

# LA DÉONTOLOGIE ET L'INTELLIGENCE ARTIFICIELLE

## GUIDE PRATIQUE



# SOMMAIRE

GLOSSAIRE.....	5
INTRODUCTION .....	10
PROTECTION DU SECRET PROFESSIONNEL ET DES DONNÉES PERSONNELLES.....	14
<b>PROTECTION DU SECRET PROFESSIONNEL</b> (loi du 31 déc. 1971, art. 66-5 ; RIN, art. 2).....	15
Principe fondamental.....	15
Données concernées.....	15
Recommandations pratiques.....	15
Pseudonymisation ou anonymisation des données.....	16
Synthèse des bonnes pratiques.....	18
<b>PROTECTION DES DONNÉES PERSONNELLES (RGPD et RIN, art. 2).....</b>	19
Principes généraux et RGPD.....	19
Principes fondamentaux du RGPD.....	19
Recommandations pratiques.....	20
Risques pour la protection des données personnelles.....	20
Vigilance et limites.....	20
Synthèse des bonnes pratiques.....	20
<b>RESPECT DES PRINCIPES ESSENTIELS (RIN, ART. 1.3).....</b>	24
<b>LA COMPÉTENCE.....</b>	24
Se former.....	25
Comparer les outils proposés par les éditeurs.....	25
<b>LA DILIGENCE ET LA PRUDENCE.....</b>	28
La diligence et la prudence.....	28
La prévention du conflit d'intérêts (code de déontologie, art. 7 ; RIN, art. 4).....	30
<b>LA CONSCIENCE ET L'INDÉPENDANCE.....</b>	30

INFORMATION SUR L'USAGE DE L'IA .....	34
L'INFORMATION DES CLIENTS .....	34
L'information des clients sur l'usage de l'IA par l'avocat .....	34
L'information des clients sur leur usage de l'IA .....	35
L'INFORMATION AU SEIN DU CABINET .....	36
L'INFORMATION DES MAGISTRATS .....	36
SYNTHÈSE DES BONNES PRATIQUES .....	36
HONORAIRES (LOI DU 31 DÉC. 1971, ART. 10 ET RIN, ART. 11) .....	40
CONCLUSION .....	44
ANNEXE .....	48
Liste des bonnes pratiques déontologiques adoptées par le Conseil consultatif conjoint (CCC) .....	48

Cliquez sur cette icône pour **revenir directement au sommaire**  
et **naviguer facilement** à travers le guide



# GLOSSAIRE

**Intelligence artificielle (IA)** : système informatique capable d'exécuter des tâches en simulant certaines fonctions cognitives humaines (apprentissage, raisonnement, créativité, etc.).

**Intelligence artificielle générative (IAG)** : forme d'IA produisant de nouveaux contenus (textes, images, sons, codes) à partir de données d'apprentissage.

**LLM** : un grand modèle linguistique (*Large Language Model*, LLM) est un type de programme d'intelligence artificielle (IA) capable, entre autres tâches, de reconnaître et de générer du texte.

Les LLM sont entraînés sur de vastes ensembles de données. Ils s'appuient, entre autres, sur l'apprentissage automatique (*Machine Learning*, ML).

**Fine-tuning** : le *fine-tuning* est une technique utilisée en intelligence artificielle pour spécialiser un modèle pré-entraîné sur une tâche spécifique, en ajustant certains paramètres d'un modèle de *Machine Learning* pré-entraîné, tels que la traduction de langage, l'analyse de sentiments ou les chatbots intelligents. Contrairement à l'entraînement initial qui nécessite des jeux de données massifs, le *fine-tuning* se concentre sur des données plus restreintes et spécialisées.

**RAG** : la génération augmentée par récupération (*Retrieval-Augmented Generation*, RAG) est le processus consistant à optimiser les résultats d'un grand modèle de langage. Elle fait appel à une base de connaissances fiable, externe aux sources de données utilisées pour l'entraîner, avant de générer une réponse.

La RAG étend ainsi les capacités déjà puissantes des LLM à des domaines spécifiques ou à la base de connaissances interne d'une organisation, le tout sans qu'il soit nécessaire de réentraîner le modèle. Il s'agit d'une approche économique pour améliorer les résultats du LLM et faire en sorte que ceux-ci restent cohérents, précis et utiles dans de nombreux contextes.

**Pseudonymisation** : la pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.).

**Anonymisation** : l'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible. L'anonymisation ne doit pas être confondue avec la pseudonymisation.

**Randomisation** : la randomisation consiste à modifier les attributs dans un jeu de données de telle sorte qu'ils soient moins précis, tout en conservant la répartition globale. Cette technique permet de protéger le jeu de données du risque d'inférence.

Exemple : il est possible de permuter les données relatives à la date de naissance des individus de manière à altérer la véracité des informations contenues dans une base de données.

**Généralisation** : la généralisation consiste à modifier l'échelle des attributs des jeux de données, ou leur ordre de grandeur, afin de s'assurer qu'ils soient communs à un ensemble de personnes. Cette technique permet d'éviter l'individualisation d'un jeu de données. Elle limite également les possibles corrélations du jeu de données avec d'autres.

Exemple : dans un fichier contenant la date de naissance des personnes, il est possible de remplacer cette information par la seule année de naissance.

**LegalBench** : banc d'essai composé de différentes tâches de raisonnement juridique. Chaque tâche possède un jeu de données associé, constitué de paires entrée-sortie.

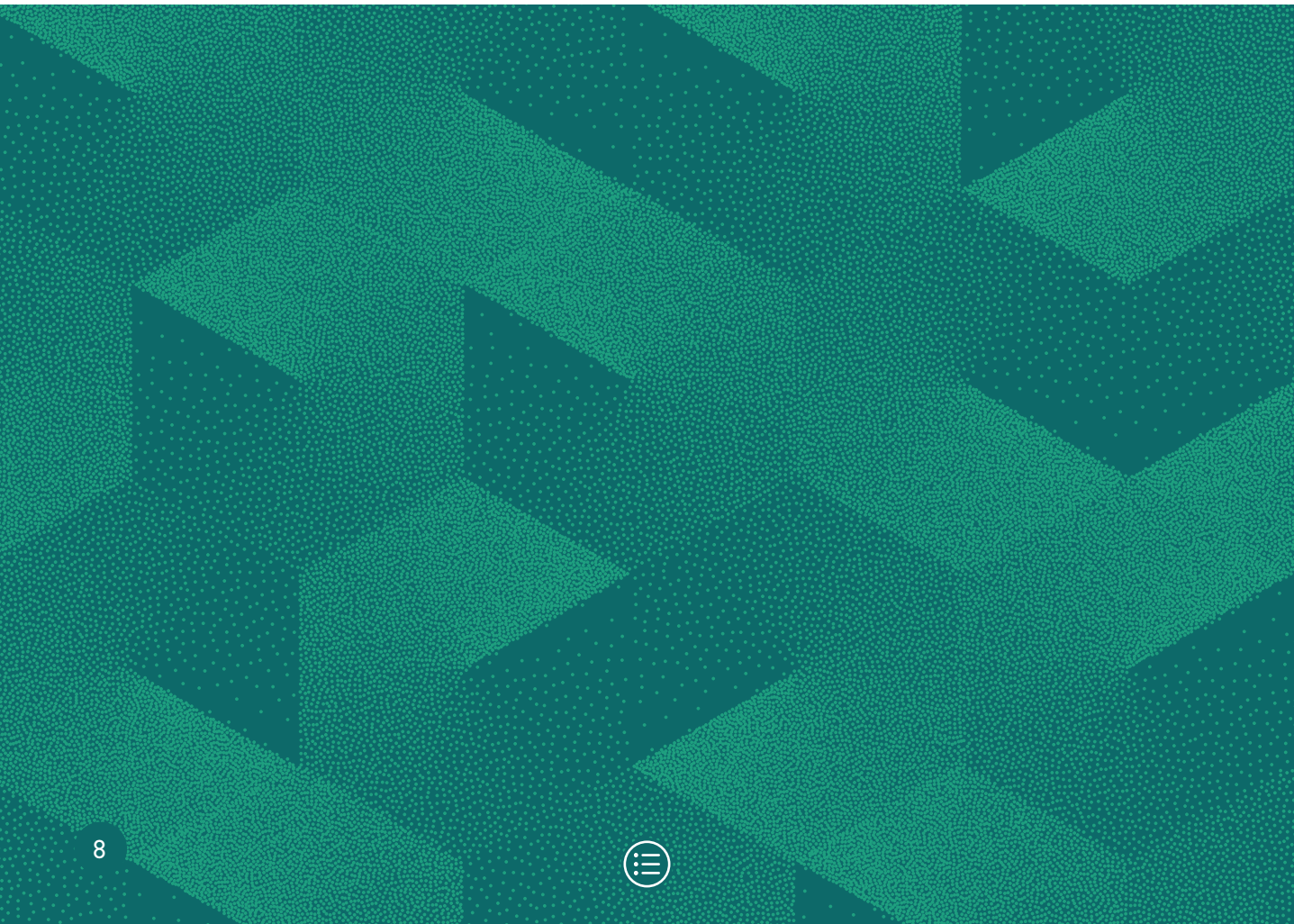
**Biais algorithmique** : distorsion ou discrimination induite par les données ou les algorithmes sur lesquels se basent les outils d'IA pour fonctionner.

**Hallucination** : production par une IA d'une information fautive ou trompeuse, due par exemple à des données d'apprentissage insuffisantes, des hypothèses erronées ou des biais, mais présentée comme crédible.

**Prompt** : instruction ou question donnée à un outil d'IA générative pour produire une réponse.

**Souveraineté numérique** : capacité à assurer le contrôle et la sécurité des données dans un cadre national ou européen.





