



LIVRE BLANC

Confidentialité et intelligence artificielle juridique

Anonymisation et pseudonymisation des dossiers
Cadre de référence pour la profession juridique

Analyse des textes français et californiens
Principes de conception et méthode d'évaluation

Comment réduire l'exposition des informations confiées à un système d'IA tout en conservant ce qui est
nécessaire au raisonnement juridique et à la restitution du résultat ?

Une publication AIDocs Studio · Max
Octobre 2026 · Première édition révisée

Résumé et méthode

Résumé

La confidentialité d'un dossier juridique se joue dans les informations qui circulent, leurs destinataires et les usages qui en sont faits. Le remplacement des noms est une mesure utile, mais son intérêt doit être apprécié avec le contenu restant et le travail attendu. Une transformation qui protège une identité tout en altérant une qualité, une date ou une obligation peut rendre le résultat juridiquement inadéquat.

Ce livre blanc propose un cadre pour examiner conjointement la protection des informations, la fidélité du contexte et la restitution des résultats. Il s'appuie sur les règles françaises du secret professionnel, les recommandations du CNB, le RGPD, la loi californienne SB 574 et des références institutionnelles sur la dé-identification. [1–10]

La conclusion centrale est que l'unité pertinente d'évaluation est le parcours de traitement. La protection doit être examinée à la réception, pendant la préparation documentaire et les traitements successifs, puis au moment de la restitution. Une vérification isolée sur un texte ne décrit pas à elle seule les propriétés de cet ensemble.

Méthode et statut des propositions

La démarche compare un corpus ciblé de textes juridiques, de recommandations professionnelles et de travaux institutionnels, sélectionnés pour leur lien direct avec la confidentialité des dossiers. Elle est complétée par un modèle de décision et un protocole d'évaluation ; elle ne constitue pas une revue systématique de la littérature. Les développements distinguent les exigences des textes, leur interprétation pour les usages de l'IA et les propositions méthodologiques de cette publication. Les références numérotées permettent de revenir aux sources ; les propositions de méthode sont celles de cette publication.

Les exemples sont fictifs. Les grilles et indicateurs constituent des outils de travail à adapter ; ils ne sont pas présentés comme une norme adoptée par les institutions citées. L'étude concerne principalement les dossiers d'avocat. Les autres professionnels peuvent reprendre la méthode en tenant compte des secrets et obligations propres à leur statut.

Apports proposés

Une distinction entre protection des identités, confidentialité du contenu et fidélité juridique.

Une lecture du parcours complet, de la demande aux livrables.

Une méthode pour choisir la protection et examiner ses résultats sur un usage défini.

Les fondements français de la protection

Le secret professionnel couvre le dossier

L'article 66-5 de la loi du 31 décembre 1971 protège notamment les consultations, les correspondances et les pièces du dossier. L'article 2 du RIN en précise l'étendue. Le secret porte ainsi sur des informations qui ne se réduisent pas aux données identifiant une personne physique. [4][5]

Cette distinction est déterminante pour l'IA. Une stratégie contentieuse, un projet de transaction ou un savoir-faire peuvent rester confidentiels après suppression des noms. La question à examiner est celle du contenu effectivement communiqué et des conditions de son traitement.

La recommandation du CNB

Le guide La déontologie et l'intelligence artificielle, première édition d'avril 2026, recommande une pseudonymisation ou une anonymisation préalable, une limitation du contexte au nécessaire et une vigilance sur l'identification indirecte. Il rappelle aussi les contraintes propres aux usages et aux environnements de traitement. [2]

Ce guide traduit les obligations professionnelles dans les pratiques de l'IA. Ses recommandations doivent être distinguées des dispositions légales et du RIN auxquels il renvoie. Leur mise en œuvre appelle une organisation : usages autorisés, préparation des demandes et validation des résultats.

