

GRILLE DE LECTURE SYNTHÈSE DES CONSULTATIONS EFFECTUÉES PAR LE GROUPE DE TRAVAIL SUR L'INTELLIGENCE ARTIFICIELLE

SOMMAIRE

Propos liminaires.....	3
Glossaire.....	4
Enjeux liés à l'utilisation de l'intelligence artificielle Pour la profession d'avocat.....	7
Critère à prendre en considération dans une perspective de choix d'un outil d'IA juridique.....	10
Comparatif des solutions d'IA juridiques auditées (à jour du 17 mars 2025)	13
Synthèse (sous couvert d'évolution et en fonction des éléments déclarés, trouvés et/ou transmis par les sociétés)	25

PROPOS LIMINAIRES

Le présent document a pour objectifs de :

- rappeler les problématiques et enjeux que pose l'utilisation de l'intelligence artificielle générative (IAG) par la profession d'avocat et qui ont été discutés durant les auditions organisées par le groupe de travail sur l'intelligence artificielle,
- tracer des lignes directrices concernant le choix de ce type d'outil en prenant en compte les fonctionnalités proposées, les conditions de souveraineté des données, la confidentialité et la sécurisation des données des cabinets ainsi que la fiabilité dont ces outils doivent faire preuve dans les réponses qu'ils apportent.
- exposer les différentes caractéristiques des outils d'intelligence artificielle (IA) juridiques audités par le Conseil national des barreaux. Certains sont déjà bien connus des avocats et professionnels du droit et mis au service des cabinets afin d'évaluer leurs forces et leurs faiblesses.

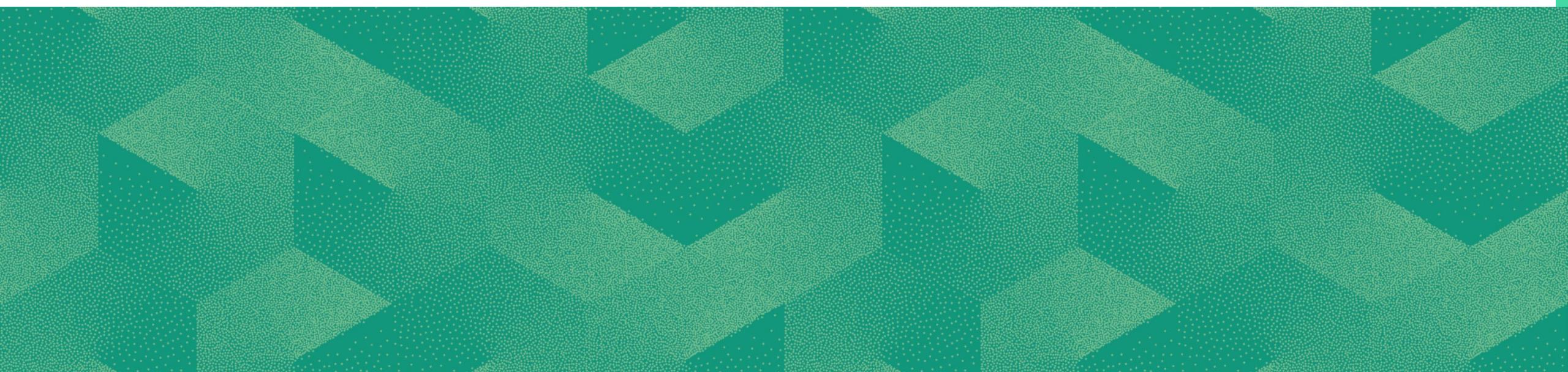
Un groupe de travail transversal « Intelligence artificielle » (GT-IA) a été créé au sein du Conseil national des barreaux (CNB) en 2024.

Ce groupe de travail coordonne les travaux des commissions du Conseil national des barreaux sur les sujets de l'IA.

Le groupe de travail a organisé des consultations dès le mois d'avril 2024 qui ont permis de rencontrer :

- des consœurs et confrères avocats, des magistrats et des universitaires engagés sur le sujet de l'IA générative appliquée au milieu du droit,
- des entreprises clés du secteur juridique proposant des solutions à destination des professionnels du droit et principalement des avocats (Septeo, Lefebvre Dalloz, Lexbase, LexisNexis, Doctrine...),
- des start-ups disruptives dans le secteur (Ordalie, Jimini, Juri'Predis...),
- une grande entreprise de la tech éditant un système d'intelligence artificielle grand public (Microsoft),
- une société spécialisée dans le conseil aux entreprises en matière de transformation digitale, incluant des services facilités par l'IAG (Niji).

GLOSSAIRE



GLOSSAIRE

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 sentiment 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 de récupération (*Retrieval Augmented Generation*, RAG) est le processus consistant à optimiser le résultat 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 que ceux-ci restent cohérents, précis et utiles dans de nombreux contextes.

Avantages

La RAG améliore les systèmes d'IA en intégrant des connaissances externes, fournissant des résultats plus précis et contextuellement pertinents.

La RAG réduit les coûts et les risques liés à la confidentialité car elle n'exige pas de réentraînement des modèles avec des données sensibles contrairement au fine-tuning.

Inconvénients

La mise en œuvre de la RAG peut être plus complexe. Il nécessite une intégration fluide entre les systèmes de récupération et de génération.

L'utilisation de données externes peut poser des risques en matière de sécurité et de confidentialité, c'est pourquoi la RAG doit être nécessairement sécurisée.

La qualité des résultats générés dépend fortement de la qualité et de la pertinence des données récupérées.

RAG sécurisée : comme évoqué précédemment, l'un des inconvénients du recours à un système de génération augmentée de récupération (RAG) est la sécurité et la confidentialité des données. Ainsi, il est essentiel de mettre en place des mesures techniques, physiques et plus particulièrement :

• des mesures techniques

- chiffrement : des données en transit et au repos ainsi que le chiffrement des serveurs, des disques et des flux (TLS/SSL, HTTPS, SFTP),
- pseudonymisation et anonymisation des données personnelles,
- journalisation et traçabilité des accès et des actions effectuées sur les données,
- gestion des droits d'accès avec une politique de mots de passe complexes et une authentification multifactorielle,
- outils de lutte contre les attaques : utilisation de pare-feux, antivirus et systèmes de détection d'intrusion pour protéger les infrastructures,

• des mesures organisationnelles :

- élaboration de politiques, notamment de sécurité de l'information basée sur des normes ISO 27001 et ISO 27002, ainsi que de gestion des droits relatifs à la protection des données (« droits RGPD ») des personnes,
- analyse des risques, passant notamment par les analyses d'impact sur la protection des données (PIA) pour identifier et gérer les risques liés aux données personnelles,
- sensibilisation et formation des membres de l'organisation aux bonnes pratiques de sécurité et de protection des données,

• des mesures physiques :

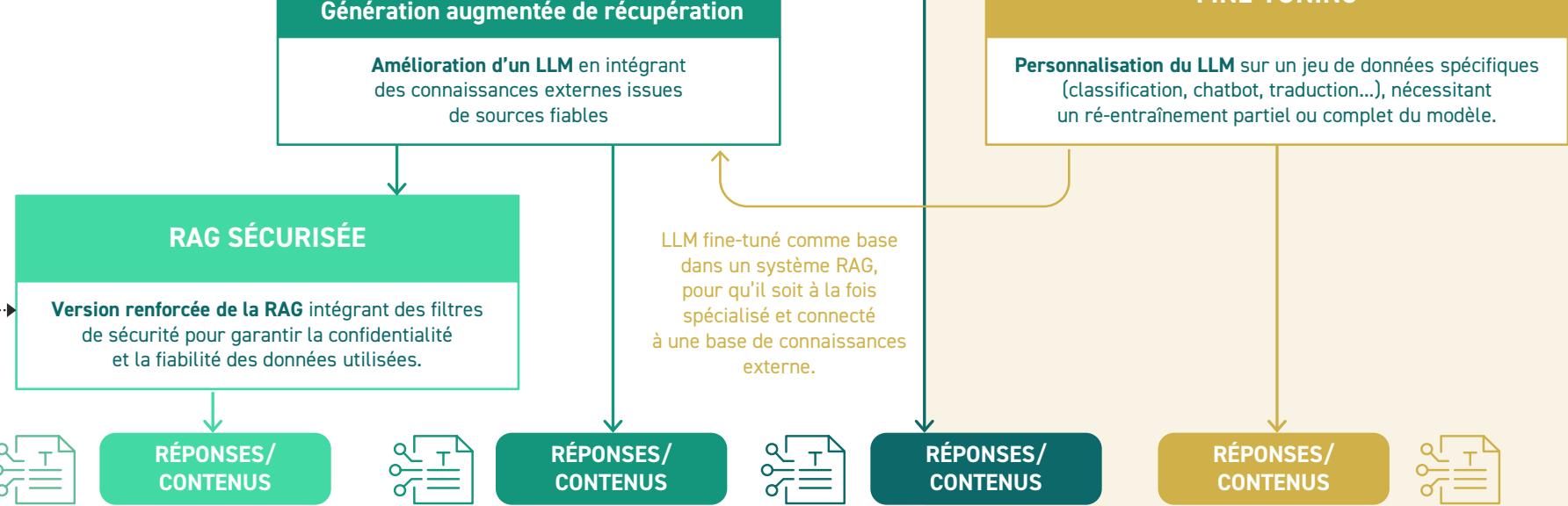
- protection des locaux par accès sécurisés à l'aide d'alarmes, de détecteurs de mouvement, de systèmes anti-intrusion, de portes et armoires fermées à clé voire de vidéosurveillance si cela est pertinent,
- archivage intermédiaire réel, à savoir des espaces physiques ou numériques d'archives cloisonnés avec un accès limité à quelques personnes dûment habilitées.

