

Riservatezza e intelligenza artificiale giuridica

Anonimizzazione e pseudonimizzazione delle pratiche
Quadro di riferimento per la professione legale

Analisi dei testi francesi e californiani
Principi di progettazione e metodo di valutazione

Come ridurre l'esposizione delle informazioni affidate a un sistema di IA preservando ciò che è necessario
per il ragionamento giuridico e la restituzione del risultato?

Sintesi e metodo

Sintesi

La riservatezza di una pratica legale dipende dalle informazioni che circolano, dai loro destinatari e dagli usi che ne vengono fatti. Sostituire i nomi è una misura utile, ma il suo valore va valutato insieme al contenuto restante e al lavoro richiesto. Una trasformazione che protegge un'identità alterando al contempo una qualità, una data o un obbligo può rendere il risultato giuridicamente inadeguato.

Questo libro bianco propone un quadro per esaminare congiuntamente la protezione delle informazioni, la fedeltà del contesto e la restituzione dei risultati. Si basa sulle norme francesi sul segreto professionale, sulle raccomandazioni del Conseil national des barreaux (CNB), sul RGPD, sulla legge californiana SB 574 e su riferimenti istituzionali in materia di de-identificazione. [1–10]

La conclusione centrale è che l'unità di valutazione pertinente è il percorso di trattamento. La protezione va esaminata alla ricezione, durante la preparazione dei documenti e i trattamenti successivi, e infine al momento della restituzione. Una verifica isolata su un testo non descrive, da sola, le proprietà dell'intero insieme.

Metodo e natura delle proposte

L'approccio confronta un corpus mirato di testi normativi, raccomandazioni professionali e studi istituzionali, selezionati per il loro legame diretto con la riservatezza delle pratiche. È integrato da un modello decisionale e da un protocollo di valutazione; non costituisce una revisione sistematica della letteratura. L'analisi distingue i requisiti dei testi, la loro interpretazione per gli usi dell'IA e le proposte metodologiche di questa pubblicazione. I riferimenti numerati consentono di risalire alle fonti; le proposte di metodo sono quelle di questa pubblicazione.

Gli esempi sono fittizi. Le griglie e gli indicatori sono strumenti di lavoro da adattare; non sono presentati come norme adottate dalle istituzioni citate. Lo studio riguarda principalmente le pratiche degli avvocati. Altri professionisti possono riprendere il metodo tenendo conto dei segreti e degli obblighi propri del loro status.

Contributi proposti

Una distinzione tra protezione delle identità, riservatezza del contenuto e fedeltà giuridica.

Un esame del percorso completo, dalla richiesta agli elaborati finali.

Un metodo per scegliere la protezione ed esaminarne i risultati rispetto a un uso definito.

I fondamenti francesi della protezione

Il segreto professionale copre il fascicolo

L'articolo 66-5 della legge del 31 dicembre 1971 protegge, in particolare, le consulenze, la corrispondenza e i documenti del fascicolo. L'articolo 2 del Regolamento interno nazionale della professione forense francese (RIN) ne precisa l'estensione. Il segreto riguarda quindi informazioni che non si limitano ai dati identificativi di una persona fisica. [4][5]

Questa distinzione è determinante per l'IA. Una strategia processuale, un progetto di transazione o un know-how possono restare riservati dopo la rimozione dei nomi. Occorre esaminare il contenuto effettivamente comunicato e le condizioni del suo trattamento.

La raccomandazione del CNB

La guida *La déontologie et l'intelligence artificielle*, prima edizione dell'aprile 2026, raccomanda una pseudonimizzazione o anonimizzazione preventiva, la limitazione del contesto a quanto necessario e attenzione all'identificazione indiretta. Richiama inoltre i vincoli specifici degli usi e degli ambienti di trattamento. [2]

La guida traduce gli obblighi professionali nelle pratiche dell'IA. Le sue raccomandazioni vanno distinte dalle disposizioni di legge e dal RIN a cui rinvia. La loro attuazione richiede un'organizzazione: usi autorizzati, preparazione delle richieste e validazione dei risultati.