# INTRODUCTION



# INTRODUCTION



**Bruno BLANQUER**

L'intelligence artificielle générative (IAG) s'impose aujourd'hui comme un outil incontournable dans le secteur juridique, offrant aux professionnels du droit des perspectives inédites en matière d'efficacité, de productivité et de collaboration. Les systèmes d'IA permettent d'automatiser et d'accélérer de nombreuses tâches : correction et amélioration de textes, synthèse de documents, rédaction de courriels ou de conclusions, assistance à la gestion des échanges et à la réflexion stratégique. Ils facilitent également la traduction, la vulgarisation et la préparation de supports de communication, contribuant ainsi à une meilleure adaptation des services aux besoins des clients et des équipes.

Cependant, l'intégration de l'IA dans la pratique professionnelle soulève des enjeux majeurs en matière de déontologie. Les risques identifiés sont multiples : l'IA peut générer des contenus erronés ou trompeurs (« hallucinations »), reproduire et amplifier des biais présents dans les données d'entraînement, ou encore compromettre la confidentialité des informations traitées. La transmission de données sensibles à des outils d'IA expose l'avocat à des risques de violation du secret professionnel et de la réglementation relative à la protection des données personnelles (RGPD), ainsi qu'à des incertitudes sur la propriété intellectuelle des contenus générés.

Dans ce contexte, les règles déontologiques et réglementaires fondamentales s'imposent :

- **La protection du secret professionnel**, qui interdit toute divulgation d'informations confidentielles relatives aux dossiers ou aux clients, y compris lors de l'utilisation d'outils d'intelligence artificielle.
- **La protection des données personnelles**, qui impose le respect de la réglementation relative à la protection des données personnelles (RGPD) et des principes de sécurité, de confidentialité et de minimisation des données lors de tout traitement impliquant des personnes physiques.
- **La compétence**, qui exige de l'avocat une maîtrise suffisante des outils numériques et de leurs limites pour garantir la qualité du service rendu.
- **La diligence et la prudence**, qui imposent une vérification systématique des résultats produits par l'IA et une utilisation réfléchie de ces technologies.
- **La conscience et l'indépendance**, qui requièrent que l'avocat conserve son libre arbitre, son esprit critique et son autonomie dans l'analyse et la prise de décision, sans se laisser influencer par les suggestions de l'IA.
- **La gestion des conflits d'intérêts**, qui suppose une vigilance accrue dans l'utilisation de l'IA.
- **L'information des clients, des magistrats et des collaborateurs au sein du cabinet.**
- **La fixation des honoraires**, qui doivent rester justes, prévisibles et proportionnés au service rendu, même lorsque l'IA intervient dans le processus de travail, afin de préserver la confiance du client et le respect des règles professionnelles.

Face à ces défis, il est essentiel d'adopter une approche responsable et encadrée de l'IA : privilégier la pseudonymisation et l'anonymisation des données, vérifier systématiquement les résultats produits, respecter les principes de sécurité et de confidentialité, et former l'ensemble des membres du cabinet aux bonnes pratiques et aux limites de ces technologies. L'utilisation de l'IA doit ainsi s'inscrire dans le respect des règles déontologiques, afin de garantir la protection des intérêts des clients, la fiabilité des prestations et la conformité aux exigences légales.

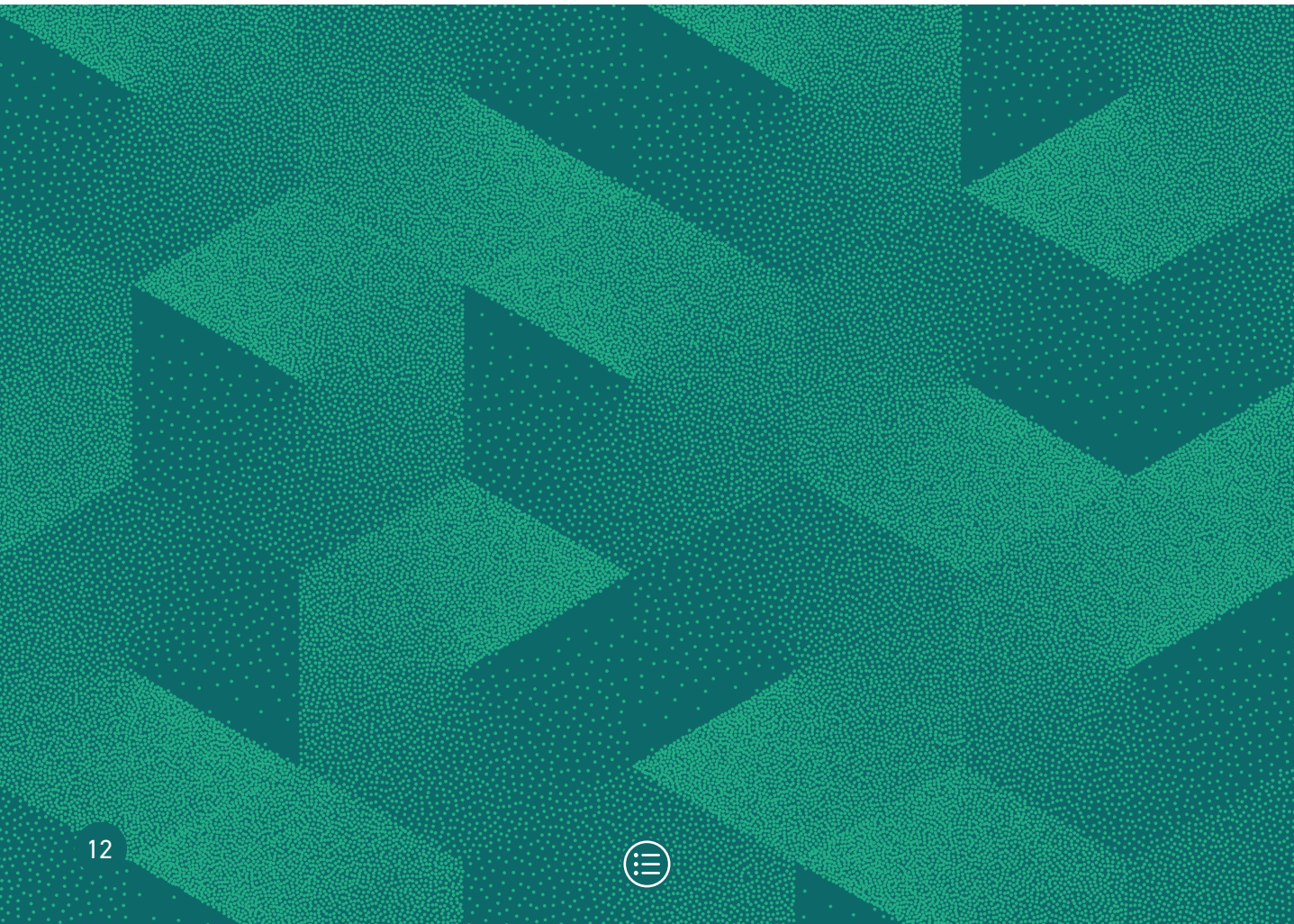
Ce document, élaboré par la commission des règles et usages du Conseil national des barreaux que je remercie vivement, propose un cadre déontologique complet pour accompagner les avocats dans l'usage des outils d'intelligence artificielle générative.

Conçu comme un guide opérationnel, il présente les risques, les bonnes pratiques, des recommandations concrètes ainsi que des exemples jurisprudentiels récents.

Cet outil a pour objectif d'aider chaque avocat à intégrer l'IA dans sa pratique de manière responsable, sécurisée et conforme aux principes essentiels de la profession.

**Bruno BLANQUER**

Président de la commission des règles et usages  
du Conseil national des barreaux (mandat 2024-2026)



# PROTECTION DU SECRET PROFESSIONNEL ET DES DONNÉES PERSONNELLES

PROTECTION DU SECRET PROFESSIONNEL (loi du 31 déc. 1971, art. 66-5 ; RIN, art. 2) .....	15
PROTECTION DES DONNÉES PERSONNELLES (RGPD et RIN, art. 2) .....	19



# PROTECTION DU SECRET PROFESSIONNEL ET DES DONNÉES PERSONNELLES

Dans un système d'IAG, le robot conversationnel est l'interface vers le LLM, modèle de fondation hébergé dans un cloud. Les utilisateurs y accèdent via internet.

Toute requête envoyée à une IAG entraîne alors la transmission de données à l'entreprise qui exploite le système d'IAG, laquelle, dans la majorité des cas, est américaine. En effet, les marchés mondiaux de l'IAG et du cloud sont dominés par des entreprises américaines.

Cette transmission s'accompagne de la conservation et du traitement de ces données par l'entreprise, les données transmises étant parfois utilisées pour l'amélioration des modèles. Ce qui caractérise ces modèles est l'opacité du traitement des données.

Les avocats sont soumis à des obligations strictes en matière de confidentialité et de protection des données, en vertu des règles déontologiques de la profession et de la réglementation nationale et européenne, telle que le règlement général sur la protection des données (RGPD).

Cette transmission d'informations à un tiers soulève deux difficultés :

- la première est relative à la confidentialité des données transmises, ce qui met en jeu le secret professionnel de l'avocat,
- la seconde est relative à la protection des données personnelles (RGPD).



## RECOMMANDATION

Lorsque vous formulez une requête, il est important d'avoir en tête que les données transmises à l'IAG sont susceptibles d'être utilisées par le propriétaire du modèle d'IAG afin de lui permettre d'améliorer et de développer les performances de son modèle.

Toutefois, il convient de noter que certains outils, dans leurs conditions générales d'utilisation, offrent la possibilité à l'utilisateur de refuser cette « réutilisation ».

