizia europea operino su basi informative solide e rappresentative della pluralità degli ordinamenti nazionali.

DigitalJustice@2030 colloca questo tema in una cornice più ampia, fondata su tre strumenti complementari: una mappatura permanente delle soluzioni digitali e IA utilizzate nei sistemi giudiziari nazionali, un «living repository» sul portale e-Justice e una Justice AI toolbox ospitata sull'Interoperable EU e-Justice Portal. L'obiettivo non è imporre un modello unico europeo, ma evitare che ventisette ordinamenti sviluppino separatamente strumenti analoghi, con costi duplicati, standard incompatibili e qualità disomogenee. Per le banche dati giurisprudenziali ciò significa che anonimizzazione, metadatazione, ECL, accessibilità e riusabilità non sono dettagli tecnici, ma condizioni strutturali per un ecosistema affidabile di IA giuridica.

Nella stessa prospettiva si colloca lo European Legal Data Space, che mira a rendere legislazione e giurisprudenza europee e nazionali più accessibili, riutilizzabili, ricercabili e, ove possibile, disponibili come dati di qualità per lo sviluppo di applicazioni legal tech e strumenti IA. Questo passaggio è cruciale: un modello addestrato su dati giudiziari incompleti, male anonimizzati o disomogenei non produce quanto atteso: risultati meno accurati; rischia di riprodurre asimmetrie informative tra uffici, territori e operatori professionali. L'interoperabilità, dunque, non è un lusso tecnologico, ma una garanzia di uguaglianza nell'accesso al diritto.

6.4. Il magistrato come «garante umano»

Il filo rosso che percorre l'intera riflessione è il ruolo del magistrato come «garante umano» della qualità del dato giudiziario e dell'integrità del processo decisionale. Le Linee guida UNESCO, l'AI Act, le Raccomandazioni CSM: tutti questi strumenti convergono nell'affermare che l'IA, per quanto sofisticata, non può sostituire il giudizio umano nell'esercizio della funzione giurisdizionale. Il principio 13 delle Linee guida UNESCO è nettissimo su questo punto: *«Judges and magistrates should not delegate any part of their mandate or rely exclusively on AI systems to adopt decisions or automate entire processes that may negatively impact the rights of individuals or communities. They should preserve the possibility of human intervention in decision-making processes where AI systems are deployed. AI tools must not replace the decision-maker's independent analysis of facts, law, and evidence»*¹¹.

Il documento *AI Essentials for Judges del 2026* ribadisce questa posizione in termini ancora più espliciti: *«AI cannot – and should not – replace judges. While AI can efficiently process and organize information, it is fundamentally a probabilistic tool that relies on instructions and existing data, which may contain biases or errors. AI lacks the capacity for nuanced legal reasoning and judgment required to weigh facts, interpret the law, and deliver a reasoned decision»* (UNESCO, 2026, p. 15). Il magistrato del futuro non sarà dunque il magistrato che ignora l'IA, né il magistrato che si affida ciecamente ad essa: sarà il magistrato che sa usare gli strumenti algoritmici con consapevolezza critica, che conosce i loro limiti e le loro potenzialità, che mantiene il controllo del processo decisionale pur beneficiando dell'efficienza che la tecnologia può offrire.

7. Conclusioni

Il percorso argomentativo sviluppato in questo contributo ha cercato di mostrare come la questione dell'intelligenza artificiale applicata alla giurisprudenza non sia riducibile a un problema tecnico o a un insieme di questioni giuridiche settoriali, ma costituisca una questione istituzionale di prima grandezza, capace di influire sulla qualità della giustizia, sull'eguaglianza dei cittadini davanti alla legge e sulla stessa credibilità dell'istituzione giudiziaria.