LES INTERACTIONS ET COMPARAISONS ENTRE LLM, RAG ET FINE-TUNING

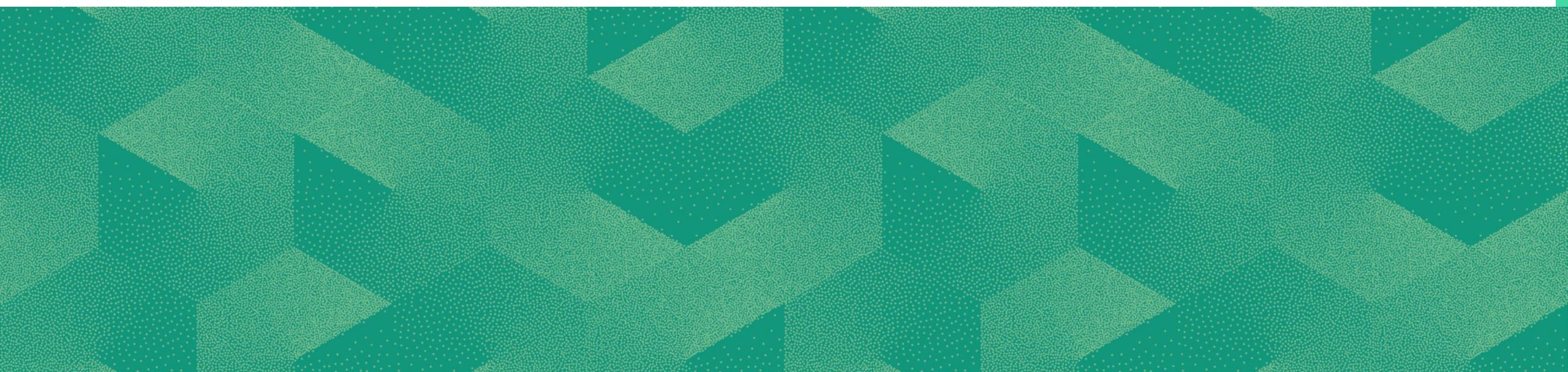
Le fine-tuning et la RAG (*Retrieval Augmented Generation*) sont deux approches complémentaires qui visent à améliorer les performances d'un modèle de langage (LLM), selon les besoins de spécialisation, de réactivité ou de confidentialité.

Données externes récupérées

La RAG peut être une alternative ou un complément au *fine-tuning* lorsqu'on ne souhaite pas ou ne peut pas modifier le modèle.
(ex. : pour des raisons de coût, de confidentialité ou de réactivité).



ENJEUX LIÉS À L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE POUR LA PROFESSION D'AVOCAT



ENJEUX LIÉS À L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE POUR LA PROFESSION D'AVOCAT

La capacité de l'intelligence artificielle générative à produire, entre autres, du texte, des clauses contractuelles, des résumés de jurisprudence, des analyses juridiques, des brouillons de rédaction d'actes juridiques, etc., présente des implications profondes pour la profession d'avocat (et pour les professionnels du droit de manière générale).

Plusieurs problématiques et défis se posent ainsi aux cabinets qui ont eu ou souhaitent avoir recours à cette technologie :

- **en matière de qualité et de fiabilité des données générées** : les outils d'IA peuvent intégrer dans leurs réponses les fameux « biais » et « hallucinations » qui, dans le cas notamment d'analyses juridiques ou de recherches de jurisprudence, pourraient entraîner des litiges ou des sanctions pour faute professionnelle si elles étaient d'aventure reprises sans vérification.

En outre, certaines IA génératives entraînées sur des données générales ont tendance à produire des réponses non adaptées à des cas spécifiques et trop sommaires.

Enfin, l'utilisation d'outils d'IA juridique ayant recours à de grands modèles de langage (LLM) d'origine américaine (GPT, Claude, etc.) pourra multiplier les « biais » (et éventuellement des « hallucinations ») de droit anglo-saxon, à défaut de réponses fiables basées sur un système romano-civiliste.

- **en matière de propriété intellectuelle** : les textes et contenus générés par l'IA peuvent violer des droits d'auteur existants ou poser des questions sur la titularité des œuvres produites.

- **en matière d'automatisation des tâches et ses conséquences** : l'IA générative permet de gagner énormément de temps en automatisant un certain nombre de tâches chronophages, voire rébarbatives, généralement à faible valeur ajoutée (comme la recherche jurisprudentielle ou la recherche de documents).

Cette situation est susceptible d'induire un besoin moindre en personnel peu qualifié ou avec un niveau plutôt junior, mais nécessite une expertise toujours élevée de vérification et d'adaptation des résultats fournis par les outils d'IA. Certaines tâches pourraient même, comme la rédaction standardisée ou la recherche, se voir être complètement externalisées à un outil d'IAG, ce qui entraînerait une redéfinition totale des rôles et des responsabilités au sein d'un cabinet.

- **en matière de formation professionnelle** : il est naturellement conseillé aux avocats de se former à l'utilisation des outils d'IA, notamment afin de leur apprendre à formuler les meilleurs prompts possibles. En contrepartie, cela va nécessairement entraîner à terme des investissements financiers pour le cabinet et un temps non négligeable alloué à ces questions. .

- **en matière de protection des données (à caractère personnel ou non)** : les outils d'IA présentent un risque de divulgation de données confidentielles et stratégiques pour le cabinet, mais également des données personnelles des clients, et notamment des « catégories particulières de données » ou données sensibles. Ainsi, l'utilisation de ces outils soulève régulièrement des questions sur la conformité effective à la législation de l'Union européenne, et notamment le respect du Règlement général sur la protection des données (RGPD).

- liés à une perte de compétence des avocats : comme bon nombre d'études le soulignent déjà, le recours systématique, ou à tout le moins généralisé, à des outils d'IA fait peser le risque pour le professionnel d'affaiblir ses aptitudes intellectuelles et cognitives, notamment concernant le raisonnement juridique, par perte d'habitude de faire ses propres recherches, de rédiger par lui-même et de faire preuve d'esprit critique.

Cette baisse des compétences et de la capacité d'analyse, à force de se « reposer » sur la machine, aura également comme conséquence mécanique de faire « stagner » le niveau des outils d'IA car le jeu de données sur lequel ils se baseront à l'avenir reposera sur des corpus déjà eux-mêmes générés par des IA, peu uniformisés et moins originaux, avec « un peu moins de génie » généré par les professionnels du droit.

- **liés à une dévaluation de l'image du travail des avocats** : une automatisation accrue et une utilisation banalisée des outils d'IA au sein des cabinets pourraient amener leurs clients à douter de la réelle valeur ajoutée des réponses et conseils fournis par les avocats et entraîner de fait une dépréciation de l'image de la profession, par la possibilité de survenance d'au moins trois situations :
 - une uniformisation des « productions » juridiques par l'utilisation des mêmes outils (par exemple la génération automatique de contrats basés sur les mêmes modèles) au détriment de l'inventivité et de l'innovation,
 - une remise en question des tarifs pratiqués voire une baisse potentielle mécanique de ces tarifs ;
 - à l'inverse, une stabilité, voire une augmentation de ces tarifs du fait du coût d'utilisation des outils d'IA pesant sur les cabinets, répercute sur les bénéficiaires.