Il est recommandé de privilégier ces IAG.

Néanmoins, en l'absence de garantie offerte par les entreprises qui offrent cette possibilité (ex. : aucun moyen de vérification n'est offert aux utilisateurs), il convient de rester vigilant, le risque de violation du secret professionnel ou de non-conformité au RGPD n'étant pas écarté pour autant.

# PROTECTION DU SECRET PROFESSIONNEL

## (loi du 31 déc. 1971, art. 66-5 ; RIN, art. 2)

Le secret professionnel, encadré par l'article 66-5 de la loi du 31 décembre 1971 et rappelé à l'article 2 du Règlement intérieur national (RIN), n'appartient pas à l'avocat ; il en est le garant et le gardien en tant que confident nécessaire.

### Principe fondamental

Il est impératif pour l'avocat de veiller à ne jamais communiquer des données relatives à ses dossiers ou à ses clients à des intelligences artificielles génératives (IAG).

### Données concernées

Ces données comprennent, entre autres, les noms, adresses, numéros de téléphone, informations financières et/ou stratégiques sur les clients et les membres du cabinet (associés, collaborateurs, assistants, etc.), ainsi que tout détail spécifique d'un dossier qui pourrait permettre d'identifier une personne ou une entreprise.

Transmettre ces informations à une IAG expose à des risques de violation de la sécurité des données, mais également du secret professionnel, et peut exposer l'avocat à des sanctions disciplinaires et/ou juridiques.

### Recommandations pratiques

Afin de respecter son secret professionnel, un avocat ne peut pas renseigner dans sa requête :

- le nom de son ou ses clients qu'ils soient une personne physique (cf. RGPD infra), une personne morale ou toute autre entité (il faut supprimer tout risque de réidentification),
- toute information confidentielle confiée par le client à l'avocat (ex. : un secret de fabrication, une idée brevetable, etc.),
- les éléments de stratégie du dossier,
- joindre à sa requête tout fichier comportant tout ou partie d'un dossier et contenant le nom du client ou des informations confidentielles communiquées par lui, ou des éléments stratégiques propres au dossier,
- toute information couverte par le secret professionnel.



## RECOMMANDATION

Il est essentiel de parvenir à un équilibre entre la nécessaire mise en contexte et le respect du secret professionnel.

Nous vous recommandons d'être vigilants dans la formulation de vos requêtes, dans leur mise en contexte, et de limiter les informations partagées avec l'outil aux seules données strictement nécessaires pour accomplir la tâche.

### Comment utiliser l'IAG dans le respect du secret professionnel ?

En pratique, comment demander à l'IAG de faire une synthèse, de rédiger une partie des conclusions ou d'une consultation, ou de vérifier l'orthographe et la grammaire d'un texte ?

La solution réside dans la pseudonymisation ou l'anonymisation des données.

## Pseudonymisation ou anonymisation des données

Afin d'utiliser des outils d'intelligence artificielle générative tout en protégeant ses données, il est conseillé à l'avocat de mettre en œuvre une bonne pratique : la pseudonymisation ou l'anonymisation des données.

### La pseudonymisation des données

#### Définition :

La pseudonymisation est un traitement de données personnelles qui consiste à « *remplacer les données directement identifiantes (noms, prénoms, etc.) d'un jeu de données par des données indirectement identifiantes* »<sup>1</sup>. Cette pratique, qui ne présente pas de caractère irréversible (contrairement à l'anonymisation), permet ainsi d'utiliser les données sans permettre d'identification.

#### Comment pseudonymiser les données ?

En pratique, pour pseudonymiser les données, il convient de retirer ou de remplacer toutes les informations personnelles identifiables par des pseudonymes ou des données génériques. Par exemple, remplacer les noms des clients par des initiales fictives (type X ou Y) ou une suite complexe de caractères, ou encore modifier les adresses en les remplaçant par des zones géographiques plus larges (comme une ville ou une région au lieu d'une rue précise) permet de garantir que les informations transmises ne puissent pas remonter jusqu'à une personne ou une entité spécifique.

1. Voir en ce sens : CNIL, « [L'anonymisation de données personnelles](#) »





## ATTENTION

À ce jour, la pseudonymisation ne s'applique pas à toutes les tâches qu'une IAG pourrait effectuer.

À titre d'exemple, la pseudonymisation ne peut pas s'appliquer à la réalisation, en direct, d'un compte-rendu d'un rendez-vous avec un client. Si des informations confidentielles sont échangées au cours de ce rendez-vous, vous transmettez ces informations confidentielles à l'IAG qui établira un compte-rendu.

Il convient donc de faire un usage approprié de l'IAG en fonction de vos besoins.

**À noter** : il existe des outils d'IA développés par des cabinets qui permettent d'effectuer toutes les tâches dans le respect du secret professionnel : il s'agit de systèmes d'IA fermés.

## L'anonymisation des données

### Définition :

L'anonymisation est définie par la CNIL comme « *un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible* »<sup>2</sup>.

Autrement dit, il s'agit de transformer les données de manière irréversible pour qu'aucune personne ou entité ne puisse plus être identifiée ou réidentifiée, que ce soit directement ou indirectement.

### Comment anonymiser tout en préservant au maximum l'utilité du jeu de données ?

Puisque le processus d'anonymisation vise à éliminer toute possibilité de réidentification, l'exploitation future des données est ainsi limitée à certains types d'utilisation. Ces contraintes sont à prendre en compte dès le début du projet.

Pour construire un processus d'anonymisation pertinent, il est ainsi conseillé :

- d'identifier les informations à conserver selon leur pertinence ;
- de supprimer les éléments d'identification directe ainsi que les valeurs rares qui pourraient permettre une réidentification aisée des personnes (par exemple, la présence de l'âge des individus peut permettre de réidentifier très facilement les personnes centenaires) ;
- de distinguer les informations importantes des informations secondaires ou inutiles (c'est-à-dire supprimables) ;
- de définir la finesse idéale et acceptable pour chaque information conservée.

Ce prérequis permet de déterminer le procédé d'anonymisation à appliquer, c'est-à-dire l'enchaînement des techniques d'anonymisation à mettre en place. Celles-ci peuvent être regroupées en deux familles : la randomisation et la généralisation.

- La randomisation consiste à modifier les attributs dans un jeu de données de telle sorte qu'ils soient moins précis, tout en conservant la répartition globale. Cette technique permet de protéger le jeu de données du risque d'inférence.

*Exemple : il est possible de permuter les données relatives à la date de naissance des individus de manière à altérer la véracité des informations contenues dans une base de données.*

- La généralisation consiste à modifier l'échelle des attributs des jeux de données ou leur ordre de grandeur, afin de s'assurer qu'ils soient communs à un ensemble de personnes. Cette technique permet d'éviter l'individualisation d'un jeu de données. Elle limite également les possibles corrélations du jeu de données avec d'autres.

*Exemple : dans un fichier contenant la date de naissance des personnes, il est possible de remplacer cette information par la seule année de naissance.*



## POUR EN SAVOIR PLUS SUR LA PSEUDONYMISATION ET L'ANONYMISATION

« [Recherche scientifique \(hors santé\) : enjeux et avantages de l'anonymisation et de la pseudonymisation](#) », CNIL, 13 janvier 2022

Jean Mindaa, « [Anonymisation et pseudonymisation : deux méthodes, une grande différence dans le cadre du RGPD!](#) », *Le Village de la Justice*, 12 mai 2025

## Synthèse des bonnes pratiques

- Utiliser avec la plus grande prudence les IAG gratuites qui ne garantissent pas la protection du secret professionnel.
- Ne jamais transmettre d'informations couvertes par le secret professionnel à une IAG.
- Pseudonymiser ou anonymiser systématiquement les données avant toute utilisation d'un outil d'IA générative.
- Limiter la mise en contexte à ce qui est strictement nécessaire pour accomplir la tâche.
- Être attentif au risque d'identification indirecte par croisement de données.

# PROTECTION DES DONNÉES PERSONNELLES

## (RGPD et RIN, art. 2)

L'avocat doit veiller au respect du règlement général sur la protection des données (RGPD) lors de tout traitement de données personnelles. Cela implique la minimisation des données transmises, la sécurisation des échanges et la garantie des droits des personnes concernées. L'utilisation de l'IA doit s'accompagner de mesures techniques et organisationnelles pour éviter toute fuite ou utilisation abusive des données.

### Principes généraux et RGPD

L'utilisation de l'intelligence artificielle générative doit être conforme au RGPD, qui impose des obligations strictes en matière de traitement des données personnelles.

Le 25 mai 2018 est entré en application le RGPD, texte renforçant les droits existants en matière de protection des données à caractère personnel pour les personnes physiques afin de garantir que le traitement de leurs données ne génère pas de risques pour les droits et libertés de ces personnes.

Le RGPD s'applique à tous les cabinets d'avocats, quelle que soit leur taille, leur structure et leur domaine d'activité, et il ne concerne que les données des personnes physiques, notamment les données considérées comme sensibles. Il s'applique, entre autres, pour les personnes dont les données sont traitées par les cabinets d'avocats établis en France ou dans un autre État membre de l'Union européenne, et ce, quelle que soit la nationalité des personnes concernées et que le traitement ait lieu ou non au sein de l'Union européenne.

Les données à caractère personnel traitées par les avocats sont principalement celles de leurs clients, mais les traitements peuvent aussi concerner les collaborateurs libéraux, les collaborateurs salariés, les salariés du cabinet, les fournisseurs et prestataires du cabinet.

### Principes fondamentaux du RGPD

Le traitement de ces données, via des outils d'intelligence artificielle générative, doit respecter les principes fondamentaux du RGPD :

- Finalité du traitement ;
- Pseudonymisation, minimisation ;
- Conservation limitée ;
- Sécurité et confidentialité ;
- Droit des personnes physiques concernées.