La place du RGPD

Pour les données personnelles, la pseudonymisation s'inscrit dans les mesures de protection envisagées par le RGPD, notamment dès la conception et pour la sécurité des traitements. Les obligations de finalité, de minimisation, d'encadrement des prestataires et, le cas échéant, des transferts doivent être examinées dans le contexte du traitement. [9]

Conséquence pour la décision professionnelle

Trois examens se complètent : le caractère personnel des données, le caractère confidentiel des informations et la nécessité de leur utilisation. Une donnée sans intérêt pour la tâche peut être écartée ; une donnée nécessaire peut exiger une transformation ; un contenu dont la valeur tient au secret peut appeler un environnement plus restreint.

Le choix ne découle donc pas d'une seule étiquette appliquée au document. Il résulte de la tâche, des informations utiles et du périmètre de confiance retenu.

L'apport de la loi californienne SB 574

SB 574, chapitre 858 des lois de 2026, a été promulguée le 30 septembre 2026. Son entrée en vigueur est attendue au 1er janvier 2027 selon le calendrier constitutionnel ordinaire. [1][3][6]

Le nouvel article 6068.1 du Business and Professions Code interdit de déléguer l'exercice du droit à une IA générative. Il encadre la saisie d'informations confidentielles, identifiantes ou non publiques par une restriction des accès à l'avocat et aux personnes autorisées soumises à des obligations de confidentialité. Il impose aussi la vérification raisonnable des sorties et la correction des erreurs. L'usage de l'IA doit être déclaré au tribunal pour les documents visés qui lui sont soumis ; sa divulgation doit être envisagée pour les contenus destinés au public. [1]

L'article 128.7 du Code of Civil Procedure, modifié, exige la vérification personnelle des citations par l'avocat responsable du dépôt, y compris celles issues de l'IA. La présente analyse porte sur les avocats ; les dispositions relatives aux arbitres et aux institutions judiciaires ne sont pas détaillées. Le texte ne prescrit pas une anonymisation générale. [1]

Deux régimes et des préoccupations communes

Les textes français et californien ne sont pas interchangeables. Le premier ensemble associe secret professionnel, protection des données et recommandations de pratique. Le second formule notamment une exigence de restriction des accès dans les usages qu'il vise. Une activité relevant de plusieurs juridictions doit être examinée au regard de chacune.

Leur rapprochement permet néanmoins d'identifier des questions de conception communes : quelles informations sont communiquées, à qui deviennent-elles accessibles et comment le professionnel conserve-t-il le contrôle du résultat ? Cette lecture comparative porte sur les problèmes à résoudre, sans uniformiser les règles.

Ce que la pseudonymisation apporte à cette lecture

La pseudonymisation peut réduire l'exposition des identités dans les traitements concernés. Les conditions d'accès et la confidentialité du contenu restant constituent un autre niveau d'examen. Il est utile de documenter ces dimensions séparément : une mesure portant sur les identifiants ne décrit pas, par elle-même, les autorisations de consultation.

Une évaluation sérieuse recherche donc les propriétés du traitement plutôt qu'une correspondance de vocabulaire. Les termes « privé », « professionnel » ou « sécurisé » doivent être précisés par le périmètre des données, les opérations réalisées et les engagements applicables.

Définir les protections sans les confondre

Les termes suivants désignent des propriétés différentes. Les distinguer permet de choisir une mesure en fonction du résultat attendu et de définir ce qui devra être vérifié. [7][8][9]

Mesure	Propriété recherchée	Conséquence pour le travail
Anonymisation	Rendre l'identification impraticable de façon irréversible, compte tenu des moyens raisonnablement susceptibles d'être utilisés.	Appropriée à un usage ne nécessitant pas de revenir aux identités.
Pseudonymisation	Dissocier les données de l'identité avec une information supplémentaire protégée.	Autorise une réattribution sous contrôle ; la restitution du livrable reste à vérifier.
Minimisation	Limiter les données au besoin de la tâche.	Réduit le contexte à traiter et les informations exposées.
Restriction des accès	Limiter la consultation aux destinataires autorisés.	Encadre l'utilisation des originaux et des contenus transformés.