NOTA

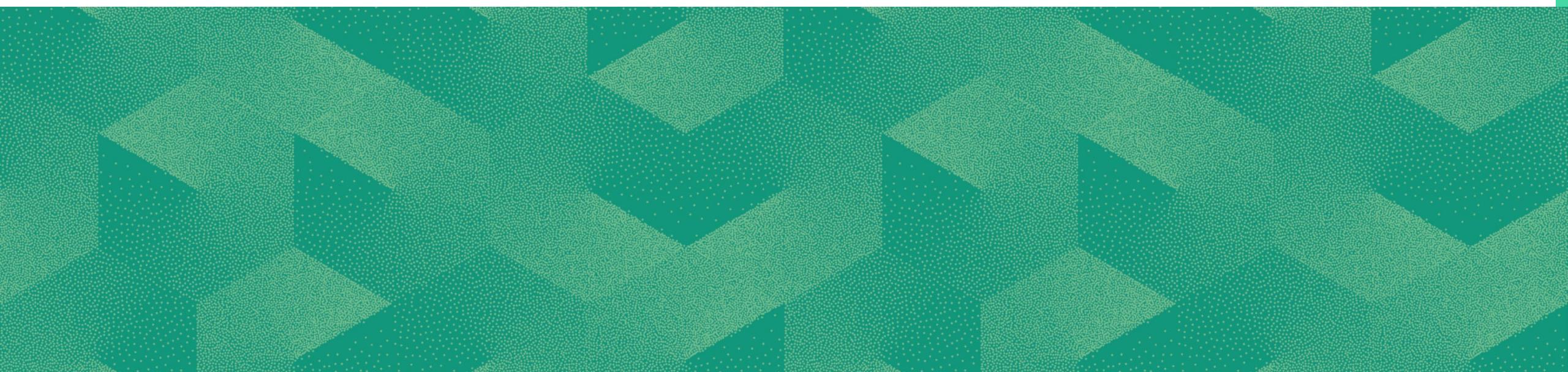
Sur le sujet du coût, l'accès à l'IA sera vécu différemment en fonction de la taille du cabinet, des tarifs relativement élevés pouvant exclure d'office les petits cabinets.

- **liés à la dépendance aux outils d'IA** : l'abandon plus ou moins marqué du savoir-faire humain et/ou la place trop importante laissée à la technologie dans l'élaboration des tâches juridiques présente(nt) le risque pour le cabinet de :
 - s'exposer mathématiquement à des failles de sécurité plus nombreuses et parfois spécifiques (cyberattaques, vol ou atteinte à la confidentialité des données, pannes, violation du droit d'auteur ou du droit de la propriété intellectuelle, etc.), par le fait de ne faire appel systématiquement qu'à des outils informatiques interconnectés et qui ne seraient pas sécurisés,
 - diminuer potentiellement son autonomie stratégique face à de grandes entreprises technologiques (OpenAI, Anthropic, Amazon, Microsoft, etc.), le lieu d'hébergement des LLM et la nationalité de la société détenant les serveurs hébergeant les données, notamment si elle est américaine, pouvant limiter la souveraineté des données et poser un problème supplémentaire en matière de respect du RGPD (cf. supra).

- **liés à l'utilisation à deux vitesses par la profession des outils d'IA** : s'il semble incontestable que l'IAG soit une véritable source d'opportunités pour les avocats, sa généralisation risque de créer une fracture de plus en plus grande entre ceux qui vont maîtriser les outils et qui pourront les utiliser – notamment en fonction du coût et de la formation – et ceux qui ne voudront ou ne pourront pas opérer de transition vers ce type d'outils.
- **liés aux destructions d'emploi** : même si les résultats des outils d'IA sont toujours basés sur des modèles probabilistes, et bien que ces outils ne « raisonnent » pas, la question de la valeur ajoutée d'un assistant juridique, d'un apprenant (stagiaire, alternant) ou d'un profil junior pourrait se poser face à la puissance et à la rapidité des réponses générées.



CRITÈRES À PRENDRE EN CONSIDÉRATION DANS UNE PERSPECTIVE DE CHOIX D'UN OUTIL D'IA JURIDIQUE



CRITÈRES À PRENDRE EN CONSIDÉRATION DANS UNE PERSPECTIVE DE CHOIX D'UN OUTIL D'IA JURIDIQUE



FONCTIONNALITÉS

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

- les éditeurs juridiques traditionnels et legaltechs, les systèmes de recherche documentaire, de recherche avancée ou « augmentée », etc.,
- les outils à pluguer 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 si étrangères ou encore la génération de mémos juridiques.

À l'inverse, une piste intéressante serait de privilégier et sélectionner des outils qui proposent des fonctionnalités rares, même si d'ailleurs elles ne seraient encore à un instant T qu'à l'état balbutiant.

Enfin, l'un des critères de choix de l'outil sera sa délimitation ou sa spécialisation au(x) droit(s) couvert(s) par l'avocat (droit pénal, droit des affaires, droit international...).



SOUVERAINETÉ DES DONNÉES

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

1. le lieu d'hébergement des données des clients (France, voire Union européenne),
2. 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 qui dispose dans son droit national de dispositions extraterritoriales permettant aux autorités de l'état correspondant de réquisitionner des données stockées sur des serveurs appartenant aux entreprises de sa nationalité, comme les entreprises américaines en l'état actuel de leur législation),
3. le lieu d'hébergement des données du grand modèle de langage (LLM) utilisé (France, voire Union européenne),
4. la nationalité de l'entreprise détenant les serveurs hébergeant les données du LLM (même caractéristique qu'exposé précédemment au point n° 2).

Un prérequis est que l'outil d'IA choisi ne réutilise pas des données à des fins d'entraînement du ou des grand(s) modèle(s) de langage utilisé(s) 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 légitime peut donc subsister sur la question.

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

La seule manière 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 totale préalable des données,
- l'installation en local du LLM sur les propres instances 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 process et fonctionnalités l'ensemble des mesures exposées dans cette section.



CONFIDENTIALITÉ ET 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 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 le rajout d'une RAG sécurisée,
- la suppression ou l'anonymisation 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 outils d'IA d'accéder aux données des avocats, ou à défaut des 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,
- tout 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 concernant la prétendue robustesse d'un outil et sa résistance théorique aux attaques informatiques.

Il peut être donc conseillé aux avocats de challenger les éditeurs d'outils d'IA juridiques par ce biais, ce qui est d'ailleurs pour ces premiers 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).



FIABILITÉ

Les éléments à prendre en considération sont :

- la présence obligatoire de sources ponctuant tous les contenus générés par l'outil, avec un lien direct pointant vers une entité extérieure hébergeant par exemple la décision de justice visée,
- la source visée doit être indiscutable et de confiance,
- la présence d'un système de RAG (Retrieval Augmented Generation) pour peu qu'il soit correctement bâti et sécurisé,
- l'origine du LLM utilisé et ce, s'il n'était pas français ou européen, afin d'éviter les biais de Common Law et privilégier ceux de droit continental,
- les certificats, labels et codes de conduite respectivement obtenus et suivis par les sociétés éditrices d'outils d'IA.

Il est recommandé aux professionnels de tester les outils avant utilisation en conditions réelles et d'évaluer les performances spécifiques des modèles d'IA dans le domaine juridique, sous forme de benchmarks spécifiques à l'aide de jeux de données du type « LegalBench ».

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



DOCTRINE



FONCTIONNALITÉS CAS D'USAGE

- Le *chatbot* : assistant conversationnel classique pour faciliter la recherche juridique,
- La « *Doctrine Flow* » qui permet d'automatiser la gestion administrative du contentieux et la rédaction de documents,
- Le module « *Detect* » qui permet d'analyser un grand nombre de documents très rapidement pour une meilleure compréhension du dossier,
- Le module « *Tableau* » qui permet de générer un tableau de jurisprudence avec des colonnes personnalisées.



LLM UTILISÉ(S)

- GPT4-o (OpenAI)**
Hébergé sur Microsoft Azure



LIEU D'HÉBERGEMENT DES DONNÉES

- Allemagne, Francfort – hébergement AWS.