## Recommandations pratiques

Pour la mise en œuvre de la réglementation sur la protection des données dans la formulation de vos requêtes, nous vous invitons à vous reporter à nos recommandations faites en matière de secret professionnel.

## Risques pour la protection des données personnelles

Pour fonctionner efficacement, l'IAG nécessite des quantités massives de données personnelles. Cette collecte peut entraîner des risques pour la vie privée des personnes concernées si les données ne sont pas correctement utilisées et pseudonymisées ou anonymisées (cf. point sur la pseudonymisation et l'anonymisation). De plus, des risques pour les données personnelles peuvent également apparaître si l'IAG est la cible de cyberattaques ou en cas de biais présents dans les données d'entraînement.

## Vigilance et limites

Il convient de rester vigilant quant à l'identification rendue possible par le croisement de plusieurs données, quand bien même ces données auraient déjà été pseudonymisées ou anonymisées (exemples : montants, noms de projets donnés en interne, façon de rédiger un contrat, qui peuvent être caractéristiques de l'identification d'un client). Cette pratique permet ainsi à l'avocat d'utiliser les capacités et bénéfices des outils d'intelligence artificielle générative, tout en protégeant la confidentialité des clients.

## Synthèse des bonnes pratiques

- Utiliser avec la plus grande prudence les IAG gratuites qui ne protègent pas les données personnelles.
- Respecter le RGPD pour tout traitement de données personnelles via l'IA.
- Pseudonymiser ou anonymiser les données avant toute utilisation d'un outil d'IA générative.
- Rester vigilant face aux risques de réidentification, de cyberattaque et de biais.
- Respecter les principes de finalité, minimisation, de conservation limitée, de sécurité et de confidentialité.



### RECOMMANDATION

Un cabinet utilise une IA pour analyser des contrats. Avant d'intégrer les documents dans l'outil, il pseudonymise ou anonymise les parties (noms, adresses, numéros de téléphone) et s'assure que l'outil respecte les standards du RGPD, notamment en matière de conservation et de suppression des données.





# RESPECT DES PRINCIPES ESSENTIELS (RIN, ART. 1.3)

LA COMPÉTENCE .....	24
LA DILIGENCE ET LA PRUDENCE .....	28
LA CONSCIENCE ET L'INDÉPENDANCE .....	30

# RESPECT DES PRINCIPES ESSENTIELS (RIN, ART. 1.3)

Comme dans l'ensemble de son activité professionnelle, l'avocat doit respecter les principes essentiels listés dans l'article 1.3 du RIN lorsqu'il utilise une IAG.

Parmi ces principes, l'accent doit être mis sur le fait que l'avocat doit faire preuve de **compétence**, de **diligence** et de **prudence** envers ses clients.

L'avocat doit aussi exercer ses fonctions avec **conscience** et **indépendance**.

La formation prend une place essentielle pour maîtriser les outils d'IA.

## LA COMPÉTENCE

La compétence impose à l'avocat de maîtriser les outils numériques qu'il utilise, de comprendre leurs limites et de s'assurer de la qualité du service rendu. L'avocat doit se former régulièrement aux évolutions technologiques et être capable d'évaluer la pertinence des résultats produits par l'IAG.

Tout avocat a le devoir de n'accepter que des missions qu'il peut exécuter avec compétence. Par conséquent, il s'interdit d'utiliser l'IAG pour prodiguer des conseils sur des sujets juridiques pour lesquels il n'a pas de connaissances ou d'expertise suffisantes et se conforme à toute autre règle déontologique applicable (Union internationale des avocats).

Les avocats doivent donc toujours procéder à une analyse critique et superviser les résultats produits par l'IA, et ne jamais utiliser directement les résultats ou s'y fier sans les avoir d'abord examinés et vérifiés (UIA).



### RECOMMANDATION

Avant d'utiliser une IA pour générer des conclusions, l'avocat suit une formation sur le fonctionnement des modèles de langage et apprend à détecter les erreurs ou les biais dans les réponses générées, afin de garantir la qualité et la fiabilité du travail fourni au client.

Il est primordial de se former à interroger l'IA.

## Se former

Le CNB s'est associé à Lefebvre Dalloz Compétences pour proposer une plateforme d'e-learning dédiée aux avocats : SKILIA.

Ce programme gratuit, destiné à toute la profession, propose 12 modules permettant de mettre à jour ses connaissances en toute flexibilité et en autonomie.

Pour accéder à la plateforme : [SKILIA | Lefebvre Dalloz Compétences](#)

## Comparer les outils proposés par les éditeurs

Il est préconisé d'avoir recours à des IA juridiques spécifiquement proposées par les legaltechs et les grands éditeurs juridiques, dont les bases de données sont plus fiables.

Le CNB a ainsi mis à la disposition de la profession une grille d'auto-évaluation permettant de guider les avocats dans le choix des logiciels juridiques augmentés par une ou plusieurs couches d'intelligence artificielle générative, selon les fonctionnalités qu'ils proposent et au regard des règles professionnelles et déontologiques.

À consulter : [la grille d'auto-évaluation](#) (1<sup>re</sup> édition, juin 2025).

Les critères à prendre en considération pour choisir un outil d'IA juridique sont les suivants :

### Les fonctionnalités

On peut classer globalement les outils d'intelligence artificielle générative en deux grandes familles :

- les éditeurs juridiques traditionnels et les legaltechs, les systèmes de recherche documentaire, de recherche avancée ou « augmentée », etc.,
- les outils à installer sur le propre contenu du cabinet, les systèmes d'IA de productivité, les « super assistants », etc.

Ensuite, l'outil devra être choisi pour répondre aux besoins spécifiques de l'avocat : recherche jurisprudentielle, analyse de contrats, rédaction assistée, etc.

Dans le prolongement, il convient d'identifier les fonctionnalités qui vont à terme être proposées de manière native par tous les outils, ou presque, telles que les résumés des décisions de justice, leur traduction en français ou dans une autre langue, ou encore la génération de mémos juridiques.

Enfin, l'un des critères de choix de l'outil sera sa délimitation ou sa spécialisation aux domaines d'intervention de l'avocat (droit pénal, droit des affaires, droit international, etc.).

## La souveraineté des données

Les éléments à prendre en compte sont, par ordre de priorité :

- le lieu d'hébergement des données des clients (France, voire Union européenne),
- la nationalité de l'entreprise détenant les serveurs hébergeant les données des clients (française, voire européenne [au sens du droit communautaire], et excluant toute entreprise soumise à des dispositions extraterritoriales permettant aux autorités de l'État correspondant d'accéder aux données stockées sur des serveurs appartenant aux entreprises de sa nationalité, comme les entreprises américaines en l'état actuel de leur législation),
- le lieu d'hébergement des données du grand modèle de langage (LLM) utilisé (France, voire Union européenne),
- la nationalité de l'entreprise détenant les serveurs hébergeant les données du LLM (mêmes caractéristiques que celles exposées précédemment).

Un prérequis est que l'outil d'IA choisi ne réutilise pas des données à des fins d'entraînement du ou des grands modèles de langage utilisés et ne transmette aucune donnée à ce ou ces LLM.

Sans surprise, l'ensemble des outils audités affirment tous appliquer ce principe au sein de leur solution.

Néanmoins, même si un modèle propriétaire indique que les données téléchargées ne seront pas réutilisées, cette assertion n'est en général ni prouvable ni vérifiable. Un doute peut donc subsister sur la question.

Il n'est ainsi ni suffisant ni pertinent de ne s'en tenir qu'aux conditions générales d'utilisation des sociétés éditant les outils d'IA.

Les seules manières d'éliminer les risques liés à la souveraineté, en plus des éléments mentionnés précédemment, et de garantir l'étanchéité et la confidentialité pour les données du cabinet « injectées » dans l'outil d'IA sont :

- l'anonymisation ou la pseudonymisation préalable des données,
- l'installation du LLM sur les propres systèmes d'information du cabinet (par exemple à partir d'un modèle open source comme Llama ou Mistral AI).

Les outils qui devraient ainsi être privilégiés en priorité sont ceux qui intègrent dans leurs processus et fonctionnalités l'ensemble des mesures exposées dans cette section.

## La confidentialité et la sécurisation des données

Les éléments à prendre en considération sont :

- le chiffrement des données des clients, aussi bien en transit (protocoles HTTPS et TLS) qu'au repos (avec un algorithme de chiffrement suffisant, tel que l'AES-256), avec une détention et une gestion par le cabinet de la clé de chiffrement,
- l'anonymisation ou la pseudonymisation des données des clients,
- la non-réutilisation des données des clients pour entraîner un LLM propriétaire (cf. supra) et le cloisonnement nécessaire pour arriver à cette fin avec l'ajout d'une RAG sécurisée<sup>1</sup>,

1. RAG sécurisée : cf. définition dans le glossaire, p. 6.





## RECOMMANDATION

Il peut être conseillé aux avocats de comparer les offres des éditeurs d'outils d'IA juridiques sur ce point, ce qui est pour eux une obligation au sens de l'article 28.1 du RGPD (qui prévoit le recours uniquement à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées).

- la suppression, l'anonymisation ou la pseudonymisation automatique, voire au bout d'un temps court défini, des prompts formulés après réponse de l'outil d'IA,
- les certifications et labels de la société ainsi que son respect de certains codes de conduite orientés IA,
- l'impossibilité pour les salariés des fournisseurs d'outils d'IA d'accéder aux données des avocats, ou, à défaut, la mise en place d'habilitations strictes d'accès,
- la journalisation, comprenant celle des personnes éventuellement habilitées à accéder aux données (cf. point précédent),
- les tests de sécurité numérique effectués (très) régulièrement,
- les mesures de sécurité physique mises en place, notamment :
  - lorsque les LLM sont hébergés en local dans les sociétés,
  - chez les prestataires, et particulièrement les hébergeurs,
- toute autre mesure organisationnelle ou technique de sécurité mise en œuvre qui viendrait renforcer la sécurité de l'ensemble de la solution.