Tre conclusioni di ordine generale si impongono al termine della riflessione. La prima è che il quadro normativo disponibile – per quanto frammentato e non sempre coerente – è già sufficientemente ricco da consentire soluzioni ragionate ai problemi più urgenti: non servono nuove leggi, serve applicazione consapevole di quelle esistenti, nell'interpretazione sistematica che emerge dal raccordo tra Linee guida UNESCO, AI Act, L. 132/2025 e Raccomandazioni CSM. La seconda è che il governo del dato giudiziario richiede una cooperazione strutturata tra attori istituzionali diversi – magistratura, Garante privacy, AGID, Agenzia per la cybersicurezza nazionale, Ministero della Giustizia – che oggi faticano a dialogare in modo sistematico; la creazione di un tavolo tecnico permanente su IA e giustizia, con partecipazione paritaria di tutti questi soggetti, sembra una misura non più rinviabile. La terza è che la formazione dei magistrati in materia digitale non può più essere considerata un lusso o un'iniziativa volontaristica: essa è una necessità funzionale all'esercizio della giurisdizione nel XXI secolo, da garantire attraverso programmi strutturali in linea con quanto raccomandato dall'UNESCO e dall'EJTN.

L'intelligenza artificiale è già nella stanza dei tribunali. La questione non è se accoglierla o respingerla: è come governarla con saggezza, nel rispetto dei valori fondamentali dello Stato di diritto.

A queste conclusioni se ne aggiunge una quarta, suggerita dalla strategia DigitalJustice@2030: la qualità dell'IA giudiziaria dipenderà dalla qualità dell'infrastruttura pubblica del dato. Senza dataset istituzionali affidabili, anonimizzati in modo proporzionato, interoperabili e liberamente riutilizzabili nei limiti di legge, gli uffici giudiziari resteranno dipendenti da soluzioni proprietarie, disomogenee e difficilmente auditabili. La vera alternativa non è dunque tra innovazione e prudenza, ma tra innovazione governata e innovazione casuale. La prima rafforza la giurisdizione; la seconda la espone a rischi di opacità, diseguaglianza e perdita di controllo sul patrimonio informativo giudiziario.

1. Sul tema della digitalizzazione della giurisprudenza v. G. Finocchiaro, *Il precedente giudiziario nell'era digitale*, in Riv. trim. dir. proc. civ., 2024, p. 315 ss.
2. UNESCO, *Guidelines for the Use of AI Systems in Courts and Tribunals*, Parigi, 2025, ISBN 978-92-3-100830-6, DOI: <https://doi.org/10.58338/LIEY8089>. Il documento è stato preparato da Juan David Gutiérrez, PhD, Associate Professor, University of Los Andes, Colombia, ed è disponibile in accesso aperto con licenza CC-BY-SA 3.0 IGO.
3. UNESCO, *AI Essentials for Judges*, Parigi, 2026, CI/DIT/AI/Judges2026, disponibile in accesso aperto con licenza CC-BY-SA 3.0 IGO. Il documento è stato preparato da Kamel El Hilali, AI & Rule of Law Specialist, Digital Policies and Digital Transformation, UNESCO.
4. UNESCO, *Global Judges' Initiative: Survey on the Use of AI Systems by Judicial Operators*, 2024. Il sondaggio è stato condotto nel 2023 su operatori giudiziari di 96 Paesi.
5. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in GUUE L 2024/1689, 12 luglio 2024.
6. CSM, *Delibera 8 ottobre 2025, Raccomandazioni sull'utilizzo dell'intelligenza artificiale da parte dei magistrati*, disponibile su <http://www.csm.it>.
7. TAR Lazio, Roma, Sez. I, 17 aprile 2025, n. 7625, sulla Banca Dati Pubblica delle decisioni di merito e sull'illegittimità dell'oscuramento generalizzato dei dati personali nelle sentenze pubblicate.
8. CGUE, Prima Sezione, 4 settembre 2025, C-413/23 P, *European Data Protection Supervisor c. Single Resolution Board*, ECLI:EU:C:2025:645, cd. sentenza «Deloitte»; in primo grado, Trib. UE, 26 aprile 2023, T-557/20, *Single Resolution Board c. EDPS*.
9. Varonis Systems, *Data Risk Report 2025. The State of Enterprise AI Data Security*, New York, 2025, p. 23.
10. Microsoft Corporation, *EU Data Boundary for the Microsoft Cloud – Technical White Paper*, versione 5.0, gennaio 2025, disponibile su <https://www.microsoft.com/en-us/trust-center>.
11. Sulla Corte Costituzionale della Colombia, Sentencia T-323/2024 (agosto 2024), che ha dichiarato legittimo l'uso dell'IA da parte della magistratura a condizione che non sostituisca il giudizio umano, con rinvio espresso alle Linee guida UNESCO, v. J.D. Gutiérrez, «un commento sull'uso di strumenti di IA generativa da parte di giudici e magistrati in Perù e Messico», Tech Policy Press, 19 aprile 2023.
12. M. Bertani, *Banche dati e diritto di accesso alla giurisprudenza*, in AIDA, 2023, p. 145 ss.
13. T. Thaler – J. Domingo-Ferrer, *Machine Unlearning: A Comprehensive Survey*, in IEEE Access, vol. 12, 2024, p. 54789 ss.
14. F. Sartor – C. Lagioia, *L'AI Act e la giustizia: luci e ombre del nuovo quadro regolatorio europeo*, in Dir. informaz. informatica, 2024, p. 891 ss.
15. L. 9 agosto 2025, n. 132, *Disposizioni in materia di intelligenza artificiale*, in G.U. n. 187 del 12 agosto 2025.
16. Sul fenomeno della memorizzazione involontaria nei grandi modelli linguistici v. N. Carlini – F. Tramèr – E. Wallace – M. Jagielski – A. Herbert-Voss – K. Lee – A. Roberts – T. Brown – D. Song – Ú. Erlingsson – A. Oprea, «Extracting Training Data from Large Language Models», in *Proceedings of the 30th USENIX Security Symposium*, 2021, pp. 2633-2650. Sul tema della narrative re-identification v. anche P. Ohm, «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», in *UCLA Law Review*, 57, 2010, pp. 1701-1777; L. Sweeney, «k-anonymity: A Model for Protecting Privacy», in *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), 2002, pp. 557-570.
17. CEDU, Pretto e altri c. Italia, 8 dicembre 1983; Axen c. Germania, 8 dicembre 1983; Sutter c. Svizzera, 22 febbraio 1984; Tierce e altri c. San Marino, 25 luglio 2000: la pubblicità della pronuncia ex art. 6 CEDU può essere soddisfatta anche mediante forme di accessibilità pubblica diverse dalla lettura integrale, purché il pubblico possa conoscere il contenuto della decisione e controllare l'esercizio della giurisdizione.
18. CEDU, B. e P. c. Regno Unito, 24 aprile 2001, sulla compatibilità tra limitazioni della pubblicità in procedimenti familiari e garanzia di controllo pubblico; Z c. Finlandia, 25 febbraio 1997, sulla particolare protezione dei dati sanitari e dell'identità dell'interessato nella motivazione giudiziaria; M.L. e W.W. c. Germania, 28 giugno 2018, sul bilanciamento tra art. 8 e art. 10 CEDU rispetto alla conservazione online di notizie giudiziarie e alla richiesta di anonimizzazione.