La réversibilité est un choix fonctionnel

Une publication peut nécessiter un résultat anonyme ; un acte peut nécessiter de retrouver les parties. La réversibilité est alors une option fonctionnelle, non une qualité supérieure en soi. La séparation de l'information de réattribution et la restriction de ses accès font partie de la pseudonymisation au sens du RGPD. [9, art. 4 § 5]

Le contexte détermine le risque d'identification

La CNIL distingue notamment les risques d'individualisation, de corrélation et d'inférence dans l'appréciation de l'anonymisation. La possibilité de reconnaître une personne dépend aussi des informations disponibles en complément. L'examen doit donc porter sur les combinaisons d'indices et sur les destinataires. [7]

Pour le cabinet qui conserve les moyens de réattribution, le seul remplacement des identités ne fait pas sortir le traitement du champ de la protection des données personnelles. [8][9]

Un modèle de risque adapté au dossier juridique

Le modèle proposé distingue quatre dimensions. Il sert à préparer l'analyse d'un usage ; il ne suppose pas de connaître les procédés internes d'un prestataire.

Les identifiants directs

Les noms, coordonnées et références individuelles peuvent relier immédiatement un texte à une personne ou à une organisation. Leur présence doit être examinée dans la demande et dans les contenus associés, y compris les titres de fichiers et les commentaires pertinents pour le traitement.

Les indices de reconnaissance

Une fonction rare, un lieu, un montant et une période peuvent rendre une opération reconnaissable. Chaque élément pris séparément semble général ; leur réunion peut être distinctive. L'évaluation doit considérer la combinaison des informations conservées et les connaissances du destinataire.

Les informations confidentielles par leur contenu

Un prix de réserve, une concession possible ou une faiblesse de procédure ont une valeur indépendamment du nom du client. Leur protection relève aussi du périmètre d'accès et du besoin de les transmettre. Une méthode centrée sur les seules identités manquerait cette dimension du dossier.

La circulation et la durée

Une information peut réapparaître lors d'un ajout de pièce, d'une reprise ou d'une synthèse intermédiaire. Elle peut aussi se retrouver dans une trace, une copie ou un livrable. L'objet à examiner est l'ensemble des passages où l'information change de destinataire, de forme ou de finalité.

Formuler une hypothèse de risque vérifiable

Une formulation utile précise un destinataire, un contenu et une conséquence : « Le rapprochement de ces trois éléments permettrait à tel intervenant de reconnaître l'opération. » On peut ensuite examiner si les éléments sont nécessaires, s'ils peuvent être transformés et quelles conditions d'accès sont adaptées.

La littérature institutionnelle sur la dé-identification souligne le compromis entre utilité et protection, ainsi que la possibilité de réidentification de certains ensembles transformés. Cette observation justifie une évaluation contextualisée plutôt qu'une conclusion fondée sur la seule présence d'un masquage. [10]

Examiner le parcours complet des informations

La grille suivante décrit des étapes fonctionnelles. Elle peut être utilisée pour un service intégré comme pour un assemblage de plusieurs outils. Chaque étape appelle une vérification de son contenu et de ses destinataires.

Étape	Question centrale	Élément à examiner
Réception	Quel contexte entre dans le service ?	Demande, échanges utiles, pièces et accès initiaux.
Préparation	Qui accède au contenu pour le rendre utilisable ?	Extraction, reconnaissance du texte et services intervenants.
Transformation	Quelles informations sont modifiées ou écartées ?	Périmètre des données et cohérence de la préparation.
Traitements	Quel contexte circule entre les étapes ?	Recherches, analyses, résultats intermédiaires et dépendances.
Restitution	Comment revient-on au résultat exploitable ?	Réponse, fichiers, rôles des parties et contrôles de restitution.
Conservation	Que reste-t-il après le travail ?	Documents, traces, accès persistants et durées retenues.

La préparation fait partie du périmètre

Le traitement juridique n'est pas nécessairement le premier moment où un service accède au contenu. La conversion d'un document ou la reconnaissance de son texte peut intervenir auparavant. La cartographie inclut ces opérations et leurs destinataires, même si le contenu est ensuite pseudonymisé.