Il ruolo del RGPD

Per i dati personali, la pseudonimizzazione rientra tra le misure di protezione previste dal RGPD, in particolare fin dalla progettazione e per la sicurezza del trattamento. Gli obblighi relativi a finalità, minimizzazione, disciplina dei rapporti con i fornitori e, ove applicabile, trasferimenti vanno esaminati nel contesto del trattamento. [9]

Conseguenze per la decisione professionale

Tre valutazioni si completano: il carattere personale dei dati, la riservatezza delle informazioni e la necessità del loro utilizzo. Un dato irrilevante per il compito può essere escluso; un dato necessario può richiedere una trasformazione; un contenuto il cui valore dipende dal segreto può richiedere un ambiente più ristretto.

La scelta non deriva quindi da una sola etichetta applicata al documento. Deriva dal compito, dalle informazioni utili e dal perimetro di fiducia prescelto.

Il contributo della legge californiana SB 574

La SB 574, capitolo 858 delle leggi del 2026, è stata promulgata il 30 settembre 2026. La sua entrata in vigore è attesa per il 1° gennaio 2027 secondo il calendario costituzionale ordinario. [1][3][6]

Il nuovo articolo 6068.1 del Business and Professions Code vieta di delegare l'esercizio della professione legale a un'IA generativa. Disciplina l'inserimento di informazioni riservate, identificative o non pubbliche limitando l'accesso all'avvocato e alle persone autorizzate soggette a obblighi di riservatezza. Impone inoltre una verifica ragionevole dei risultati e la correzione degli errori. L'uso dell'IA deve essere dichiarato al tribunale per i documenti contemplati che gli vengono presentati; per i contenuti destinati al pubblico occorre valutare se renderlo noto. [1]

L'articolo 128.7 del Code of Civil Procedure, come modificato, richiede la verifica personale delle citazioni da parte dell'avvocato responsabile del deposito, comprese quelle prodotte dall'IA. La presente analisi riguarda gli avvocati; le disposizioni relative agli arbitri e alle istituzioni giudiziarie non sono approfondite. Il testo non prescrive un'anonimizzazione generalizzata. [1]

Due regimi e preoccupazioni comuni

I testi francesi e californiani non sono intercambiabili. I primi combinano segreto professionale, protezione dei dati e raccomandazioni pratiche. I secondi formulano, in particolare, un requisito di limitazione degli accessi per gli usi contemplati. Un'attività soggetta a più giurisdizioni va esaminata alla luce di ciascuna.

Il loro confronto consente tuttavia di individuare questioni progettuali comuni: quali informazioni vengono comunicate, a chi diventano accessibili e in che modo il professionista mantiene il controllo del risultato? Questa lettura comparativa riguarda i problemi da risolvere, senza uniformare le regole.

Il contributo della pseudonimizzazione a questa analisi

La pseudonimizzazione può ridurre l'esposizione delle identità nei trattamenti interessati. Le condizioni di accesso e la riservatezza del contenuto restante costituiscono un ulteriore livello di valutazione. È utile documentare separatamente queste dimensioni: una misura sugli identificatori non descrive, di per sé, le autorizzazioni alla consultazione.

Una valutazione rigorosa ricerca quindi le proprietà del trattamento anziché una corrispondenza terminologica. Espressioni come «privato», «professionale» o «sicuro» vanno precisate in relazione al perimetro dei dati, alle operazioni effettuate e agli impegni applicabili.

Definire le protezioni senza confonderle

I termini seguenti indicano proprietà diverse. Distinguerli consente di scegliere una misura in funzione del risultato atteso e di definire ciò che dovrà essere verificato. [7][8][9]

Misura	Proprietà ricercata	Conseguenza per il lavoro
Anonimizzazione	Rendere l'identificazione impraticabile in modo irreversibile, tenendo conto dei mezzi ragionevolmente utilizzabili.	Adatta a un uso che non richiede di risalire alle identità.
Pseudonimizzazione	Separare i dati dall'identità mediante informazioni aggiuntive protette.	Consente una riattribuzione controllata; resta da verificare la restituzione nell'elaborato finale.
Minimizzazione	Limitare i dati alle esigenze del compito.	Riduce il contesto da trattare e le informazioni esposte.
Limitazione degli accessi	Limitare la consultazione ai destinatari autorizzati.	Disciplina l'utilizzo degli originali e dei contenuti trasformati.