19. CEPEJ – Commissione europea per l'efficienza della giustizia, *Guidelines on the use of generative artificial intelligence (AI) for courts and tribunals*, Consiglio d'Europa, dicembre 2025. Cfr. altresì CEPEJ, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente*, 2018.
20. CSM, *Aggiornamento delle raccomandazioni sull'uso dell'intelligenza artificiale nell'amministrazione della giustizia, adottate con delibera dell'8 ottobre 2025*, delibera 22 luglio 2026 (pratica n. 118/VV/2024, rel. Cons. Eccher e Forziati, rel. esterno Cons. Bisogni).
21. Sul requisito della verificabilità documentale quale prima misura di legittimità dell'ausilio algoritmico e sulla nozione di grounding, v. M. Sciacca, *Giustizia e High-risk AI Systems*, Milano, Giuffrè Francis Lefebvre, 2026.
22. Sulla distinzione tra checkpoint come presidio sostanziale e come mero adempimento, e sulle nozioni di scivolamento funzionale e integrità cognitiva del magistrato, v. M. Sciacca, *Integrare senza sostituire. L'aggiornamento 2026 delle raccomandazioni del CSM sull'intelligenza artificiale nella giustizia, tra continuità regolatoria e tutela dell'integrità cognitiva del magistrato*, in *Diritto giustizia e costituzione*, 23 luglio 2026; per la prospettiva della governance del rischio, C. Parodi, *Le nuove Raccomandazioni del CSM sull'intelligenza artificiale nella giustizia. Dalla cautela difensiva alla governance del rischio*, in *Sistema Penale*, 24 luglio 2026.
23. Reg. (UE) 2026/1744, che ha differito al 2 dicembre 2027 l'applicazione degli obblighi per i sistemi ad alto rischio autonomi dell'Allegato III dell'AI Act, recependo l'accordo provvisorio sul c.d. Digital Omnibus on AI del 7 maggio 2026.
24. Cass. pen., Sez. III, 11 giugno 2026 (dep. 22 giugno 2026), n. 23006, in tema di citazione, nel ricorso per cassazione, di precedenti giurisprudenziali inesistenti o "allucinati" da sistemi di intelligenza artificiale e di colpa qualificata ai sensi dell'art. 616 c.p.p.