La restitution est une nouvelle étape de confidentialité

Un livrable où les identités sont rétablies contient de nouveau des identifiants explicites ; son contenu pouvait déjà être confidentiel avant cette restitution. Il faut examiner ses destinataires, son lieu de dépôt et ses droits d'accès. Le retour aux informations d'origine est une fonction utile dont les conditions doivent être prévues dès le début.

Cette cartographie fournit une base commune aux équipes juridiques, aux responsables de la protection des données et aux concepteurs du service. Elle relie chaque étape à des données, des destinataires et des preuves observables.

Préserver la fidélité du raisonnement juridique

Ce qui doit rester exact

La qualité d'une transformation ne se résume pas au nombre d'éléments remplacés. Un raisonnement peut dépendre d'une chronologie, d'une qualité juridique ou d'une relation entre deux parties. La préparation doit préserver ces éléments lorsque leur modification changerait l'analyse.

La conservation d'un délai d'un mois, d'une date de réception ou d'un taux peut être décisive. Généraliser automatiquement une date à une année ou un montant à un ordre de grandeur peut être pertinent pour une publication statistique, mais inadéquat pour le calcul d'une échéance ou d'une créance.

Ce qui doit rester cohérent

Une même personne peut apparaître comme mandataire dans une pièce, dirigeante dans une autre et signataire dans une troisième. Il faut maintenir la distinction entre l'identité de l'acteur et la qualité dans laquelle il intervient. Le rapprochement des rôles est une propriété juridique à préserver.

La cohérence concerne aussi les documents successifs. Un avenant peut modifier seulement une obligation ou seulement certains signataires. La transformation doit permettre de comparer ces états sans fusionner des acteurs distincts ni dissocier artificiellement le même intervenant.

Ce qui doit pouvoir être restitué

La réversibilité se vérifie sur les éléments transformés et sur les supports réellement utilisés. Le retour fidèle d'un texte préparé est un contrôle différent de la restitution dans un document généré : ce dernier peut contenir des formulations nouvelles, des tableaux ou des commentaires.

Deux axes à évaluer ensemble

La protection examine ce qui peut être appris sur les personnes et le dossier. La fidélité examine ce qui permet encore de raisonner correctement et de produire un résultat exploitable. Une solution pertinente doit être appréciée sur ces deux axes pour l'usage défini.

Le protocole d'évaluation doit donc relever à la fois les informations à protéger qui subsistent et les transformations qui dégradent le sens. La restitution complète les vérifications ; elle ne remplace ni l'une ni l'autre.

Choisir une protection en fonction du besoin

Le modèle de décision proposé part du travail attendu. Il permet de comparer plusieurs réponses, y compris la réduction du contexte avant tout recours à une transformation.

1 La question peut-elle être abstraite

Pour comprendre un mécanisme juridique général, il peut suffire d'indiquer le droit applicable et une situation type. Une demande abstraite évite de communiquer les éléments propres au dossier. Elle convient tant que la particularité de la réponse ne dépend pas de faits omis.

2 Quelles données sont nécessaires

Pour les informations retenues, préciser leur fonction : identifier un rôle, établir un fait, calculer une échéance ou interpréter une clause. Un élément sans fonction dans la tâche peut être retiré. Cette étape réduit le périmètre à protéger et clarifie le besoin de contexte.

3 Le besoin impose-t-il un retour aux identités

Lorsque le résultat doit rejoindre le dossier avec ses parties, une pseudonymisation réversible est une option à examiner. Pour une diffusion extérieure sans retour aux identités, l'objectif d'anonymisation appelle une évaluation distincte du caractère identifiable de l'ensemble produit. [7][8]

4 Le contenu conserve-t-il une sensibilité propre

Une information stratégique peut rester sensible après transformation des identifiants. Son maintien dépend du besoin de la tâche et des garanties de l'environnement. Le choix peut porter sur une réduction supplémentaire du contexte ou sur un traitement à accès plus restreint.

