



# Evaluation d'outils d'IA pour avocat-e-s

## Légende

-  Introduction
-  Remarques
-  Recommandations de l'AAB
-  Mentions légales

 Les avocats sont sollicités de manière intensive, parfois même par téléphone, par des prestataires qui commercialisent des outils d'IA\* spécialisés dans le secteur juridique. Ces outils sont censés présenter les fonctions suivantes:


- Un grand modèle linguistique (LLM\*\*) répond à des questions d'ordre juridique en s'appuyant sur des données accessibles au public, telles que la jurisprudence.
- Révision et analyse de textes juridiques (notamment révision de contrats).
- Stockage de ses propres données, notamment de ses propres dossiers et modèles de contrats, dans index vectoriel\*\*\* et possibilité d'interroger un LLM à ce sujet.
- Anonymisation\*\*\*\* de documents.


\* Par «outils d'IA», nous entendons ici l'ensemble des logiciels qui s'appuient sur des grands modèles linguistiques (LLM), y compris les modèles d'embeddings


\*\* Large Language Model


\*\*\* En termes simples, un index vectoriel est une structure d'accès aux données spécifique, optimisée pour la recherche assistée par l'IA. À l'aide d'un modèle d'embedding, une représentation vectorielle sémantique est créée et enregistrée pour chaque document. Cela facilite la recherche de documents pertinents en réponse aux requêtes adressées aux LLM.


\*\*\*\* Dans certains cas, on ne sait pas clairement s'il s'agit d'une anonymisation ou simplement d'une pseudonymisation.


 L'utilisation de ces outils d'IA par les avocats se heurte à divers obstacles. Tout d'abord, le secret professionnel doit être préservé. L'intégration de données externes peut en outre soulever des problèmes liés au droit d'auteur. Enfin, il convient de noter que les LLM ne sont pas des systèmes experts basés sur des règles, mais des modèles générés par des processus d'optimisation fondés sur des données et reposant sur des schémas statistiques de texte. La génération de texte s'effectue par l'application de ces schémas statistiques, sans que le modèle ait une «compréhension» du texte généré.


 Ces modèles sont optimisés pour générer des textes pertinents sur le plan linguistique et structurel. Dans le cadre de débats argumentatifs, ce recours à des modèles est souvent voulu et approprié. Cependant, des contradictions factuelles ou logiques peuvent également apparaître dans ce contexte. Le fonctionnement des LLM en matière de mention de sources est encore plus problématique: ces références sont également générées selon les mêmes schémas, sans que leur existence réelle ou leur contenu ne soient systématiquement vérifiés. Cela peut donner lieu à des références qui semblent plausibles, mais qui sont inexactes ou inexistantes (ce que l'on appelle des «hallucinations»). Cela concerne l'existence et le contenu des sources citées.


 Lors de l'anonymisation à l'aide d'outils d'IA, les méthodes probabilistes donnent souvent de meilleurs résultats que les méthodes basées sur des règles, mais elles ne garantissent pas un remplacement complet, cohérent et traçable des noms et autres informations d'identification. Cela peut notamment entraîner une détection incomplète, un remplacement incohérent ou partiel, ainsi que des risques d'identification difficiles à détecter. De plus, pour permettre une anonymisation adéquate, le LLM doit naturellement avoir accès au texte non anonymisé.


 Les outils d'IA actuellement proposées diffèrent en termes de produit, de prix et d'autres conditions contractuelles. Il n'est pas facile de se faire une idée d'ensemble de ces offres et de les comparer à d'autres outils d'IA spécialisés ainsi qu'à des prestataires généralistes nettement moins chers tels qu'OpenAI, Anthropic ou Google. Les questions suivantes, à poser au prestataire, peuvent vous aider dans cette démarche.

 On constate que certaines déclarations faites par les prestataires dans des contextes publicitaires au sujet de leurs outils d'IA prêtent, au mieux, à confusion. Il convient donc d'examiner avec autant d'attention les liens invoqués avec des institutions renommées que les informations relatives aux capacités et aux conditions d'utilisation des outils proposés. Avant de conclure un contrat, il convient également d'en examiner les conditions. Il faut notamment vérifier si le contrat reflète les éventuelles promesses faites par le prestataire oralement ou par e-mail.

 Dans l'état actuel de la technique, il n'est pas possible d'exclure totalement les affirmations factuellement erronées («hallucinations») générées par un outil d'IA. Tout résultat produit par un outil d'IA doit être vérifié manuellement. De même, dans l'état actuel de la technique, il n'est pas possible de détecter toutes les catégories de données personnelles dans un fichier avec une précision de 100% et avec la profondeur requise en matière de digital forensics. Pour chaque tâche exécutée par des outils d'IA, il convient donc d'inclure dans l'analyse coûts-bénéfices les efforts nécessaires à une vérification manuelle approfondie.

 Etant donné que ni les résultats de recherche ni les textes juridiques ne peuvent être considérés dans tous les cas comme objectivement corrects ou incorrects, mais que cette évaluation est souvent de nature subjective, les affirmations du prestataire concernant les gains d'efficacité ainsi que les éventuels benchmarks relatifs aux outils d'IA juridiques doivent être considérés avec prudence. Cela vaut en particulier lorsqu'un prestataire a participé à l'élaboration du benchmark. Il n'est donc pas possible d'évaluer de manière fiable et à l'avance l'ampleur des avantages qu'un outil d'IA apportera à son activité propre, ni même s'il en résultera une valeur ajoutée.