La reversibilità è una scelta funzionale

Una pubblicazione può richiedere un risultato anonimo; un atto può richiedere di ritrovare le parti. La reversibilità è allora un'opzione funzionale, non una qualità superiore in sé. La separazione delle informazioni di riattribuzione e la limitazione dei relativi accessi fanno parte della pseudonimizzazione ai sensi del RGPD. [9, art. 4, par. 5]

Il contesto determina il rischio di identificazione

Nella valutazione dell'anonimizzazione, la CNIL distingue in particolare i rischi di individuazione, correlazione e inferenza. La possibilità di riconoscere una persona dipende anche dalle informazioni complementari disponibili. L'esame deve quindi riguardare le combinazioni di indizi e i destinatari. [7]

Per lo studio che conserva i mezzi di riattribuzione, la sola sostituzione delle identità non sottrae il trattamento all'ambito della protezione dei dati personali. [8][9]

Un modello di rischio adatto alla pratica legale

Il modello proposto distingue quattro dimensioni. Serve a preparare l'analisi di un uso; non presuppone la conoscenza dei processi interni di un fornitore.

Gli identificatori diretti

Nomi, recapiti e riferimenti individuali possono collegare immediatamente un testo a una persona o a un'organizzazione. La loro presenza va esaminata nella richiesta e nei contenuti associati, compresi i nomi dei file e i commenti pertinenti al trattamento.

Gli indizi di riconoscimento

Una funzione rara, un luogo, un importo e un periodo possono rendere riconoscibile un'operazione. Ogni elemento, preso separatamente, sembra generico; la loro combinazione può essere distintiva. La valutazione deve considerare l'insieme delle informazioni conservate e le conoscenze del destinatario.

Le informazioni riservate per il loro contenuto

Un prezzo di riserva, una possibile concessione o una debolezza procedurale hanno valore indipendentemente dal nome del cliente. La loro protezione dipende anche dal perimetro degli accessi e dalla necessità di trasmetterle. Un metodo incentrato sulle sole identità trascurerebbe questa dimensione della pratica.

La circolazione e la durata

Un'informazione può riapparire quando si aggiunge un documento, si riprende il lavoro o si produce una sintesi intermedia. Può anche trovarsi in una traccia, una copia o un elaborato finale. Occorre esaminare l'insieme dei passaggi in cui l'informazione cambia destinatario, forma o finalità.

Formulare un'ipotesi di rischio verificabile

Una formulazione utile precisa un destinatario, un contenuto e una conseguenza: «Il collegamento tra questi tre elementi consentirebbe a tale soggetto di riconoscere l'operazione». Si può poi esaminare se gli elementi siano necessari, se possano essere trasformati e quali condizioni di accesso siano adeguate.

La letteratura istituzionale sulla de-identificazione sottolinea il compromesso tra utilità e protezione, nonché la possibilità di reidentificare alcuni insiemi di dati trasformati. Questa osservazione giustifica una valutazione contestualizzata anziché una conclusione fondata sulla sola presenza di un mascheramento.

[10]

Esaminare il percorso completo delle informazioni

La griglia seguente descrive fasi funzionali. Può essere utilizzata per un servizio integrato o per una combinazione di più strumenti. Ogni fase richiede una verifica del contenuto e dei destinatari.

Fase	Domanda centrale	Elemento da esaminare
Ricezione	Quale contesto entra nel servizio?	Richiesta, scambi utili, documenti e accessi iniziali.
Preparazione	Chi accede al contenuto per renderlo utilizzabile?	Estrazione, riconoscimento del testo e servizi coinvolti.
Trasformazione	Quali informazioni vengono modificate o escluse?	Perimetro dei dati e coerenza della preparazione.
Trattamenti	Quale contesto circola tra le fasi?	Ricerche, analisi, risultati intermedi e dipendenze.
Restituzione	Come si ottiene nuovamente un risultato utilizzabile?	Risposta, file, ruoli delle parti e controlli di restituzione.
Conservazione	Che cosa resta dopo il lavoro?	Documenti, tracce, accessi persistenti e durate prescelte.

La preparazione fa parte del perimetro

Il trattamento giuridico non è necessariamente il primo momento in cui un servizio accede al contenuto. La conversione di un documento o il riconoscimento del suo testo possono avvenire prima. La mappatura include queste operazioni e i loro destinatari, anche se il contenuto viene successivamente pseudonimizzato.