De manière globale, et même si cet aspect ne concerne pas uniquement la sécurité, le respect de la conformité au RGPD est un bon indicateur pour les avocats de la prétendue robustesse d'un outil et de sa résistance théorique aux attaques informatiques.

## La fiabilité

Les éléments à prendre en considération sont :

- la citation des sources de référence avec un lien permettant de les consulter en intégralité,
- les sources visées doivent être fiables,
- la présence d'un système de RAG, pour peu qu'il soit correctement conçu et sécurisé,
- l'adaptation du LLM au droit applicable (ex. : un LLM entraîné en droit du Common Law ne sera pas forcément adapté à une problématique relevant du droit continental),
- les certificats, labels et codes de conduite respectivement obtenus et suivis par les sociétés éditrices d'outils d'IA.



## RECOMMANDATION

Il est recommandé aux professionnels de tester les outils avant leur utilisation en conditions réelles et d'évaluer les performances spécifiques des modèles d'IA dans le domaine juridique, au moyen d'études comparatives reposant sur des jeux de données du type « LegalBench ».

## LA DILIGENCE ET LA PRUDENCE

### La diligence et la prudence

#### Vérification systématique des résultats produits par l'IAG

La diligence et la prudence exigent de l'avocat une vérification systématique des résultats produits par l'IA et une utilisation réfléchie de ces technologies. Il doit relire, contrôler et valider chaque contenu généré avant de l'utiliser ou de le transmettre à un client ou à une juridiction.

En effet, comme l'a rappelé l'ancienne présidente du CNB, Christiane Féral-Schuhl, lors de la Grande Rentrée des avocats du 18 octobre 2024, les logiciels intégrant l'IA sont des « **outils d'assistance et pas de substitution** » à l'exercice professionnel. Ils doivent seulement « assister » l'avocat. L'intelligence artificielle peut se tromper et donner de mauvaises informations.

L'avocat ayant recours à des contenus générés par l'intelligence artificielle sans vérification appropriée prend le risque de produire des éléments erronés, ce qui est de nature à engager sa responsabilité civile. Il est susceptible de faire l'objet de poursuites disciplinaires.

Le guide du CCBE sur l'utilisation de l'intelligence artificielle générative par les avocats<sup>2</sup> rappelle que, dans ce contexte, l'avocat doit également garder à l'esprit d'autres principes fondamentaux inclus dans la Charte des principes essentiels de l'avocat européen<sup>3</sup>, tels que la dignité et l'honneur de la profession d'avocat, la probité et la réputation de l'avocat, la loyauté à l'égard de son client ou le respect de l'État de droit et la contribution à une bonne administration de la justice.

Il existe plusieurs cas où le recours à l'IA sans vérification a été mis en exergue par les juridictions françaises. Parmi les plus récents, nous pouvons citer les décisions suivantes :

- **Tribunal judiciaire de Périgueux, 18 décembre 2025 (n° 23/00452) :** « À titre préliminaire, le tribunal relève que les références de jurisprudence citées par le requérant, mais non produites dans ses pièces, ne semblent pas correspondre à des décisions publiées. Le tribunal invitera donc le requérant et son conseil à vérifier à l'avenir que les références qu'ils ont pu trouver sur des moteurs de recherche ou à l'aide de l'intelligence artificielle ne sont pas des "hallucinations". »
- **Tribunal administratif d'Orléans, reconduite à la frontière, 29 décembre 2025 (n° 2506461) :** « Il y a lieu de faire remarquer au conseil de M. B... la nécessité de vérifier les décisions juridictionnelles citées, au demeurant non produites, avant de saisir le juge. En effet, les décisions "[...]" n'existent pas, soit qu'aucune décision juridictionnelle n'existe avec le numéro indiqué, soit que les numéros de ces affaires ne correspondent pas aux dates y accolées. Quant à la décision "CE, 30 décembre 2013, n° 367533", elle n'est pas relative à une question de fond relative à une assignation à résidence. Il y a donc lieu d'inviter le conseil du requérant à vérifier à l'avenir que les références trouvées par quelque moyen que ce soit ne constituent pas une "hallucination" ou une "confabulation". »

2. [Le guide du CCBE sur l'utilisation de l'intelligence artificielle générative par les avocats](#), octobre 2025.

3. [Charte des principes essentiels de l'avocat européen et code de déontologie des avocats européens](#)



- **Tribunal administratif de Rennes, 28 janvier 2026 (n° 2506364)** : « *Aucun des moyens invoqués n'est assorti des précisions nécessaires permettant au juge d'en apprécier le bien-fondé. Ainsi, la requête, qui, au demeurant, a manifestement été rédigée à l'aide d'un outil d'intelligence artificielle générative, doit être rejetée sur le fondement des dispositions précitées du 7° de l'article R. 222-1 du code de justice administrative.* »
- **CAA Bordeaux, juge des référés, 26 février 2026 (n° 25BX02906)** : « *Il y a lieu de faire remarquer au conseil de M. B... la nécessité de vérifier les décisions juridictionnelles citées, au demeurant non produites, avant de saisir le juge [...] "CE, 7 février 2018, n° 409302" et "CE, 11 janvier 2007, Association SOS Racisme" n'existent pas. Il y a donc lieu d'inviter le conseil du requérant à vérifier à l'avenir que les références trouvées par quelque moyen que ce soit ne constituent pas une "hallucination" ou une "confabulation".* »

#### Autres décisions de juridictions étrangères :

- **Décision de la cour suprême de la Colombie-Britannique du 26 février 2024** : une avocate en Colombie-Britannique a été condamnée à payer les frais de la partie adverse pour avoir cité deux affaires inexistantes générées par l'intelligence artificielle dans une requête déposée au tribunal.
- **Décision de la cour suprême de New York du 1<sup>er</sup> octobre 2025<sup>4</sup>** : la cour explique que le problème ne vient pas de l'utilisation de l'IA. Le problème survient lorsque les avocats renoncent à leur responsabilité de garantir l'exactitude de leurs déclarations factuelles et juridiques devant la cour, même si celles-ci proviennent de l'IA.
- **Décision de la cour d'appel de l'Utah du 29 mai 2025** : « *Dans le cas présent, les avocats du requérant ont manqué à leurs responsabilités de contrôle en tant que membres du barreau de l'État de l'Utah lorsqu'ils ont déposé une requête contenant un faux précédent généré par ChatGPT* ».
- **Décision du juge fédéral de Los Angeles de mai 2025** : ce juge avait infligé une amende de 31 000 dollars à deux cabinets d'avocats pour une requête qui contenait neuf erreurs de jurisprudence en dix pages, qualifiant l'opération de « *débâcle collective* ».



### RECOMMANDATION

Après avoir obtenu une synthèse d'un jugement via une IA, comparez le texte généré avec la décision officielle pour vous assurer qu'aucune erreur ou interprétation erronée n'a été introduite, évitant ainsi tout risque de mauvaise information.

## Respect des droits de propriété intellectuelle

L'avocat utilisateur d'une IAG doit respecter les règles en matière de propriété intellectuelle. Il s'assure notamment que les conditions générales d'utilisation de l'IAG ne permettent pas à son fournisseur de s'appropriier ou de réutiliser les éléments communiqués dans le cadre d'une cession de droits. En effet, sur nombre de ces éléments, l'avocat utilisateur ne détient pas lui-même ces droits (conclusions adverses, contrats, articles de doctrine non rédigés par l'avocat utilisateur, etc.).

4. Ader v. Ader, Supreme Court of New York, New York County, Decided October 1, 2025, Index No. 653917/2024.

## La prévention du conflit d'intérêts (code de déontologie, art. 7 ; RIN, art. 4)

L'article 7, alinéa 3, du décret n° 2023-552 du 30 juin 2023 portant code de déontologie des avocats dispose que l'avocat ne peut accepter l'affaire d'un nouveau client si le secret des informations données par un ancien client risque d'être violé ou si la connaissance, par l'avocat, des affaires de l'ancien client est susceptible de favoriser le nouveau client.

L'utilisation de l'IA doit être encadrée pour éviter toute situation de conflit d'intérêts. L'avocat doit s'assurer que les données transmises à l'outil ne risquent pas d'être réutilisées dans le cadre d'autres dossiers.

L'utilisation de l'IA générative peut créer des risques pour le respect des obligations en matière de conflits d'intérêts, étant donné que les systèmes d'intelligence artificielle peuvent être formés ou avoir accès à des informations confidentielles provenant de plusieurs cabinets d'avocats et de clients, ce qui peut entraîner un partage involontaire d'informations ou des conflits d'intérêts.

## LA CONSCIENCE ET L'INDÉPENDANCE



### RECOMMANDATION

Lorsqu'une IAG propose une stratégie de défense, l'avocat analyse la suggestion, la confronte à son expérience et à la jurisprudence, et ne retient la proposition que si elle est conforme à ses convictions et à l'intérêt du client.

L'IA, en reproduisant les biais du corpus sur lequel elle a été entraînée et en tendant à conforter les attentes de l'utilisateur, est susceptible de dégrader la qualité de la réponse donnée et de priver l'avocat de l'indépendance intellectuelle dont il ne doit jamais se départir.

Les avocats qui s'appuient sur de tels outils sans esprit critique risquent d'intérioriser ces biais, ce qui pourrait influencer leur conduite et nuire à leur devoir de fournir des conseils avisés.