RÉUTILISATION/COMMUNICATION DES DONNÉES

- Pas de réutilisation des données par le LLM.
- Pas de transfert à OpenAI aux États-Unis.
- Engagement de non-réentraînement des modèles sur les données utilisateurs.



MESURES DE SÉCURITÉ

Les questions posées à l'IA sont réalisées sous le compte de Doctrine, de sorte qu'on ne peut pas savoir quelle recherche le client a effectué. Toutes les données sont supprimées. Il n'y a donc aucun transfert à OpenAI. De la pseudonymisation des requêtes au chiffrement des données, Doctrine détient la clé de chiffrement.



DÉPLOIEMENT



COÛT

- Doctrine Pro : 2 094 € HT par an.
- Doctrine Flow : 1 392 € HT par an.

Tarifs dégressifs en fonction du nombre de licences prises.



ACCOMPAGNEMENT À LA PRISE EN MAIN

- Formations,
- Tutoriels,
- Support client dédié.



SPÉCIFICITÉS OUTIL/SOCIÉTÉ



LABELS/CERTIFICATIONS/ CODES DE CONDUITE

- Code de conduite sur l'IA générative,
- Code de conduite de la *legaltech* sur l'IA juridique,
- Certification ISO 27001,
- Membre du *Hub IA* de Bpifrance.



REMARQUES/ OBSERVATIONS

Doctrine est accompagné par la CNIL pour la conformité au RGPD notamment en matière d'IA générative. L'Autorité nationale de protection des données personnelles a déjà contrôlé Doctrine, de 2020 à 2022, avec une absence de sanction à la clé.

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



GENIA-L (LEFEFEBVRE DALLOZ) Assistant recherche & production



FONCTIONNALITÉS CAS D'USAGE

- Synthèse de réponse à une question posée basée sur les fonds Lefebvre Dalloz,
- Synthèse de documents,
- Tableau de cas pratiques, explication juridique permettant d'analyser les bases légales et arguments en lien avec la question posée,
- Explication en langage non-expert (adaptée à des non-juristes),
- Tableau de conclusions,
- Arguments de doctrine administrative « pour et contre »,
- Analyse de documents,
- Questions alternatives.



LLM UTILISÉ(S)

- GPT4-o (OpenAI)
Hébergé sur Microsoft Azure (France)



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> • France, hébergement Microsoft Azure. 	<p>GenIA-L ne s'entraîne pas avec les données personnelles de ses clients, mais exclusivement à partir de la base documentaire de Lefebvre Dalloz.</p> <p>L'IA traite les questions sans besoin de données liées à des clients spécifiques. Les données personnelles restent confidentielles sauf si le client les fournit expressément au moyen de la fonction de <i>feedback</i> dans l'interface.</p> <p>Cette solution n'utilise donc pas des données issues de l'interaction avec l'utilisateur pour améliorer ses réponses ou pour s'entraîner davantage.</p>	<p>GenIA-L a plusieurs mesures de sécurité pour éviter les fuites et les abus de données : en respectant les normes RGPD et en protégeant les données des clients.</p> <p>La solution priviliege la confidentialité des utilisateurs et la sécurité des données.</p> <p>En clair, tout est fait « <i>by design</i> » afin qu'aucune donnée client ne soit exposée aux SI d'OpenAI et que rien ne soit jamais stocké (<i>stateless</i> ou <i>Zero Data Retention</i>).</p>



DÉPLOIEMENT

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATIONS/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> • 250 € HT par mois (ne comprend pas l'accès au fonds documentaire Dalloz) pour une équipe inférieure à 50 juristes 	<ul style="list-style-type: none"> • Formations, • Accompagnement personnalisé, • Support technique. 	<ul style="list-style-type: none"> • Certification ISO 27001 en cours. 	<p>Lefebvre Dalloz surveille l'évolution du LLM Mistral, en remplacement d'Open AI, car la société souhaite renforcer la souveraineté de sa solution. Solution utilisée par le Barreau de Paris et offerte aux avocats pendant un an.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



JIMINI (ODYSAI) Copilot d'IA pour les professionnels du droit



FONCTIONNALITÉS CAS D'USAGE

- Analyse sourcée dans de grandes bases documentaires des cabinets,
- Audits et grilles d'analyse de volumes importants de documents en conseil et contentieux,
- Assistant rédactionnel « *Draft* » (réalisation de premières versions de contrats, conclusions, mémos, ...),
- Correction orthographique, de mise en page et des références croisées avec surveillance des modifications
- Traductions juridiques assistées par IA,
- Recherche juridique croisée avec les décisions en open data et les bases internes du cabinet,
- Publipostage intelligent via des trames évolutives.



LLM UTILISÉ(S)

- Combinaison de modèles propriétaires et *open source* (*start-up* membre du Mistralship de Mistral (Mistral AI))
- Hébergé chez Microsoft Azure (France et Suède)

SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> • France, hébergements Scaleway [ISO 27001, 27017, 27018, 9001 et HDS]. 	<p>Les données d'un client ne sont jamais partagées avec d'autres ni avec un tiers.</p> <p>Les données de recherche peuvent être prises, de manière sécurisée, à partir de la base de données documentaire du cabinet.</p>	<ul style="list-style-type: none"> • Chiffrement 256 bits des données au repos et en transit. • Sécurité physique des données avec formation des employés, accès sécurisé aux locaux et surveillance 24h/24. • Contrôle d'accès basé sur le principe du moindre privilège. • Tests réguliers pour identifier et corriger d'éventuelles vulnérabilités.

DÉPLOIEMENT

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATIONS/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> • Licence à 150 € par mois et par utilisateur. Degréssif en fonction du nombre de licences souscrites et de la taille du cabinet. 	<ul style="list-style-type: none"> • Formation et accompagnement <i>ad hoc</i> lors de la prise en main, en présentiel ou en ligne, • Accompagnement technique et service client en continu, • Ressources d'aide en ligne, formations à l'IA juridique. 	<ul style="list-style-type: none"> • Certification ISO 27001. 	<p>L'outil utilise principalement des données <i>open source</i> fiables (Légifrance, Cour de cassation, etc.) ainsi que les données internes des cabinets (valorisation et exploitation de données souvent non structurées et mal utilisées). En partenariat avec Gide depuis mars 2025. La fonction « <i>Draft</i> » peut directement interagir avec Word et y être intégrée.</p>

SPÉCIFICITÉS OUTIL/SOCIÉTÉ

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



JURI'PREDIS Outil d'aide à la décision



FONCTIONNALITÉS CAS D'USAGE

- Moteur de recherche jurisprudentielle,
- Commentaire de décisions,
- détection automatique des références juridiques dans des documents,
- Veilles sur l'actualité juridique spécialisée,
- Accès aux informations légales, financières et contentieuses des entreprises,
- Publication de formalités légales.



LLM UTILISÉ(S)

- Mistral (Mistral AI)
Hébergé sur Microsoft Azure



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> • Pays-Bas et Allemagne, hébergement DigitalOcean (acteur américain) certifié DPF jusqu'au 14 mars 2026. 	<p>L'apprentissage du LLM à partir des requêtes des clients est désactivé.</p>	<p>Les données au repos chez l'hébergeur sont chiffrées, mais nous ne savons pas qui détient les clés de chiffrement</p>



DÉPLOIEMENT

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATIONS/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> • 45 € HT par mois pour un compte individuel (engagement de 12 mois). • 100 € HT par mois pour des comptes multiples de cabinet (engagement de 12 mois). 	<ul style="list-style-type: none"> • NC 	<ul style="list-style-type: none"> • NC 	<p>Juri'Predis n'a pour le moment pas développé sa propre IA générative. L'entreprise indique avoir fait le choix de développer ses solutions en lien et en conformité avec le cadre déontologique, notamment par des mécanismes de pseudonymisation des données. Juri'Predis a mis en place une RAG permettant d'obtenir des réponses plus précises, plus contextuelles et plus récentes selon les données fournies. L'outil propose, au final, une aide à la décision.</p>