La restituzione è una nuova fase di riservatezza

Un elaborato in cui le identità sono state ripristinate contiene nuovamente identificatori espliciti; il suo contenuto poteva già essere riservato prima di tale restituzione. Occorre esaminarne i destinatari, il luogo di archiviazione e i diritti di accesso. Il ritorno alle informazioni originarie è una funzione utile le cui condizioni vanno previste fin dall'inizio.

Questa mappatura offre una base comune ai team legali, ai responsabili della protezione dei dati e ai progettisti del servizio. Collega ogni fase a dati, destinatari ed evidenze osservabili.

Preservare la fedeltà del ragionamento giuridico

Ciò che deve restare esatto

La qualità di una trasformazione non si riduce al numero di elementi sostituiti. Un ragionamento può dipendere da una cronologia, da una qualità giuridica o da una relazione tra due parti. La preparazione deve preservare questi elementi quando la loro modifica cambierebbe l'analisi.

Conservare un termine di un mese, una data di ricezione o un tasso può essere decisivo. Generalizzare automaticamente una data all'anno o un importo a un ordine di grandezza può essere pertinente per una pubblicazione statistica, ma inadeguato per calcolare una scadenza o un credito.

Ciò che deve restare coerente

La stessa persona può comparire come mandatario in un documento, dirigente in un altro e firmatario in un terzo. Va mantenuta la distinzione tra l'identità del soggetto e la qualità nella quale interviene. Il collegamento tra i ruoli è una proprietà giuridica da preservare.

La coerenza riguarda anche i documenti successivi. Un atto integrativo può modificare soltanto un obbligo o soltanto alcuni firmatari. La trasformazione deve consentire di confrontare questi stati senza fondere soggetti distinti né separare artificialmente lo stesso soggetto.

Ciò che deve poter essere restituito

La reversibilità va verificata sugli elementi trasformati e sui supporti effettivamente utilizzati. Il ripristino fedele di un testo preparato è un controllo diverso dalla restituzione in un documento generato: quest'ultimo può contenere formulazioni nuove, tabelle o commenti.

Due assi da valutare insieme

La protezione esamina ciò che si può apprendere sulle persone e sulla pratica. La fedeltà esamina ciò che consente ancora di ragionare correttamente e produrre un risultato utilizzabile. Una soluzione pertinente va valutata su entrambi gli assi per l'uso definito.

Il protocollo di valutazione deve quindi rilevare sia le informazioni da proteggere ancora presenti sia le trasformazioni che degradano il significato. La restituzione completa le verifiche; non sostituisce né l'una né l'altra.

Scegliere una protezione in funzione dell'esigenza

Il modello decisionale proposto parte dal lavoro atteso. Consente di confrontare più risposte, compresa la riduzione del contesto prima di ricorrere a una trasformazione.

1 La domanda può essere resa astratta?

Per comprendere un meccanismo giuridico generale, può bastare indicare il diritto applicabile e una situazione tipo. Una richiesta astratta evita di comunicare gli elementi propri della pratica. È adatta finché la specificità della risposta non dipende da fatti omessi.

2 Quali dati sono necessari?

Per le informazioni mantenute, precisarne la funzione: identificare un ruolo, accertare un fatto, calcolare una scadenza o interpretare una clausola. Un elemento privo di funzione nel compito può essere rimosso. Questa fase riduce il perimetro da proteggere e chiarisce il bisogno di contesto.

3 L'esigenza impone un ritorno alle identità?

Quando il risultato deve rientrare nella pratica con le sue parti identificate, la pseudonimizzazione reversibile è un'opzione da esaminare. Per una diffusione esterna senza ritorno alle identità, l'obiettivo di anonimizzazione richiede una valutazione distinta dell'identificabilità dell'insieme prodotto. [7][8]

4 Il contenuto conserva una propria sensibilità?

Un'informazione strategica può restare sensibile dopo la trasformazione degli identificatori. La sua conservazione dipende dalle esigenze del compito e dalle garanzie dell'ambiente. La scelta può riguardare un'ulteriore riduzione del contesto o un trattamento con accessi più ristretti.

5 Il risultato può essere validato?

Definire chi verificherà il contenuto restituito, i riferimenti e l'utilizzo previsto. Se il contesto disponibile non consente una risposta sufficientemente fondata, integrare la richiesta o rivedere il compito prima di utilizzare il risultato.