 **Recommandation 1:** Demandez au prestataire s'il exploite lui-même les modèles d'IA. Si ce n'est pas le cas, demandez-lui quelle entreprise fournit ces modèles. Dans tous les cas, vous devriez demander où se trouvent les serveurs concernés et où s'effectuent les autres traitements de données par le prestataire ainsi que par d'éventuelles tiers (par exemple pour l'exploitation de l'interface utilisateur de l'outil d'IA ou traitements de données à des fins d'assistance et de développement). Demandez également quels modèles d'IA sont utilisés et si vous serez informé des changements dans ce domaine après la conclusion d'un éventuel contrat.

 **Recommandation 2:** Demandez au prestataire si a) lui-même, b) l'entreprise qui fournit les modèles d'IA, ou c) des tiers peuvent, d'un point de vue technique, consulter les documents enregistrés dans la base de données ainsi que les requêtes que vous adressez à l'outil. Demandez également s'il existe des accords visant à empêcher légalement cet accès, et le cas échéant, de quelle nature sont ces accords. Demandez également, tant pour les fichiers que vous téléversez que pour vos requêtes, quelles opérations de traitement des données sont effectuées sur quels serveurs, qui exploite ces serveurs, où ils se trouvent et si les données sont utilisées pour l'entraînement de modèles également utilisés par des tiers.



**Recommandation 3:** Si le prestataire vante l'expertise juridique particulière de son outil d'IA, demandez-lui en quoi elle consiste. En principe, il est concevable que le prestataire entraîne son propre LLM avec des données juridiques ou qu'il réentraîne un modèle de base existant avec des données juridiques, c'est-à-dire qu'il ait procédé à un réglage fin. Cependant, cette pratique est actuellement rare en raison des coûts élevés, de l'impact limité sur la qualité des réponses et de l'évolution rapide des modèles. Le plus souvent, l'«expertise» repose plutôt sur des prompts préformulés ainsi que sur l'intégration de sources de données externes telles que des bases de données de jurisprudence, de littérature juridique et de textes législatifs. À cet égard, vous pouvez demander quelles sources de données externes ont été intégrées, d'où elles proviennent et dans quelle mesure la solution va au-delà d'une simple recherche sur le Web ou de l'intégration d'un MCP\* (par exemple OpenCaseLaw) dans un chatbot généraliste tel que ChatGPT ou Claude.

\* Le MCP (Model Context Protocol) est une norme relative aux interfaces de programmation qui permettent aux grands modèles de langage (LLM) d'accéder à des bases de données et à des outils externes. Ce terme est également utilisé ici (comme dans le langage courant) pour désigner une interface qui respecte la norme MCP.



**Recommandation 4:** Si le prestataire donne l'impression que sa solution exclut toute hallucination, il convient de faire preuve de scepticisme. Une exclusion totale et garantie des hallucinations n'est actuellement pas techniquement possible, même en intégrant des sources de données externes et internes. Il est uniquement possible, pour les mentions de sources indiquées, de vérifier automatiquement si la référence existe et, le cas échéant, si elle est classée dans un domaine juridique préalablement identifié. À l'heure actuelle, il est absolument impossible de vérifier de manière fiable le contenu des textes générés par l'outil d'IA. Vous pouvez demander au prestataire s'il assume une responsabilité objective pour les dommages consécutifs à une hallucination.



**Recommandation 5:** Il en va de même pour l'anonymisation automatisée de fichiers électroniques. Demandez au prestataire quelles catégories de données personnelles sont identifiées et s'il garantit une anonymisation complète. Demandez également si l'anonymisation est effectuée par un modèle d'IA et quelles étapes de traitement les fichiers subissent avant l'anonymisation. Renseignez-vous sur les tests effectués et leurs résultats en matière d'anonymisation.



**Recommandation 6:** Demandez au prestataire s'il existe des preuves, ou au moins des études d'avocat de référence, pouvant attester d'un gain d'efficacité grâce à l'utilisation de l'outil d'IA.



**Recommandation 7:** N'hésitez pas à transmettre les réponses des prestataires d'outils d'IA à l'AAB, qui les mettra à la disposition de tous ses membres de manière appropriée. Vous pouvez également répondre à toutes les questions directement via le formulaire en ligne: <https://form.jotform.com/260965005190050>



Numérisation de la justice / Justitia 4.0, aide-mémoire n°4 de l'AAB: Évaluation d'outils d'IA pour avocat-e-s  
Langues: AL/FR

Version 1 du 10 avril 2026

Editeur: Association des avocats bernois AAB

Auteur: Jan Reinhardt, dr en droit (hyqu.ch)

Review: Jörn Erbguth (erbguth.net), Me Daniel Kettiger (kettiger.ch), Me Claudia Schreiber (advoschreiber.ch), Me Bettina Beck (beck-kloeti.ch), Me Eleonor Gyr (m15.ch)

Disclaimer: Cet aide-mémoire n'a pas la prétention d'être exhaustif et sert d'orientation aux membres de l'Association des avocats bernois AAB. Les aide-mémoires sur la numérisation de la justice / Justitia 4.0 sont mis à jour périodiquement, vous trouverez les versions actuelles sur le site de l'Association des avocats bernois AAB: <https://www.bav-aab.ch/fr> → Numérisation, Justitia 4.0