SPÉCIFICITÉS OUTIL/SOCIÉTÉ

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES

 <p>JUS AI ASSISTANT (JUS MUNDI)</p>
 <p>FONCTIONNALITÉS CAS D'USAGE</p> <ul style="list-style-type: none"> Recherche juridique, conception de mémos de recherche, Interaction avec une affaire particulière, Système de questions/réponses (sourcées), Rédaction d'arguments juridiques, Analyse de documents, Traduction juridique.
 <p>LLM UTILISÉ(S)</p> <ul style="list-style-type: none"> GPT4-o (OpenAI) Version fine-tunée Hébergé sur Microsoft Azure

SÉCURITÉ ET CONFIDENTIALITÉ

 LIEU D'HÉBERGEMENT DES DONNÉES	 RÉUTILISATION/ COMMUNICATION DES DONNÉES	 MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France, Gravelines – hébergement OVH [ISO 27001 et HDS]. 	<p>Aucune interaction ni requête effectuée avec l'outil n'est conservée ni accessible par d'autres systèmes ou par des tiers.</p> <p>Jus Mundi a appliqué la « <i>Zero Retention Policy</i> » : les données, transmises vers les serveurs Azure et retournées ensuite, seront supprimées immédiatement. Ainsi, il n'y aura pas de possibilité, même avec le Cloud Act, de revenir dessus et de savoir ce qu'il s'est passé.</p>	<ul style="list-style-type: none"> Base de données versée dans une RAG : aucune recherche vers l'extérieur, Recherches sécurisées et chiffrées avant transfert vers leurs serveurs (protocole HTTPS-TLS 1.2 et algorithme de chiffrement AES-256), Serveurs sécurisés et conformes aux standards internationaux de sécurité des données personnelles (hébergement OVH), Identifiants de connexion bénéficiant d'un très haut degré de sécurisation : mots de passe hachés (cryptage par empreinte irréversible sans possibilité de décryptage).

DÉPLOIEMENT

 COÛT	 ACCOMPAGNEMENT À LA PRISE EN MAIN	 LABELS/CERTIFICATIONS/ CODES DE CONDUITE	 REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> Entre 1 500 € et 3 000 € par an en fonction du package retenu. 	<ul style="list-style-type: none"> Tutoriels, Support client. 	<ul style="list-style-type: none"> Certification ISO 27001. 	<p>À la base spécialisée dans le droit international et dans l'arbitrage, la solution évolue et intègre aujourd'hui le droit du sport et le droit maritime. à venir : le droit social, les droits de l'Homme, la protection de l'environnement, le droit fiscal, etc. Par l'utilisation de GPT-4, c'est le droit anglo-saxon qui ressort naturellement le plus, et Jus Mundi a une compréhension plus fine des concepts anglo-saxons. Jus Mundi investit également pour entraîner leur LLM sur du droit continental avec une vraie représentation du droit civil.</p> <p>L'enjeu est que les outils de la plateforme puissent passer d'un concept civiliste à un concept anglo-saxon sans problème majeur</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



LAMYLINE (LAMY LIAISONS) Plateforme juridique d'IA native



FONCTIONNALITÉS CAS D'USAGE

- Assistant IA conversationnelle et illimité,
- Assistant IA+ dédié à la jurisprudence,
- Analyse IA des documents éditoriaux et du document de l'utilisateur (discussion avec le document, identification des points clés, résumé et traduction),
- Création IA de mémos juridiques sur la base des documents Lamyline + documents de l'utilisateur (disponible en septembre 2025)
- Création et amélioration de documents juridiques de l'utilisateur (contrat, droit des sociétés, etc.) fonction disponible en septembre 2025.
- Toutes les fonctionnalités Lamyline New : recherche classique, veille, modèle d'actes, fiches pratiques, synthèses, calculateurs, etc.), dont toute la doctrine, la documentation officielle (jurisprudence, doctrine administrative, revues Lamy, etc.)



LLM UTILISÉ(S)

- GPT4-o (OpenAI)
Hébergé sur Microsoft Azure
- RAG combinant LLM et les contenus propriétaires Lamy Liaisons et toute la documentation officielle pour fournir des réponses précises et fiables.



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France 	<p>Environnement dédié et sécurisé où l'ensemble des <i>prompts</i> posés est cloisonné, de sorte que les données des utilisateurs ne se répercutent pas dans ChatGPT.</p> <p>L'environnement du <i>chatbot</i> juridique est lui aussi sécurisé et n'interroge pas le web.</p>	<ul style="list-style-type: none"> <i>Cloud</i> privé réservé et sécurisé, Chiffrement en AES 256 bits de toutes les données, Conformité du matériel de cryptographie à la norme FIPS 140-2.



DÉPLOIEMENT

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/CODES DE CONDUITE	REMARQUES/OBSERVATIONS
<ul style="list-style-type: none"> Le recours à la plateforme Lamyline coûte 1 700 € par an, les prix étant dégressifs en fonction du volume de comptes. 	<ul style="list-style-type: none"> Formations, support client. Conférences d'actualités et formations dédiées à l'IA directement intégrées au sein de la plateforme. 	<ul style="list-style-type: none"> NC 	<p>Lamy Liaisons a intégré nativement l'IA et n'a pas fait le choix de créer une solution IA séparée comme peuvent le faire les concurrents GenIA-L ou Lexis+AI par exemple (API LLM).</p> <p>Lamy Liaisons travaille aujourd'hui avec des UX/UI designers afin de comprendre comment réfléchit et s'exprime chaque professionnel du droit utilisateur du système d'intelligence artificielle. Ils analysent l'ensemble des contenus avec l'idée <i>in fine</i> d'améliorer l'expérience utilisateur.</p> <p>Les fonctionnalités IA Lamyline peuvent être directement intégrées dans Microsoft 365.</p> <p>Les données d'entreprise Pappers sont elles-aussi directement intégrées à la plateforme.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



LEGORA

Plateforme d'IAG à destination des professionnels du droit, notamment les avocats



FONCTIONNALITÉS CAS D'USAGE

- Analyse de documents en masse,
- Recherche d'éléments factuels sur un très grand volume de données,
- Analyse de contrats, de pièces, de stratégies et chat avec *sourcing* précis,
- Plateforme multilingue, traduction illimitée,
- Implémentation directe dans Word,
- Assistant de rédaction de conclusions sur la base d'un modèle cabinet,
- Résumé de jurisprudence,
- Recherches juridiques.



LLM UTILISÉ(S)

- **GPT4-o (OpenAI)**
Hébergé sur Microsoft Azure,
- **Claude Sonnet 4 (Anthropic)**
Hébergé chez Amazon Bedrock,
- L'éditeur teste actuellement certains modèles open source.



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> • Union européenne (Microsoft Azure), • Union européenne (AWS). 	<p>La plateforme ne réutilise jamais les données des avocats pour entraînement.</p> <p>Il existe même une exemption pour la revue humaine sur l'infrastructure Microsoft.</p> <p>Legora partage exclusivement les données avec ses sous-traitants (Azure, AWS, Cloudflare, DeepL) dans le but d'héberger et traiter les données strictement nécessaires. Ces prestataires sont soumis à des accords de confidentialité et de traitement des données.</p>	<ul style="list-style-type: none"> • Approche « <i>Zero Trust</i> », • Cloisonnement des environnements de manière étanche, • Chiffrement des données en transit (TLS 1.2 ou 1.3) et au repos (AES-256 certifié FIPS 140-2), • La plateforme offre au client la possibilité de gérer ses propres clés de chiffrement.



DÉPLOIEMENT



SPÉCIFICITÉS OUTIL/SOCIÉTÉ

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<p>Licence nominative standard à partir de 3 000 € HT par an. Les prix sont fortement dégressifs et des tarifs « cabinet » sont proposés sur demande (les tarifs sont établis en fonction du nombre d'utilisateurs et/ou du volume de données traitées).</p>	<p>Accompagnement personnalisé lors de l'intégration incluant des sessions de formation en ligne, des démonstrations et un support technique continu. Un guide détaillé est également fourni pour une prise en main rapide. Legora accompagne ses clients sur place dans leurs bureaux français sur tout le territoire.</p>	<p>Certifications ISO 27001:2022 et SOC 2 Type II.</p>	<p>Les données ne sont pas transférées hors de l'Union européenne. La plateforme se déclare conforme au RGPD.</p> <p>Elle met un point d'honneur à ne pas toucher aux données du cabinet.</p> <p>La plateforme ne pratique pas le <i>fine-tuning</i>.</p> <p>Création de <i>workflows</i> sur-mesure, permettant d'enchaîner plusieurs tâches y compris celles effectuées par des agents autonomes.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES

 <p>LEXBASE INTELLIGENCE & JP INTELLIGENCE (LEXBASE) Chatbot d'IA générative et outils de recherche jurisprudentielle et d'IA générative</p>
<p>FONCTIONNALITÉS CAS D'USAGE</p> <ul style="list-style-type: none"> Recherche juridique et documentaire, Résumé de décisions, chatbot de questions/réponses en droit, Identification de décisions de justice avec une grande précision factuelle Réponses sourcées sur un sujet
<p>LLM UTILISÉ(S)</p> <ul style="list-style-type: none"> LLM open source (confidentiels) Hébergés dans les locaux de Lexbase et sur AWS (France) + agentique Mistral (Mistral AI) pour une partie du conversationnel Hébergé chez Microsoft Azure (Europe).

SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France, hébergements, local chez Lexbase à Paris 16^e et externalisé chez AWS Paris. 	<p>Impossibilité de réutilisation des données par des tiers avec des modèles de langage open source hébergés dans le data center situé dans les locaux de Lexbase et sur AWS Paris.</p> <p>Aucune donnée n'est communiquée à des tiers, à l'exception du prompt saisi par l'utilisateur ainsi que les paragraphes pertinents des sources sélectionnées et envoyées au LLM Mistral (internalisation en cours).</p> <p>Les données des utilisateurs ne sont pas réutilisées pour entraîner les modèles.</p>	<ul style="list-style-type: none"> Protocoles de sécurité « maison » et robustes mis en place dans le data center local ou les <i>clouds</i> utilisés, Souveraineté de l'IA générative par l'installation des algorithmes de Lexbase sur les propres serveurs des clients, Anonymisation des prompts tant que la solution n'est pas totalement internalisée, Serveurs et clusters sont redondés, Mises en place de <i>load balancers</i> pour la charge et de firewalls pour les intrusions, Installation de connexions via SSO ou via des MFA (<i>Multi-Factor Authentication</i>).
DÉPLOIEMENT		
COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/CODES DE CONDUITE
<ul style="list-style-type: none"> L'IA n'existe que dans le pack à 1 395 € HT par an pour un individuel. Pour un cabinet de + de 100 avocats, avec autant de connexions, le prix du pack contenu doctrinal + IA est compris entre 12 000 et 25 000 € HT selon le nombre d'avocats Le pack contenu doctrinal + IA en illimité est de 105 € TTC par an par avocat si l'ordre le souscrit pour tous ses avocats (offre mutualisée ordinaire). 	<p>Formations et conférences en présentiel et à distance ou hybrides pour sensibiliser à l'utilisation de l'IA et son application au droit. Aide à l'hébergement des données directement chez les clients et non sur des clouds propriétaires. Hotline pour les clients aux heures ouvrées.</p>	<ul style="list-style-type: none"> Code de conduite de la legaltech sur l'IA juridique, Charte éthique de l'IA, Charte des données personnelles (Lexbase), Descriptif technique des solutions (Lexbase), Charte de la CEPEJ, Certification iso 27001 AWS et Azure.
REMARQUES/ OBSERVATIONS		
<p>Lexbase met au cœur de son ouvrage le concept de sécurité juridique et, à ce titre, lie dans la plupart des cas ses résultats proposés aux sources du droit en vigueur. Le syllogisme est respecté. Les sources sont intégrées, fiables et accessibles intégralement.</p> <p>Elles sont constituées des ouvrages, des revues, des décisions de justice et des textes de lois.</p> <p>L'actionnaire majoritaire est un avocat en exercice et un membre du directoire est un avocat omis.</p>		

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES

 <p>LEXIS+AI (LEXISNEXIS) Assistant IA adossé au fonds documentaire Lexis+</p>
<p>FONCTIONNALITÉS CAS D'USAGE</p> <ul style="list-style-type: none"> • Recherche conversationnelle, • Assistant rédactionnel, • Résumé et synthèse de jurisprudence (fiches), • Résumé automatique et comparatif des documents, • Résumé de décisions.
<p>LLM UTILISÉ(S)</p> <ul style="list-style-type: none"> • GPT4-o (OpenAI) Hébergé sur Microsoft Azure (France). • Claude 3 Sonnet (Anthropic) Hébergé chez Amazon Bedrock (France) • Infrastructure de Lexis+AI Hébergée sur Microsoft Azure et Amazon AWS

SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> • France et Union européenne, Paris et Francfort (Microsoft), Paris et Dublin (AWS) 	<p>Lexis+AI n'utilise pas les données des clients pour ajuster ou former ses LLM. Les utilisateurs peuvent supprimer à tout moment l'historique des prompts. Les partenaires ne peuvent pas entraîner les modèles personnalisés à partir des données. En outre, la solution utilise des fournisseurs tiers de technologie approuvés par des processus d'examen de sécurité. Tous les modèles déployés par LexisNexis utilisent des connexions dédiées, cryptées et authentifiées qui respectent des normes de sécurité élevées. Toutes les données sont cryptées et restent sous le contrôle de LexisNexis à tout moment.</p>	<p>Toutes les données fournies par les clients sont chiffrées pendant leur transfert via des protocoles de transfert sécurisés utilisant les normes de chiffrement du secteur : le chiffrement au repos utilise l'algorithme AES-256 et s'applique également aux copies principales et de sauvegarde. La rotation des clés est automatique. Seuls les propriétaires opérationnels pré-identifiés ou les processus autorisés ont accès aux clés de chiffrement via un coffre-fort sécurisé.</p> <p>Les données sont transmises en toute sécurité grâce au chiffrement TLS 1.2, norme du secteur, et permettent un chiffrement de 2048 bits. LexisNexis utilise une autorité de certification de confiance qui délivre un certificat numérique TLS pour informer les utilisateurs de la sécurité du service. Les clés cryptographiques sont gérées de manière centralisée selon une méthodologie standard du secteur afin de garantir la mise en place de processus de génération, de distribution, de stockage, d'archivage, de récupération et de destruction. L'accès aux clés cryptographiques est réservé au personnel autorisé.</p> <p>Autres mesures :</p> <ul style="list-style-type: none"> - centre d'opérations et de sécurité, 24h/24 et 7j/7 pour surveiller les systèmes et les applications afin de détecter et de contenir rapidement les événements malveillants potentiels, - tous les problèmes liés à la production sont suivis dans un système de tickets avec une analyse des causes profondes (ACR), - requêtes, prompts et conversations attachés aux documents supprimés au bout de 90 jours, - documents cryptés, chiffrés et supprimés après 10 minutes d'inactivité ; aucun document n'est conservé en fine.

DÉPLOIEMENT	SPÉCIFICITÉS OUTIL/SOCIÉTÉ		
COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/CODES DE CONDUITE	REMARQUES/OBSERVATIONS
<p>Entre 5 000 et 6 000 € pour tous les services (500 € par an pour la base LexisNexis + IAG). L'accès à la base de données seule sans IA sera de 3 000 € par an (260 € par mois).</p>	<ul style="list-style-type: none"> • Formations, • Webinaires, • Support client. 	<p>Certifications AWS de conformité aux normes ISO/IEC :</p> <ul style="list-style-type: none"> • ISO 9001:2015. • ISO/IEC 27017:2015 • ISO/IEC 20000-1:2018 • ISO/IEC 27018:2019 • ISO/IEC 27701:2019 • ISO 22301:2019 • ISO/IEC 27001:2022 <p>Certifications SOC 2 Type II et SOC 3 Type II : Audit LexisNexis réalisé entre le 1er février 2024 et le 31 janvier 2025</p>	<p>Le LLM Mistral AI est en phase de test chez LexisNexis, la société souhaitant éviter les biais de Common Law et revenir à un modèle de droit continental.</p> <p>Pour augmenter la fiabilité des réponses, la société a mis en place une RAG afin d'éviter les hallucinations et les inventions, notamment de jurisprudence.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES


NOTAE AI Outil d'aide à la décision
 FONCTIONNALITÉS CAS D'USAGE <ul style="list-style-type: none"> Retranscriptions et comptes-rendus automatiques à partir d'enregistrements audio, Synthèses basées sur des notes audio, Assistant rédactionnel (pré-rédaction de rapports d'audit, de synthèses de dossier, d'assignation, de mises en demeure, etc. et mise en forme automatique) à des fins d'aide à la décision.
 LLM UTILISÉ(S) <ul style="list-style-type: none"> Claude 3 Sonnet (Anthropic) Hébergé par Google Cloud Vertex AI en Belgique (possibilité de passer par AWS pour un hébergement en France). Sous-traitant « Gladia » pour l'enregistrement des sessions Données hébergées en France (OVH).