La scelta può combinare più misure. Una domanda astratta richiede poco contesto; una pubblicazione può richiedere un'anonimizzazione; un lavoro che richiede di risalire alle parti può richiedere una pseudonimizzazione. Un trattamento senza trasformazione impone un esame degli accessi e della riservatezza. Quando mancano garanzie adeguate, ridurre il compito o scegliere un altro ambiente.

Un protocollo per valutare i risultati

Una valutazione utile è riproducibile e legata a un uso. Il protocollo proposto può essere applicato a uno strumento sul mercato o a un sistema interno, a partire da pratiche fittizie rappresentative.

Costruire un insieme di riferimento

Prevedere più documenti collegati, soggetti con ruoli distinti, varianti nelle denominazioni ed elementi contestuali riconoscibili. Includere i supporti utilizzati nella pratica: testo della richiesta, documenti e commenti pertinenti. Definire in anticipo gli elementi da proteggere e quelli di cui va conservato il significato.

Esaminare protezione e fedeltà

Per ogni caso, confrontare il risultato con questo riferimento. Rilevare le informazioni da proteggere ancora presenti, le trasformazioni inutili e le alterazioni del significato. Registrare gli elementi sensibili trattati correttamente in rapporto agli elementi attesi, poi le sostituzioni ingiustificate in rapporto alle sostituzioni effettuate. Distinguere questi risultati dagli errori di ruolo, data o importo. Pubblicare i conteggi e la gravità degli errori: una sola percentuale nasconde i casi critici.

Dimensione	Osservazione da registrare
Protezione	Elementi attesi trattati correttamente e informazioni sensibili ancora presenti.
Fedeltà	Ruoli, fatti, relazioni, date e importi conservati quando necessari.
Restituzione	Elementi ripristinati, errori di corrispondenza e contenuti irrisolti.
Copertura	Formati, fasi e situazioni effettivamente esaminati.

Valutare anche le sequenze

Riprendere un risultato in una fase successiva, aggiungere un documento e verificare la restituzione finale. Osservare il comportamento quando un documento è incompleto o una trasformazione non può essere completata. La risposta attesa a queste situazioni va definita nel perimetro dell'uso.

Rendere interpretabile la conclusione

Registrare versione, impostazioni, data, casi, ripetizioni e correzioni. Far riesaminare le annotazioni controverse da un secondo valutatore. Definire prima delle prove gli errori che impediscono l'uso, quindi ripetere i test sui casi interessati dopo la correzione. Le pratiche fittizie rendono condivisibili le prove; non dimostrano, da sole, la copertura delle pratiche reali.

Tre casi pratici e i loro insegnamenti

Questi casi fittizi servono ad applicare il metodo. Non descrivono prestazioni misurate di uno strumento.

Un contratto e due atti integrativi

Il compito consiste nel determinare gli obblighi ancora applicabili. Il fascicolo comprende parti indicate in forme diverse e una persona che interviene a due titoli. La preparazione deve consentire il collegamento delle denominazioni mantenendo le qualità e la cronologia.

Il controllo riguarda la relazione tra i testi: quali clausole vengono modificate, per quali parti e a quale data? Le identità possono essere sostituite durante il trattamento e poi ripristinate nel risultato. Criterio decisionale: una confusione sul firmatario o sulla data impedisce l'utilizzo del risultato, anche se tutti i nomi sono stati sostituiti.

Una nota negoziale senza il nome del cliente

Una nota descrive un'operazione rara e l'importo minimo accettabile per il cliente. L'assenza del nome non elimina né la possibilità di riconoscere l'operazione né il valore strategico dell'importo. Occorre esaminare separatamente gli indizi di riconoscimento e la riservatezza del contenuto.

Se basta un'analisi generale, la richiesta può essere riformulata con un contesto più astratto. Se l'importo esatto è necessario, la sua trasmissione va valutata nell'ambiente prescelto. Criterio decisionale: scegliere la versione astratta se sufficiente; altrimenti esaminare le garanzie di trattamento dell'importo e della strategia prima della trasmissione.