Riferimenti bibliografici

- Carlini, N. – Tramèr, F. – Wallace, E. – Jagielski, M. – Herbert-Voss, A. – Lee, K. – Roberts, A. – Brown, T. – Song, D. – Erlingsson, Ú. – Oprea, A. (2021), "Extracting Training Data from Large Language Models", in *Proceedings of the 30th USENIX Security Symposium*, pp. 2633-2650.
- Ohm, P. (2010), "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", in *UCLA Law Review*, 57, pp. 1701-1777.
- Sweeney, L. (2002), "k-anonymity: A Model for Protecting Privacy", in *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), pp. 557-570.
- Bertani, M. (2023), «Banche dati e diritto di accesso alla giurisprudenza», in *AIDA – Annali italiani del diritto d'autore, della cultura e dello spettacolo*, XXXII, pp. 145-189.
- CEPEJ – Commissione europea per l'efficienza della giustizia (2025), *Guidelines on the use of generative AI for courts and tribunals*, Strasburgo, Consiglio d'Europa.
- CSM – Consiglio Superiore della Magistratura (2025), *Raccomandazioni sull'utilizzo dell'intelligenza artificiale da parte dei magistrati*, delibera 8 ottobre 2025, Roma, CSM.
- CSM – Consiglio Superiore della Magistratura (2026), *Aggiornamento delle raccomandazioni sull'uso dell'intelligenza artificiale nell'amministrazione della giustizia*, delibera 22 luglio 2026 (pratica n. 118/VV/2024), Roma, CSM.
- Finocchiaro, G. (2024), «Il precedente giudiziario nell'era digitale», in *Rivista trimestrale di diritto e procedura civile*, LXXVIII (2), pp. 315-342.
- Gutiérrez, J.D. (2024), «Critical Appraisal of Large Language Models in Judicial Decision-Making», in *Handbook on Public Policy and Artificial Intelligence*, Edward Elgar Publishing, pp. 323-338, doi:10.4337/9781803922171.00033.
- Microsoft Corporation (2025), *EU Data Boundary for the Microsoft Cloud – Technical White Paper*, v. 5.0, Redmond, Microsoft.

- Parodi, C. (2026), «Le nuove Raccomandazioni del CSM sull'intelligenza artificiale nella giustizia. Dalla cautela difensiva alla governance del rischio», in *Sistema Penale*, 24 luglio 2026.
- Sartor, G. – Lagioia, F. (2024), «L'AI Act e la giustizia: luci e ombre del nuovo quadro regolatorio europeo», in *Diritto dell'informazione e dell'informatica*, XL (4), pp. 891-935.
- Sciacca, M. (2026a), *Giustizia e High-risk AI Systems*, Milano, Giuffrè Francis Lefebvre.
- Sciacca, M. (2026b), «Integrare senza sostituire. L'aggiornamento 2026 delle raccomandazioni del CSM sull'intelligenza artificiale nella giustizia, tra continuità regolatoria e tutela dell'integrità cognitiva del magistrato», in *Diritto giustizia e costituzione*, 23 luglio 2026.
- Thaler, T. – Domingo-Ferrer, J. (2024), «Machine Unlearning: A Comprehensive Survey», in *IEEE Access*, XII, pp. 54789-54821.
- UNESCO (2025), *Guidelines for the Use of AI Systems in Courts and Tribunals*, Parigi, ISBN 978-92-3-100830-6, DOI: <https://doi.org/10.58338/LIEY8089>.
- UNESCO (2026), *AI Essentials for Judges*, Parigi, CI/DIT/AI/Judges2026.
- Varonis Systems (2025), *Data Risk Report 2025. The State of Enterprise AI Data Security*, New York, Varonis.