SÉCURITÉ ET CONFIDENTIALITÉ

 LIEU D'HÉBERGEMENT DES DONNÉES	 RÉUTILISATION/COMMUNICATION DES DONNÉES	 MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> Allemagne (Hetzner). France (OVH). <p>Possibilité de se fixer sur OVH uniquement.</p>	<ul style="list-style-type: none"> Aucune donnée n'est transmise à l'éditeur du LLM (fine-tuning). Aucune conservation des données input/output des partenaires. L'éditeur du modèle n'a accès à aucune donnée, ni requête du client. 	<ul style="list-style-type: none"> Authentification sécurisée via Clerk, Création d'une BDD séparée pour chaque profession/partenaire et accès à un environnement propre (exemple : cnb.notae.ai), Chiffrement des données en transit entre l'utilisateur, les serveurs et les bases de données (protocole TLS 1.3), Suppression automatique des données et documents sur les serveurs suite à l'action de l'utilisateur, Audits externes réguliers : dernier en date novembre 2024, Tests d'intrusion réguliers (aucune vulnérabilité à risque détectée).

DÉPLOIEMENT

 COÛT	 ACCOMPAGNEMENT À LA PRISE EN MAIN	 LABELS/CERTIFICATION/CODES DE CONDUITE	 REMARQUES/OBSERVATIONS
99 € HT par mois (offre annuelle à 990 € HT par an). Offres dégressives sur mesure. Frais en plus pour de nouvelles fonctionnalités à venir.	<ul style="list-style-type: none"> Démo en visio, Tutoriel vidéo/articles, Accompagnement en phase de test offert, Personnalisation/création/itération sur les règles de rédaction comprises dans l'abonnement, Disponibilité via chat/téléphone (formateur assigné). 	<ul style="list-style-type: none"> Certification ISO 27001 (en cours – audit d'ici la fin du 1er semestre 2025). 	Possibilité de s'adapter aux attentes et de passer par des modèles de Mistral ou autres si souhaité. Contrat de « <i>zero data rétention</i> » (une fois la conversion faite, suppression automatique des données audio/texte chez Gladia). à noter : suppression automatique de l'audio de leurs serveurs dès que la conversion texte est réalisée pour limiter les sources de données. Retranscription écrite uniquement. La technologie « <i>speech-to-text</i> » permet de séparer les voix et de distinguer ainsi les intervenants. Peut se <i>plugger</i> aux Teams des clients.

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



ORDALIE Outil d'aide à la décision



FONCTIONNALITÉS CAS D'USAGE

- Recherche simple ou approfondie d'informations,
- Recherche documentaire dans des sources externes (françaises et européennes), dans le web ou dans les documents internes de l'utilisateur
- Workflows : chaînes d'agents IA entraînés et spécialisés sur des cas d'usage spécifiques : rédaction, analyse multi-documents, chronologie d'un dossier, préparation d'audiences, comparaison de contrats et compilation de commentaires.



LLM UTILISÉ(S)

- Mistral (Mistral AI)**
Hébergé chez Microsoft Azure (France)
- GPT4-o (OpenAI)**
Hébergé sur Microsoft Azure (France)



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/ COMMUNI-CATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France exclusivement, hébergement Scaleway [ISO 27001, 27017, 27018, 9001 et HDS] et Azure. 	<p>Aucune transmission de données à des tiers. L'outil « Legal OS » permet de connecter les archives du cabinet de manière sécurisée. En cas d'import de leurs propres sources, les environnements sont cloisonnés pour éviter tout partage ou entraînement sur les documents utilisateurs. Ordalie n'entraîne pas ses modèles d'IA sur les données de ses utilisateurs mais sur des données en open data.</p>	<ul style="list-style-type: none"> Effacement effectif et définitif des documents sur décision de suppression du client, Aucune copie ou sauvegarde des fichiers après leur suppression, ni par Ordalie ni par ses partenaires qui pourraient être impliqués dans le traitement des documents, Chiffrement systématique de chaque fichier temporairement stocké sur les serveurs avec l'algorithme AES-256, Connexions sécurisées en HTTPS, Aucun salarié non autorisé ne peut avoir accès aux fichiers, Tous les serveurs sont journalisés.



DÉPLOIEMENT

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> Offre Standard/Individuelle à 57€ HT par mois et par utilisateur Offre Vault/Organisation à partir de 115€ HT par mois et par utilisateur. 	<ul style="list-style-type: none"> Présentiel ou à distance, Tutoriels et documentation en ligne, Documentation écrite dédiée. 	<ul style="list-style-type: none"> Certification SOC 2 en cours (Type I ou II à confirmer), Code de conduite de la legaltech sur l'IA juridique. 	<p>Modèles d'IA développés spécialement par Ordalie et entraînés exclusivement sur du droit français. Certains modèles sont publiés en open source. Les seuls LLM non open source sont utilisés uniquement à la toute fin d'un process, soit pour rédiger un document complet ou la réponse finale. Les espaces entre chaque utilisateur/cabinets sont cloisonnés sur le serveur d'Ordalie. Nous proposons aussi des serveurs dédiés en fonction des besoins du client. Les seuls développeurs salariés à temps plein d'Ordalie travaillent sur les fonctionnalités liées à la mise en ligne de documents peuvent accéder aux fichiers dont le traitement a abouti à une erreur, uniquement à des fins de correction. Les cabinets peuvent notifier à Ordalie leur refus qu'il soit procédé à la correction d'erreurs et/ou leur demander de supprimer les fichiers concernés. Dans tous les cas, l'utilisation du fichier est strictement limitée à ces salariés autorisés et à la correction. Les copies des fichiers créées à des fins de correction sont irrémédiablement détruites 24 heures après la survenance de l'erreur. En partenariat avec le Barreau de Paris.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES


SEPTEO BRAIN (SEPTEO)
 FONCTIONNALITÉS CAS D'USAGE <ul style="list-style-type: none"> Recherches en langage naturel pour étayer une base documentaire, Extraction de données qualifiées, Relève automatique d'informations dans les documents, y compris par océrisation, Création de dossiers par importation automatique, potentiellement des données des comptes-rendus, échanges, enregistrements, rendez-vous à venir, etc., des avocats utilisant Teams, Analyse jurisprudentielle qui irait interroger des données échangées via le RPVA et qui sont renseignées dans la plateforme, Contrôle, correction et classement automatiques de la donnée/d'un fichier, Identification de notions juridiques, contextualisation et renvoi vers Legifrance, Questions/réponses, Génération de résumés Génération de contenus et de clauses, Tableaux comparatifs et synthèse de plusieurs documents.
 LLM UTILISÉ(S) <ul style="list-style-type: none"> LLM open source, dont Mistral (Mistral AI)
Hébergé chez Microsoft Azure



SÉCURITÉ ET CONFIDENTIALITÉ

 LIEU D'HÉBERGEMENT DES DONNÉES	 RÉUTILISATION/ COMMUNICATION DES DONNÉES	 MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France, hébergeur français. 	<p>L'outil n'utilise pas les données pour s'entraîner davantage. Septeo a mis en place la RAG combinant les forces des modèles d'intelligence artificielle (IA) basés sur l'extraction et sur la génération. L'IA RAG fournit des résultats précis qui tirent le meilleur parti des connaissances préexistantes et peut également traiter et consolider ces connaissances pour créer des réponses, des instructions ou des explications uniques. Celles-ci sont adaptées au contexte et rédigées dans un langage proche de celui des humains.</p>	<ul style="list-style-type: none"> Analyse du code par des outils de SCA et de DAST, Tests de surface externes continus par l'équipe Red Team Septeo, Tests d'intrusion au minimum annuels par l'équipe Red Team Septeo, Sensibilisations spécifiques des développeurs.