5 Le résultat peut-il être validé

Définir qui vérifiera le contenu restitué, les références et l'utilisation envisagée. Si le contexte disponible ne permet pas une réponse suffisamment fondée, compléter la demande ou revoir la tâche avant d'utiliser le résultat.

Le choix peut combiner plusieurs mesures. Une question abstraite appelle peu de contexte ; une publication peut appeler une anonymisation ; un travail avec retour aux parties peut appeler une pseudonymisation. Un traitement sans transformation exige un examen des accès et de la confidentialité. Lorsque les garanties adaptées ne sont pas réunies, réduire la tâche ou choisir un autre environnement.

Un protocole pour évaluer les résultats

Une évaluation utile est reproductible et liée à un usage. Le protocole proposé peut être appliqué à un outil du marché ou à un dispositif interne, à partir de dossiers fictifs représentatifs.

Construire un jeu de référence

Prévoir plusieurs pièces liées, des intervenants aux rôles distincts, des variantes de désignation et des éléments contextuels reconnaissables. Inclure les supports utilisés dans la pratique : texte de demande, documents et commentaires pertinents. Définir à l'avance les éléments à protéger et ceux dont le sens doit être conservé.

Examiner la protection et la fidélité

Pour chaque cas, comparer le résultat à cette référence. Relever les informations à protéger qui subsistent, les transformations inutiles et les altérations de sens. Consigner les éléments sensibles correctement traités rapportés aux éléments attendus, puis les substitutions injustifiées rapportées aux substitutions réalisées. Distinguer ces résultats des erreurs de rôle, de date ou de montant. Publier les effectifs et la gravité des erreurs : un pourcentage seul masque les cas critiques.

Dimension	Observation à consigner
Protection	Éléments attendus correctement traités et informations sensibles encore présentes.
Fidélité	Rôles, faits, relations, dates et montants conservés lorsque nécessaires.
Restitution	Éléments rétablis, erreurs de correspondance et contenus non résolus.
Couverture	Formats, étapes et situations effectivement examinés.

Évaluer aussi les enchaînements

Reprendre un résultat dans une étape suivante, ajouter une pièce et vérifier la restitution finale. Observer le comportement lorsqu'un document est incomplet ou qu'une transformation ne peut pas aboutir. La réponse attendue à ces situations doit être définie dans le périmètre de l'usage.

Rendre la conclusion interprétable

Consigner version, réglages, date, cas, répétitions et corrections. Faire relire les annotations litigieuses par un second évaluateur. Définir avant les essais les erreurs bloquantes pour l'usage, puis retester les cas concernés après correction. Les dossiers fictifs rendent les essais partageables ; ils ne démontrent pas à eux seuls la couverture des dossiers réels.

Trois cas pratiques et leurs enseignements

Ces cas fictifs servent à appliquer la méthode. Ils ne décrivent pas une performance mesurée d'un outil.

Un contrat et deux avenants

La tâche consiste à déterminer les obligations encore applicables. Le dossier comporte des parties désignées sous des formes variables et une personne intervenant à deux titres. La préparation doit permettre le rapprochement des désignations tout en maintenant les qualités et la chronologie.

Le contrôle porte sur la relation entre les textes : quelles clauses sont modifiées, pour quelles parties et à quelle date ? Les identités peuvent être substituées pendant le traitement, puis restituées dans le résultat. Critère de décision : une confusion de signataire ou de date bloque l'utilisation du résultat, même si tous les noms ont été remplacés.

Une note de négociation sans nom de client

Une note décrit une opération rare et le montant minimal acceptable par le client. L'absence de nom ne supprime ni la possibilité de reconnaître l'opération ni la valeur stratégique du montant. Il faut examiner séparément les indices de reconnaissance et la confidentialité du contenu.

Si une analyse générale suffit, la demande peut être reformulée avec un contexte plus abstrait. Si le montant exact est nécessaire, sa transmission doit être appréciée dans l'environnement retenu. Critère de décision : retenir la version abstraite si elle suffit ; sinon examiner les garanties de traitement du montant et de la stratégie avant transmission.