Un autre risque qui se pose dans ce contexte est la dépendance excessive à l'égard des résultats, qui peut conduire à une « complaisance vis-à-vis de l'automatisation » et à la substitution de la décision humaine par des conclusions automatisées.

Ce risque est amplifié lorsque le contrôle de la qualité et la vérification de l'exactitude des résultats sont insuffisants et que l'analyse juridique indépendante effectuée par l'avocat l'est également.

Cela peut aussi conduire à une dépendance à l'égard des (rares) fournisseurs d'outils d'intelligence artificielle de qualité et de leurs avis juridiques<sup>5</sup>.

Les avocats doivent rester pleinement responsables du travail effectué pour leurs clients et conserver leur libre arbitre, leur esprit critique et leur autonomie dans l'analyse et la prise de décision.

L'IAG ne doit jamais se substituer à l'avocat qui reste responsable des choix et des conseils qu'il prodigue.

5. [Le guide du CCBE sur l'utilisation de l'intelligence artificielle générative par les avocats](#), octobre 2025





# INFORMATION SUR L'USAGE DE L'IA

L'INFORMATION DES CLIENTS .....	34
L'INFORMATION AU SEIN DU CABINET.....	36
L'INFORMATION DES MAGISTRATS .....	36
SYNTHÈSE DES BONNES PRATIQUES.....	36

# INFORMATION SUR L'USAGE DE L'IA

Une transparence totale pourrait être de nature à limiter l'indépendance technique de l'avocat, qui doit rester souverain dans le choix des moyens qu'il met en œuvre pour réaliser sa prestation.

## L'INFORMATION DES CLIENTS

### L'information des clients sur l'usage de l'IA par l'avocat

La question de la transparence dans l'usage de l'IA par l'avocat doit être guidée par la relation de confiance avec le client<sup>1</sup>.

Certains estiment que l'utilisation d'outils d'IA par les avocats est comparable à l'utilisation des bases de données et de jurisprudence, et qu'il n'est donc pas nécessaire pour les avocats d'en informer systématiquement leurs clients.

D'autres pensent que le principe de loyauté implique d'informer le client sur les moyens utilisés pour atteindre les objectifs fixés<sup>2</sup>.

C'est à l'avocat de décider s'il informe son client de l'utilisation d'outils d'IA pour traiter un dossier, en fonction du contexte, de la nature du dossier et des attentes du client. Parfois, la relation commandera de partager l'information, d'autres fois elle rendra ce partage inutile.

Il est toutefois pertinent d'informer le client lorsque celui-ci interroge l'avocat sur ses pratiques de travail, ou lorsque les données du client sont utilisées pour entraîner un système d'IA interne au cabinet : dans ce cas, le consentement du client doit être obtenu.

Par ailleurs, lorsque des robots conversationnels<sup>3</sup> sont utilisés par un avocat pour répondre directement à des questions générales posées par des clients actuels ou potentiels, il convient d'indiquer clairement qu'il s'agit d'un système d'IA et non d'un être humain.

Enfin, il est important de souligner que l'information donnée au client ne limite pas la responsabilité de l'avocat.

1. Hélène Laudic-Baron, Vice-présidente du CNB, « Les enjeux du recours à l'IA à l'égard du respect des règles déontologiques de la profession d'avocat », *L'Observateur de Bruxelles*, 2024/3, n° 137.
2. Christiane Féral-Schuhl, ancienne Présidente du CNB, lors de la Grande Rentrée des avocats du 18 octobre 2024 : « La transparence est un principe fondamental de l'éthique professionnelle du barreau ; il n'est pas question pour l'avocat d'utiliser l'IA sans que cela soit fait en toute transparence à l'égard des clients et à l'égard de ses collègues. »  
Union internationale des avocats (UIA) : « L'avocat maintient une communication transparente avec ses clients, en les informant de l'utilisation qu'il fait des systèmes d'IA, des finalités de cette utilisation et des précautions prises. En tout état de cause, l'avocat veille à ce que la stratégie de chaque dossier qu'il prend en charge pour son client et sa mise en œuvre soient déterminées et réalisées par lui-même et non par l'IA, étant entendu que le jugement professionnel ne peut être délégué à l'IA. En outre, si les informations et les dossiers du client doivent être utilisés pour entraîner un système d'IA, le client doit en être informé et son consentement doit être obtenu. »
3. Le terme robot conversationnel (en anglais, *chatbot* ou plus rarement *chatterbot*) désigne plus particulièrement un agent conversationnel simple conçu pour automatiser un ensemble relativement restreint de tâches répétitives, par exemple afin d'assurer la première ligne d'un service à la clientèle.



La Cour de justice de l'Union européenne, dans son arrêt du 15 janvier 2015 (affaire C-537/13), a jugé abusive la clause limitative de responsabilité de l'avocat à l'égard d'un client consommateur.



## RECOMMANDATION

L'avocat pourrait intégrer dans sa convention d'honoraires une clause rédigée en ces termes :

*« Pour le traitement du dossier, l'Avocat peut utiliser, de manière ponctuelle et encadrée, des outils d'intelligence artificielle, notamment pour l'assister dans la recherche juridique, l'analyse de documents ou la préparation de projets d'actes.*

*Le Client est informé que ces outils n'interviennent qu'à titre d'assistance technique. Ils ne remplacent en aucun cas l'analyse, le raisonnement et le jugement professionnels de l'Avocat, qui restent exclusivement humains. L'Avocat conserve l'entière maîtrise et la responsabilité de l'ensemble des travaux réalisés.*

*L'Avocat veille à utiliser ces outils dans le respect du secret professionnel, des règles déontologiques de la profession d'avocat et de la réglementation applicable en matière de protection des données personnelles. Aucune information confidentielle ou sensible ne sera transmise à un outil ne présentant pas des garanties suffisantes de confidentialité. »*

## L'information des clients sur leur usage de l'IA

Il est recommandé à l'avocat d'informer le client sur les risques qu'il y aurait à ce qu'il soumette à un outil d'intelligence artificielle les documents, analyses, consultations ou travaux élaborés par l'avocat. Ces productions sont soumises au secret professionnel qui risquerait d'être compromis par l'utilisation d'une IA qui n'en garantirait pas le respect.

D'autre part, la non-anonymisation de ces productions serait susceptible d'exposer le client à des poursuites en responsabilité civile ou pénale engagées par les personnes citées si ces productions étaient utilisées par l'IA.

Enfin, l'usage d'outils d'IA pour interpréter ou compléter les travaux de l'avocat est susceptible d'introduire des erreurs ou des interprétations inexactes qui pourraient être préjudiciables au dossier.

## L'INFORMATION AU SEIN DU CABINET

La transparence dans l'utilisation de l'IAG s'applique également à l'intérieur du cabinet : entre associés, entre associés et collaborateurs, et aussi avec le personnel du cabinet en veillant « à communiquer clairement à l'ensemble de ses membres les modalités et les finalités de l'utilisation des outils d'IAG, notamment au regard de leurs risques inhérents et de leurs risques en matière de confidentialité. [...] Autrement dit, cette communication doit permettre à chacun des membres du cabinet de savoir quand et comment les outils d'IAG peuvent être utilisés au sein du cabinet et comprendre les implications de leur utilisation. »<sup>4</sup>

Il est recommandé de mettre en place une charte d'usage de l'IA, de communiquer les bonnes pratiques à l'ensemble des collaborateurs et de documenter les processus liés à l'utilisation de ces technologies.

## L'INFORMATION DES MAGISTRATS

L'avocat ayant nécessairement vérifié, relu et corrigé les réponses générées par l'IAG, les documents qu'il adresse à la juridiction doivent être de la même qualité que s'il n'y avait pas eu de recours à l'IAG.

Dans ces conditions, aucune information spécifique n'a à être donnée à la juridiction, aucune règle n'imposant à l'avocat d'indiquer quels sont les moyens humains, technologiques ou documentaires qu'il a utilisés pour l'élaboration de son dossier.

## SYNTHÈSE DES BONNES PRATIQUES

- Quel que soit le degré d'information du client pour l'usage de l'IA, l'avocat doit toujours protéger les données du client.
- Lorsque le client interroge l'avocat sur ses pratiques de travail, ce dernier doit l'informer de l'usage d'une IAG.
- Lorsqu'ils utilisent des robots conversationnels pour répondre à des questions générales posées par des clients actuels ou potentiels, les avocats doivent indiquer clairement qu'il s'agit d'un système d'IA.
- En interne, le cabinet met en place une charte d'usage de l'IA, communique les bonnes pratiques à l'ensemble des collaborateurs et documente les processus liés à l'utilisation de ces technologies.

4. David Lévy, avocat au barreau de Paris, chargé d'enseignement à l'Université Paris Dauphine-PSL : « Avocats : utiliser déontologiquement les outils d'intelligence artificielle générative », Livre blanc Septeo, décembre 2024.







# HONORAIRES (LOI DU 31 DÉC. 1971, ART. 10 ET RIN, ART. 11)

# HONORAIRES (LOI DU 31 DÉC. 1971, ART. 10 ET RIN, ART. 11)

L'article 10, alinéa 4, de la loi du 31 décembre 1971 dispose que les honoraires tiennent compte, selon les usages, de la situation de fortune du client, de la difficulté de l'affaire, des frais exposés par l'avocat, de sa notoriété et des diligences de celui-ci.