Una richiesta seguita dalla produzione di una lettera

Un'analisi iniziale alimenta poi una bozza di lettera. Le informazioni trasformate passano attraverso più fasi, quindi le identità vengono ripristinate nell'elaborato finale. Il controllo riguarda l'insieme: contenuto iniziale, risultato intermedio, documento finale e destinatari.

La preparazione e la restituzione devono evitare di attribuire un fatto alla parte sbagliata o di riprendere un contesto divenuto incompleto. Criterio decisionale: approvare la lettera soltanto dopo aver verificato le attribuzioni, le informazioni ripristinate e il destinatario. Un risultato intermedio corretto non valida automaticamente l'elaborato finale.

Insegnamento comune

La protezione pertinente dipende tanto dalle relazioni tra le informazioni quanto dalla loro forma. La valutazione deve partire dal risultato giuridico atteso e risalire alle fasi che lo rendono possibile.

Organizzare responsabilità e tracciabilità

Definire un perimetro di fiducia

Lo studio identifica le categorie di lavori affidati all'IA, le informazioni interessate e le persone autorizzate. La mappatura dei destinatari include i servizi di preparazione e gli accessi necessari all'operatività. Gli impegni di riservatezza e il quadro dei trattamenti vengono esaminati con i responsabili competenti. [9]

Distinguere le validazioni

La validazione della preparazione riguarda il contesto e le protezioni scelti. La validazione del risultato riguarda i fatti, i riferimenti e la pertinenza giuridica. La decisione di trasmissione riguarda il destinatario e l'uso. Queste validazioni possono essere svolte dalla stessa persona, ma i loro oggetti restano distinti.

Conservare una traccia utile

La traccia documenta il compito, il perimetro prescelto, le verifiche e la decisione finale. Deve consentire di comprendere il lavoro senza moltiplicare copie inutili dei documenti o delle informazioni riservate. Gli accessi alle tracce e la loro durata di conservazione rientrano nello stesso esame previsto per i documenti.

Mantenere operative le regole dello studio

Una procedura breve può precisare gli usi comuni, le situazioni che richiedono un esame specifico e la condotta da seguire quando un contenuto è incompleto. Esempi fittizi aiutano i team a riconoscere le questioni di identificazione indiretta e riservatezza strategica.

Una revisione diventa utile quando cambia un uso, un formato, un soggetto coinvolto o una condizione di trattamento. La documentazione deve consentire di determinare quali conclusioni restano applicabili e quali controlli vanno ripetuti.

Preservare la libertà di scelta

Descrivere esigenze e criteri senza dipendere dal vocabolario di un fornitore rende le offerte più confrontabili. Lo studio può richiedere risposte sul percorso, sui dati, sugli accessi, sulla fedeltà e sulla restituzione, per poi valutare le evidenze pertinenti ai propri usi.

Questa disciplina è utile anche al progettista del servizio: precisa le proprietà attese e le situazioni che una dimostrazione deve consentire di osservare.

Scheda pratica da adattare a ciascun uso

Questa scheda riassume le decisioni e le osservazioni utili. Può essere ripresa in una procedura di studio, in un fascicolo di valutazione o in uno scambio con un fornitore.

Il compito

Risultato atteso: _____

Diritto e contesto utili: _____

Responsabile della validazione: _____

Le informazioni

Documenti e contenuti necessari: _____

Dati da rimuovere o trasformare: _____

Informazioni riservate da trattare separatamente: _____

Il percorso e i destinatari

Preparazione dei documenti e soggetti coinvolti: _____

Trattamenti e accessi autorizzati: _____

Restituzione, archiviazione e destinatari degli elaborati: _____

Conservazione dei documenti e delle tracce: _____

Le proprietà da preservare

Ruoli, fatti e relazioni indispensabili: _____

Date e importi determinanti: _____

Elementi da ripristinare nel risultato: _____

Le osservazioni e la decisione

Casi rappresentativi esaminati: _____

Informazioni sensibili residue: _____

Alterazioni di significato o errori di restituzione: _____

Decisione, condizioni d'uso e data: _____

Un uso è documentato quando il professionista può spiegare che cosa si attende dal trattamento, quali informazioni vi immette, quali protezioni sceglie e su cosa si basa la decisione di utilizzare il risultato.