Une requête suivie de la production d'un courrier

Une analyse initiale alimente ensuite un projet de courrier. Les informations transformées passent entre plusieurs étapes, puis les identités sont rétablies dans le livrable. Le contrôle porte sur l'ensemble : contenu de départ, résultat intermédiaire, document final et destinataires.

La préparation et la restitution doivent éviter d'attribuer un fait à la mauvaise partie ou de reprendre un contexte devenu incomplet. Critère de décision : ne retenir le courrier qu'après vérification des attributions, des informations rétablies et de son destinataire. Un résultat intermédiaire correct ne valide pas automatiquement le livrable.

Enseignement commun

La protection pertinente dépend autant des relations entre les informations que de leur forme. L'évaluation doit partir du résultat juridique attendu et remonter les étapes qui le rendent possible.

Organiser la responsabilité et la traçabilité

Définir un périmètre de confiance

Le cabinet identifie les catégories de travaux confiés à l'IA, les informations concernées et les personnes autorisées. La cartographie des destinataires inclut les services de préparation et les accès nécessaires à l'exploitation. Les engagements de confidentialité et le cadre des traitements sont examinés avec les responsables compétents. [9]

Distinguer les validations

La validation de la préparation porte sur le contexte et les protections choisis. La validation du résultat porte sur les faits, les références et la pertinence juridique. La décision de transmission porte sur le destinataire et l'usage. Ces validations peuvent être réalisées par une même personne, mais leurs objets restent distincts.

Conserver une trace utile

La trace documente la tâche, le périmètre retenu, les vérifications et la décision finale. Elle doit permettre de comprendre le travail sans multiplier les copies inutiles des pièces ou des informations confidentielles. Les accès aux traces et leur durée de conservation entrent dans le même examen que ceux des documents.

Faire vivre les règles du cabinet

Une procédure courte peut préciser les usages courants, les situations nécessitant un examen particulier et la conduite à tenir lorsqu'un contenu est incomplet. Des exemples fictifs aident les équipes à reconnaître les questions d'identification indirecte et de confidentialité stratégique.

Une revue devient utile lorsqu'un usage, un format, un intervenant ou une condition de traitement change. La documentation doit permettre de déterminer quelles conclusions restent applicables et quels contrôles doivent être repris.

Préserver la liberté de choix

Décrire les besoins et les critères sans dépendre du vocabulaire d'un fournisseur rend les offres plus comparables. Le cabinet peut demander des réponses sur le parcours, les données, les accès, la fidélité et la restitution, puis apprécier les preuves correspondant à ses usages.

Cette discipline sert aussi le concepteur du service : elle précise les propriétés attendues et les situations qu'une démonstration doit permettre d'observer.

Fiche pratique à adapter à chaque usage

Cette fiche résume les décisions et observations utiles. Elle peut être reprise dans une procédure de cabinet, un dossier d'évaluation ou un échange avec un prestataire.

La tâche

Résultat attendu : _____

Droit et contexte utiles : _____

Responsable de la validation : _____

Les informations

Pièces et contenus nécessaires : _____

Données à retirer ou à transformer : _____

Informations confidentielles à traiter séparément : _____

Le parcours et les destinataires

Préparation des documents et intervenants : _____

Traitements et accès autorisés : _____

Restitution, dépôt et destinataires des livrables : _____

Conservation des documents et des traces : _____

Les propriétés à préserver

Rôles, faits et relations indispensables : _____

Dates et montants déterminants : _____

Éléments à restituer dans le résultat : _____

Les observations et la décision

Cas représentatifs examinés : _____

Informations sensibles restantes : _____

Altérations de sens ou erreurs de restitution : _____

Décision, conditions d'usage et date : _____

Un usage est documenté lorsque le professionnel peut expliquer ce qu'il attend du traitement, quelles informations il y engage, quelles protections il retient et sur quoi repose sa décision d'utiliser le résultat.