L'article 11 du RIN ajoute que la rémunération de l'avocat est fonction, notamment, de chacun des éléments suivants, conformément aux usages :

- le temps consacré à l'affaire,
- le travail de recherche,
- la nature et la difficulté de l'affaire,
- l'importance des intérêts en cause,
- l'incidence des frais et charges du cabinet auquel il appartient,
- sa notoriété, ses titres, son ancienneté, son expérience et la spécialisation dont il est titulaire,
- les avantages et le résultat obtenus au profit du client par son travail, ainsi que le service rendu à celui-ci,
- la situation de fortune du client.

L'utilisation de l'IA peut impacter le montant des honoraires dans le sens de la réduction ou de l'augmentation : « La réduction des honoraires en raison du gain de temps permis par l'IA et l'augmentation des honoraires en raison des coûts associés à son utilisation. »<sup>1</sup>

Les honoraires doivent être établis de manière équilibrée et transparente, en tenant compte du temps gagné grâce à l'IA, des coûts de création, de formation et d'utilisation de la technologie, ainsi que de la responsabilité de l'avocat pour le contenu généré par l'IA.

La convention d'honoraires, qui reste obligatoire, joue un rôle central pour permettre à l'avocat et au client de s'accorder sur les pratiques et conditions de facturation.

La Charte des principes essentiels de l'avocat européen et le code de déontologie des avocats européens précisent que les honoraires doivent rester justes, prévisibles et proportionnés au service rendu, même lorsque l'IA intervient dans le processus de travail, afin de préserver la confiance du client et le respect des règles professionnelles<sup>2</sup>.

L'American Bar Association précise que la règle exigeant des honoraires raisonnables s'applique également à l'utilisation de l'IA.

L'Union internationale des avocats (UIA) recommande que les avocats déterminent les honoraires de manière équilibrée et transparente vis-à-vis du client, en tenant compte du gain de temps permis par l'IA, des coûts liés à sa création, à son entraînement et à son utilisation, et du fait que l'avocat porte la responsabilité du contenu généré par l'IA ou avec l'aide de l'IA<sup>3</sup>.

1. Hélène Laudic-Baron, Vice-présidente du CNB, « Les enjeux du recours à l'IA à l'égard du respect des règles déontologiques de la profession d'avocat », *L'Observateur de Bruxelles*, 2024/3, n° 137.

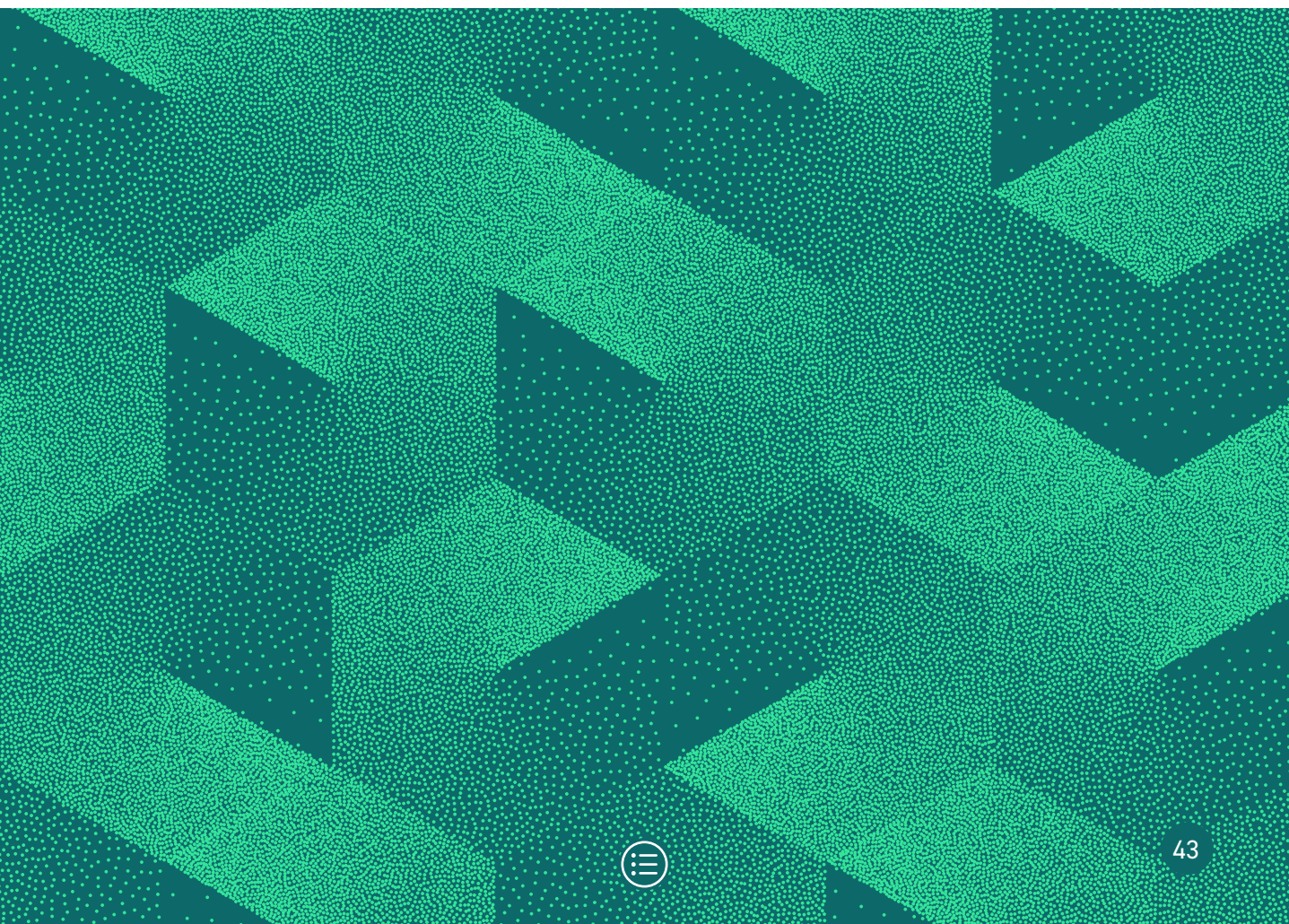
2. [Charte des principes essentiels de l'avocat européen et code de déontologie des avocats européens](#).

3. Union internationale des avocats, [Directives sur l'utilisation des systèmes d'intelligence artificielle par les avocats](#), Congrès de Paris, 30 octobre 2024 [en anglais].





# CONCLUSION



# CONCLUSION

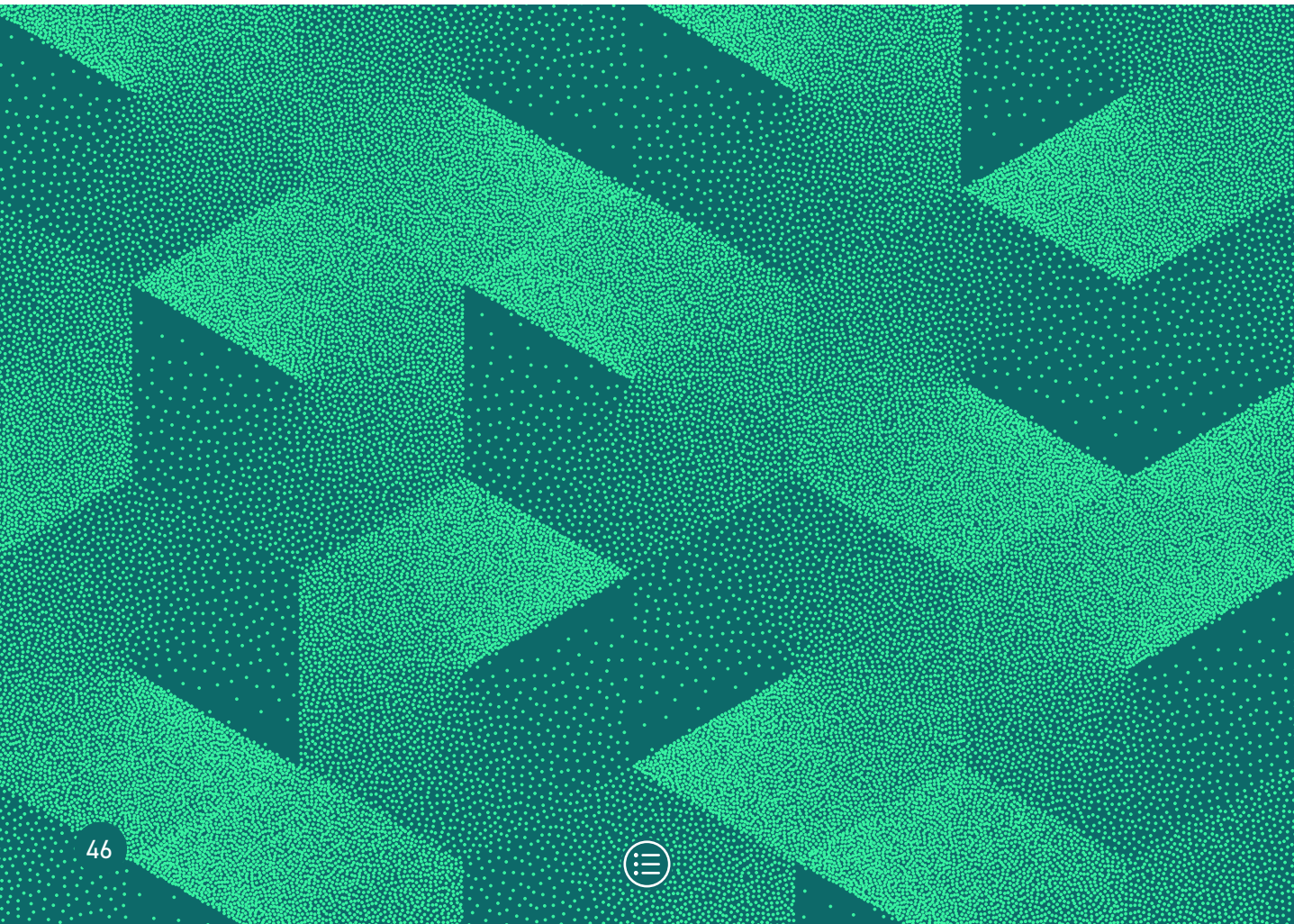
L'IA, bien encadrée, augmente la capacité des avocats à délivrer un service efficace et pertinent. Mais elle n'exonère jamais l'avocat de ses devoirs déontologiques : secret, RGPD, compétence, diligence, prudence, indépendance, absence de conflit d'intérêts, transparence et honoraires raisonnables.