Conclusioni e prospettive

La scelta di una protezione parte dall'esigenza giuridica e dalle informazioni necessarie. Astrazione, minimizzazione, anonimizzazione, pseudonimizzazione e limitazione degli accessi rispondono a obiettivi diversi e possono essere combinate. La loro pertinenza si valuta sul percorso reale, sulla riservatezza del contenuto e sulla fedeltà del risultato, senza presumere che una misura sia adatta a tutte le pratiche.

Valutare un percorso anziché un testo isolato

La richiesta, i documenti, i servizi di preparazione, i trattamenti successivi e la restituzione formano un insieme. Le stesse informazioni possono cambiare forma e destinatario più volte. Questa continuità deve figurare nella mappatura e nelle prove.

Misurare la protezione insieme alla fedeltà giuridica

La conservazione delle qualità, dei fatti e delle relazioni è un criterio di qualità necessario quanto il trattamento degli identificatori. Una valutazione deve rendere visibili gli errori di protezione e le alterazioni del significato, per poi esaminare la restituzione sui supporti effettivamente utilizzati.

Documentare decisioni trasferibili

Una descrizione chiara del compito, del perimetro e dei criteri consente di discutere le scelte tra professionisti. Le griglie proposte sono destinate a essere adattate, confrontate con nuovi casi e arricchite dall'esperienza; non costituiscono uno standard di certificazione. Possono fungere da linguaggio comune per studi legali, responsabili della protezione dei dati e progettisti di servizi.

Ambiti di lavoro

Le valutazioni trarrebbero beneficio da una maggiore copertura di pratiche con più documenti, riprese del contesto e formati di restituzione. Un confronto utile renderebbe pubblici i casi, i criteri e la natura degli errori, proteggendo al contempo le informazioni delle pratiche. Distinguerebbe le proprietà di un componente da quelle del percorso completo.

Informazioni su questa pubblicazione

Questo libro bianco è pubblicato da AIDocs Studio, editore di Max. Propone un quadro di riflessione e strumenti metodologici applicabili a qualsiasi servizio di IA giuridica. Le analisi sono quelle dell'editore; le istituzioni citate costituiscono le fonti di riferimento. Stato della ricerca documentale al 16 ottobre 2026.

Riferimenti normativi e professionali

[1] California • Senate Bill 574

Capitolo 858 delle leggi del 2026. Testo promulgato, in particolare sezioni 1 e 3. Riproduzione LegiScan.

Fonte: legiscan.com

[2] Conseil national des barreaux • 2026

La déontologie et l'intelligence artificielle. Guida pratica, prima edizione, aprile 2026, in particolare pagine 15–18.

Fonte: cnb.avocat.fr

[3] Governatore della California • 30 settembre 2026

Comunicato istituzionale che menziona la SB 574 tra le leggi firmate.

Fonte: www.gov.ca.gov

[4] Francia • Legge n. 71-1130 del 31 dicembre 1971

Articolo 66-5, relativo al segreto professionale dell'avvocato.

Fonte: www.legifrance.gouv.fr

[5] Conseil national des barreaux • RIN

Titolo primo, articolo 2: principi ed estensione del segreto professionale.

Fonte: cnb.avocat.fr

Riferimenti sulla protezione delle informazioni

[6] Costituzione della California

Articolo IV, sezione 8. Calendario ordinario di entrata in vigore. La data attesa per la SB 574 è dedotta da questo calendario. Riproduzione istituzionale degli organi giudiziari californiani.

Fonte: courts.ca.gov

[7] CNIL • 19 maggio 2020

L'anonymisation de données personnelles. Definizione e rischi di reidentificazione.

Fonte: www.cnil.fr

[8] CNIL • 13 gennaio 2022

Recherche scientifique hors santé : enjeux et avantages de l'anonymisation et de la pseudonymisation. Riferimento per la distinzione dei concetti.

Fonte: www.cnil.fr

[9] Unione europea • Regolamento (UE) 2016/679

RGPD, in particolare articolo 4, paragrafo 5; articoli 5, 25, 28 e 32; capo V per i trasferimenti interessati.

Fonte: eur-lex.europa.eu

[10] Garfinkel S L • NIST • 2015

De-Identification of Personal Information. NISTIR 8053. Sintesi della ricerca sulla de-identificazione, sulla sua utilità e sui rischi di reidentificazione. DOI: 10.6028/NIST.IR.8053.

Fonte: csrc.nist.gov