Conclusions et perspectives

Le choix d'une protection part du besoin juridique et des informations nécessaires. L'abstraction, la minimisation, l'anonymisation, la pseudonymisation et la restriction des accès répondent à des objectifs différents et peuvent se combiner. Leur pertinence se juge sur le parcours réel, la confidentialité du contenu et la fidélité du résultat, sans présumer qu'une mesure convient à tous les dossiers.

Évaluer un parcours plutôt qu'un texte isolé

La demande, les pièces, les services de préparation, les traitements successifs et la restitution forment un ensemble. Les mêmes informations peuvent changer de forme et de destinataire à plusieurs reprises. Cette continuité doit figurer dans la cartographie et dans les essais.

Mesurer la protection avec la fidélité juridique

La conservation des qualités, des faits et des relations est un critère de qualité aussi nécessaire que le traitement des identifiants. Une évaluation doit rendre visibles les erreurs de protection et les altérations du sens, puis examiner la restitution sur les supports réellement utilisés.

Documenter des décisions transférables

Une description claire de la tâche, du périmètre et des critères permet de discuter les choix entre professionnels. Les grilles proposées ont vocation à être adaptées, confrontées à de nouveaux cas et enrichies par l'expérience ; elles ne constituent pas un référentiel de certification. Elles peuvent servir de langage commun aux cabinets, aux responsables de la protection des données et aux concepteurs de services.

Axes de travail

Les évaluations gagneraient à couvrir davantage de dossiers multi-documents, de reprises de contexte et de formats de restitution. Une comparaison utile rendrait publics les cas, les critères et la nature des erreurs, tout en protégeant les informations des dossiers. Elle distinguerait les propriétés d'un composant de celles du parcours complet.

À propos de cette publication

Ce livre blanc est publié par AIDocs Studio, éditeur de Max. Il propose un cadre de réflexion et des outils méthodologiques applicables à tout service d'IA juridique. Les analyses sont celles de l'éditeur ; les institutions citées constituent les sources de référence. État de la recherche documentaire au 16 octobre 2026.

Références juridiques et professionnelles

[1] Californie • Senate Bill 574

Chapitre 858 des lois de 2026. Texte promulgué, notamment sections 1 et 3. Reproduction LegiScan.

Source : legiscan.com

[2] Conseil national des barreaux • 2026

La déontologie et l'intelligence artificielle. Guide pratique, première édition, avril 2026, notamment pages 15 à 18.

Source : cnb.avocat.fr

[3] Gouverneur de Californie • 30 septembre 2026

Communiqué institutionnel mentionnant SB 574 parmi les lois signées.

Source : www.gov.ca.gov

[4] France • Loi n° 71-1130 du 31 décembre 1971

Article 66-5, relatif au secret professionnel de l'avocat.

Source : www.legifrance.gouv.fr

[5] Conseil national des barreaux • RIN

Titre premier, article 2 : principes et étendue du secret professionnel.

Source : cnb.avocat.fr

Références sur la protection des informations

[6] Constitution de Californie

Article IV, section 8. Calendrier ordinaire d'entrée en vigueur. La date attendue pour SB 574 est déduite de ce calendrier. Reproduction institutionnelle des juridictions californiennes.

Source : courts.ca.gov

[7] CNIL • 19 mai 2020

L'anonymisation de données personnelles. Définition et risques de réidentification.

Source : www.cnil.fr

[8] CNIL • 13 janvier 2022

Recherche scientifique hors santé : enjeux et avantages de l'anonymisation et de la pseudonymisation. Référence pour la distinction des notions.

Source : www.cnil.fr

[9] Union européenne • Règlement (UE) 2016/679

RGPD, notamment article 4 paragraphe 5 ; articles 5, 25, 28 et 32 ; chapitre V pour les transferts concernés.

Source : eur-lex.europa.eu

[10] Garfinkel S L • NIST • 2015

De-Identification of Personal Information. NISTIR 8053. Synthèse de recherche sur la dé-identification, son utilité et les risques de réidentification. DOI : 10.6028/NIST.IR.8053.

Source : csrc.nist.gov