Comme le rappelle Hélène Laudic-Baron, Vice-présidente et responsable du groupe de travail IA du CNB : « *La déontologie et la responsabilité restent des atouts concurrentiels inégalables. Ainsi, l'avocat augmenté par les outils d'IA reste le seul interlocuteur de confiance tant dans le conseil que dans l'accompagnement juridique.* »

## Pour aller plus loin, les sources citées dans le rapport :

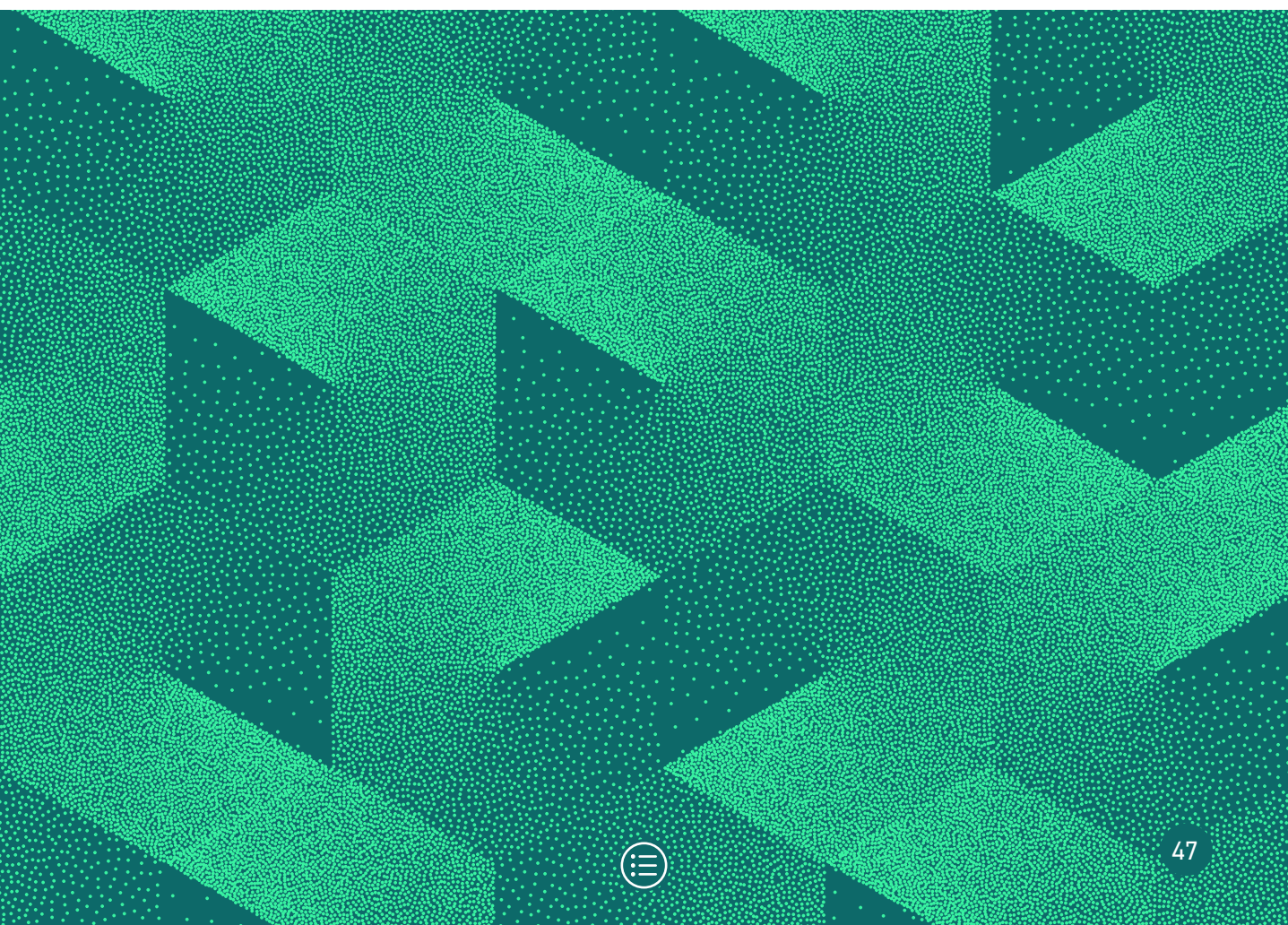
- [Guide de bonnes pratiques dans l'utilisation des systèmes d'intelligence artificielle générative](#), CNB, 1<sup>re</sup> édition, septembre 2024.
- [Le guide du CCBE sur l'utilisation de l'intelligence artificielle générative par les avocats](#), octobre 2025.
- [Grille d'auto-évaluation permettant de guider les avocats dans le choix des logiciels juridiques augmentés par une ou plusieurs couches d'intelligence artificielle générative](#), CNB, 1<sup>re</sup> édition, juin 2025.
- David Lévy, avocat au barreau de Paris, chargé d'enseignement à l'Université Paris Dauphine-PSL : « Avocats : utiliser déontologiquement les outils d'intelligence artificielle générative », Livre blanc Septeo, décembre 2024.
- Hélène Laudic-Baron, Vice-présidente du CNB, « Les enjeux du recours à l'IA à l'égard du respect des règles déontologiques de la profession d'avocat », *L'Observateur de Bruxelles*, 2024/3, n° 137.
- Christiane Féral-Schuhl, intervention lors de la Grande Rentrée des avocats du 18 octobre 2024.
- Union internationale des avocats, [Directives sur l'utilisation des systèmes d'intelligence artificielle par les avocats](#), Congrès de Paris, 30 octobre 2024 [en anglais].
- Barreau de Paris : [Livre blanc sur l'IA](#)
- [Guide du Conseil consultatif conjoint de déontologie de la relation magistrat-avocat](#) (CCC).





# ANNEXE

Liste des bonnes pratiques déontologiques adoptées par le Conseil consultatif conjoint de déontologie de la relation magistrat-avocat (CCC).....	48
--	----



# ANNEXE

## LISTE DES BONNES PRATIQUES DÉONTOLOGIQUES ADOPTÉES PAR LE CONSEIL CONSULTATIF CONJOINT DE DÉONTOLOGIE DE LA RELATION MAGISTRAT-AVOCAT (CCC)

1. **Comprendre le fonctionnement des différents outils d'IAG**, leur niveau de sécurité ; connaître le cadre juridique applicable (obligations en matière de respect de la vie privée, de la propriété intellectuelle et des droits d'auteur) ; se former spécifiquement à la déontologie en matière de recours à l'IA générative pour mieux appréhender les risques de biais, les limites et les usages éthiques de ces outils.
2. **Le recours à l'IAG ne doit pas se substituer à l'expertise humaine** ; tout usage de l'IAG sans aucune relecture critique doit être exclu.
3. **Vérifier** l'exactitude des informations recueillies.
4. **Exclure l'introduction de toute donnée personnelle ou confidentielle dans un outil non sécurisé** ; plus généralement, se renseigner sur la souveraineté des outils utilisés.
5. **Informers les justiciables des risques juridiques et éthiques** concernant l'introduction de données personnelles ou de documents couverts par le secret dans un outil d'IAG non souverain et libre d'accès.
6. **Utiliser les outils d'IAG de manière raisonnée et maîtrisée** afin de limiter leur empreinte environnementale.
7. **Favoriser des échanges réguliers entre les juridictions et les barreaux** pour assurer une compréhension partagée des outils utilisés.



# REMERCIEMENTS

Le Conseil national des barreaux remercie vivement toutes les personnes ayant contribué à ce guide :

## Les membres élus de la commission des règles et usages :

- Bruno BLANQUER, Président
- Frédérique MOREL, vice-présidente
- Juliette SCHWEBLIN, vice-présidente
- Hélène LAUDIC-BARON
- Sophie ANDRIEU
- Agnès BLOISE
- Audrey CHEMOULI
- Brice COTTERET
- Valentine GUIRIATO
- Guillaume ISOUARD
- Simon LAMBERT
- David LEVY
- Yanick LOUIS-HODEBAR
- Karine THIEBAULT
- Alexis WERL
- Thierry TROIN
- Frédéric NAQUET

## Les experts de la commission des règles et usages :

- Laurence JUNOD-FANGET
- Dominique PIAU
- Jean-François BRUN
- Thomas CHARAT
- Dominique de GINESTET
- Frédéric KIEFFER
- Joël MORET-BAILLY
- Karine RIVOALLAN
- Delphine PUJOS
- Jean-Charles NEGREVERGNE
- Jean VILLACEQUE

## Les salariés du Conseil national des barreaux :

- Géraldine CAVAILLE
- Laurence DUPONT
- Guillaume LHUILLIER





## LE CONSEIL NATIONAL DES BARREAUX EST À VOTRE ÉCOUTE

---

Par téléphone au **01 53 30 85 60**

de 8 h 30 à 19 h 00

Par courrier électronique :

**[cnb@cnb.avocat.fr](mailto:cnb@cnb.avocat.fr)**

Sur les réseaux sociaux



Au siège

**180 boulevard Haussmann - 75008 Paris**