DÉPLOIEMENT

 COÛT	 ACCOMPAGNEMENT À LA PRISE EN MAIN	 LABELS/CERTIFICATION/ CODES DE CONDUITE	 REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> 60 € par mois (+500 € pour l'installation dans une entité). 	<ul style="list-style-type: none"> Formations, Accompagnement personnalisé, Support technique. 	<ul style="list-style-type: none"> Certification ISO 27001. 	<p>Septeo prétend être en avance sur ses concurrents concernant le chantier de la contextualisation et du raisonnement « comme un avocat » en étant capable de lui faire des suggestions et lui proposer des choix au sein de ses dossiers.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES

 <p>CEDIE Application bureau traitant localement les données</p>
 <p>FONCTIONNALITÉS CAS D'USAGE</p> <ul style="list-style-type: none"> Organisation, extraction, recherches, résumé de documents.
 <p>LLM UTILISÉ(S)</p> <ul style="list-style-type: none"> Small Language Models (SLMs) exécutés localement sur le poste utilisateur.

SÉCURITÉ ET CONFIDENTIALITÉ

 LIEU D'HÉBERGEMENT DES DONNÉES	 RÉUTILISATION/ COMMUNICATION DES DONNÉES	 MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> En local, directement sur la machine de l'utilisateur. 	<p>Aucune réutilisation possible de la part de Cedie, toutes les données sont hébergées localement sur la machine de l'utilisateur. Cedie n'accède à aucune donnée.</p>	<ul style="list-style-type: none"> Installation de la solution exclusivement On-Device entièrement hors-ligne ; de ce fait, il n'est pas obligatoire de disposer d'une connexion Internet pour interagir avec les données via l'outil.

DÉPLOIEMENT

SPÉCIFICITÉS OUTIL/SOCIÉTÉ

 COÛT	 ACCOMPAGNEMENT À LA PRISE EN MAIN	 LABELS/CERTIFICATION/ CODES DE CONDUITE	 REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> Tarifs non disponibles à présent, l'outil étant encore en version de test avec un nombre d'utilisateurs restreint. 	<ul style="list-style-type: none"> Formations, Tutoriels, Support client dédié. 	<ul style="list-style-type: none"> N/C 	<p>Cedie est la seule application sur le marché qui permet d'exécuter des modèles d'IA localement, sans aucun risque de violation du secret professionnel. Toutes les données des utilisateurs restent stockées sur leurs machines.</p>

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES



PREDICTICE



FONCTIONNALITÉS CAS D'USAGE

- Recherche et analyse de l'information juridique (jurisprudence, textes de loi, actualité),
- Accès aux données légales et financières des entreprises,
- Assistant : outil conversationnel,
- Fonctionnalités d'analyse, de comparaison, de traduction et de résumé de documents.



LLM UTILISÉ(S)

GPT4-o (OpenAI)
Hébergé sur Microsoft Azure
(Union européenne)

Claude 3 Sonnet (Anthropic), Hébergé aux États-Unis



SÉCURITÉ ET CONFIDENTIALITÉ

LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/ COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> France et Allemagne (OVH). 	<p>Predictice déclare n'utiliser aucun contenu traité pour entraîner les modèles et de fonctionner via un RAG sécurisé, pour un respect strict annoncé du secret professionnel et de la confidentialité des données utilisateurs.</p>	<ul style="list-style-type: none"> Authentification des utilisateurs via un mot de passe, Accords de confidentialité auprès du personnel, L'ensemble des actions réalisées sur les serveurs et sur le code source de Predictice est contrôlé, Chiffrement des données en transit via le protocole TLS 1.2, et la transmission de chaque donnée utilisateur est chiffrée de bout-en-bout par le protocole HTTPS, Sauvegardes quotidiennes des données et réplication des données dans plusieurs datacenters, Toutes les politiques de sécurité et de gestion des données chez Predictice sont centralisées dans leur « Trust Center » : https://trust.predictice.com. (l'accès peut être demandé).



DÉPLOIEMENT



SPÉCIFICITÉS OUTIL/SOCIÉTÉ

COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> Abonnements dépendant du nombre d'utilisateur au sein de la structure. 	<ul style="list-style-type: none"> Formations, Ateliers pratiques, Support client réactif. 	<ul style="list-style-type: none"> Certifications ISO 27001 et de mise en conformité SOC 2 Type 2 en cours. Certifications ISO27001, SOC 2 Type II, ISO27018, EU-US Privacy Shield Framework, Gold CSA STAR, PCI DSS Certification pour le système d'authentification utilisé par Predictice. 	<ul style="list-style-type: none"> Procédures de conservation et de suppression des données conformes aux meilleures pratiques, Données clients supprimées à la fin de la relation contractuelle, Accords de confidentialité signés par tous les collaborateurs et prestataires.

COMPARATIF DES SOLUTIONS D'IA JURIDIQUES AUDITÉES

 <p>HAIKU IA juridique</p>
<p>FONCTIONNALITÉS CAS D'USAGE</p> <ul style="list-style-type: none"> Recherche juridique en langage naturel sur les données internes du cabinet et bases jurisprudentielles/légales, Analysé mono et multi-documentaire : synthèse, analyse de risques, délais, chronologie, identification des acteurs/sources, Rédaction libre & Capacité à générer des documents de plus de 30 pages, en reprenant le style d'écriture d'un document fourni en modèle, Extraction massive d'informations sur plusieurs centaines de documents.
<p>LLM UTILISÉ(S)</p> <ul style="list-style-type: none"> Combinaison de LLMs open source et propriétaires. Hébergés chez Microsoft Azure (France et Suède), Google Cloud Platform (France et Belgique).

SÉCURITÉ ET CONFIDENTIALITÉ

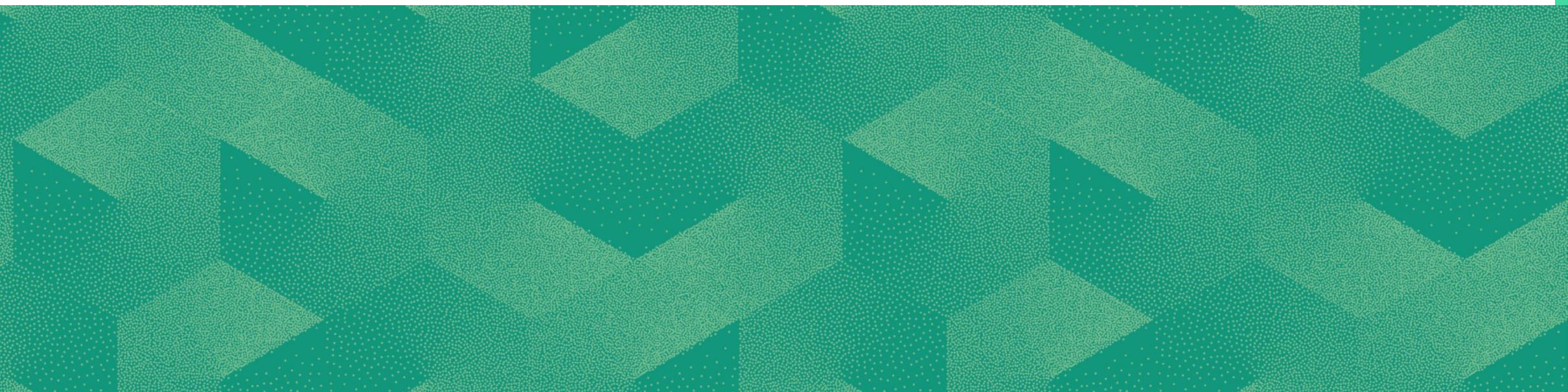
LIEU D'HÉBERGEMENT DES DONNÉES	RÉUTILISATION/ COMMUNICATION DES DONNÉES	MESURES DE SÉCURITÉ
<ul style="list-style-type: none"> Google Cloud Platform (France et Belgique). 	<p>Aucune réutilisation et aucun accès des données par un tiers. Les données restent sur le sol européen. Le client reste l'unique propriétaire de ses données et des données qu'il produit avec Haiku. Aucun LLM ne sauvegarde ou ne réutilise les données, les données qui y transitent sont éphémères.</p>	<ul style="list-style-type: none"> Chiffrement AES256 de toutes les données au repos, chiffrement HTTPS-TLS 1.3 en transit, Authentification via OAuth 2.0, contrôle d'accès sur principe du moindre privilège (ex : les employés de Haiku n'ont accès à aucune donnée appartenant aux clients), Rotation régulière des clés de sécurité, Clé de chiffrement possédée par Haiku mais possibilité prochaine de laisser le client être seul propriétaire de sa clé.

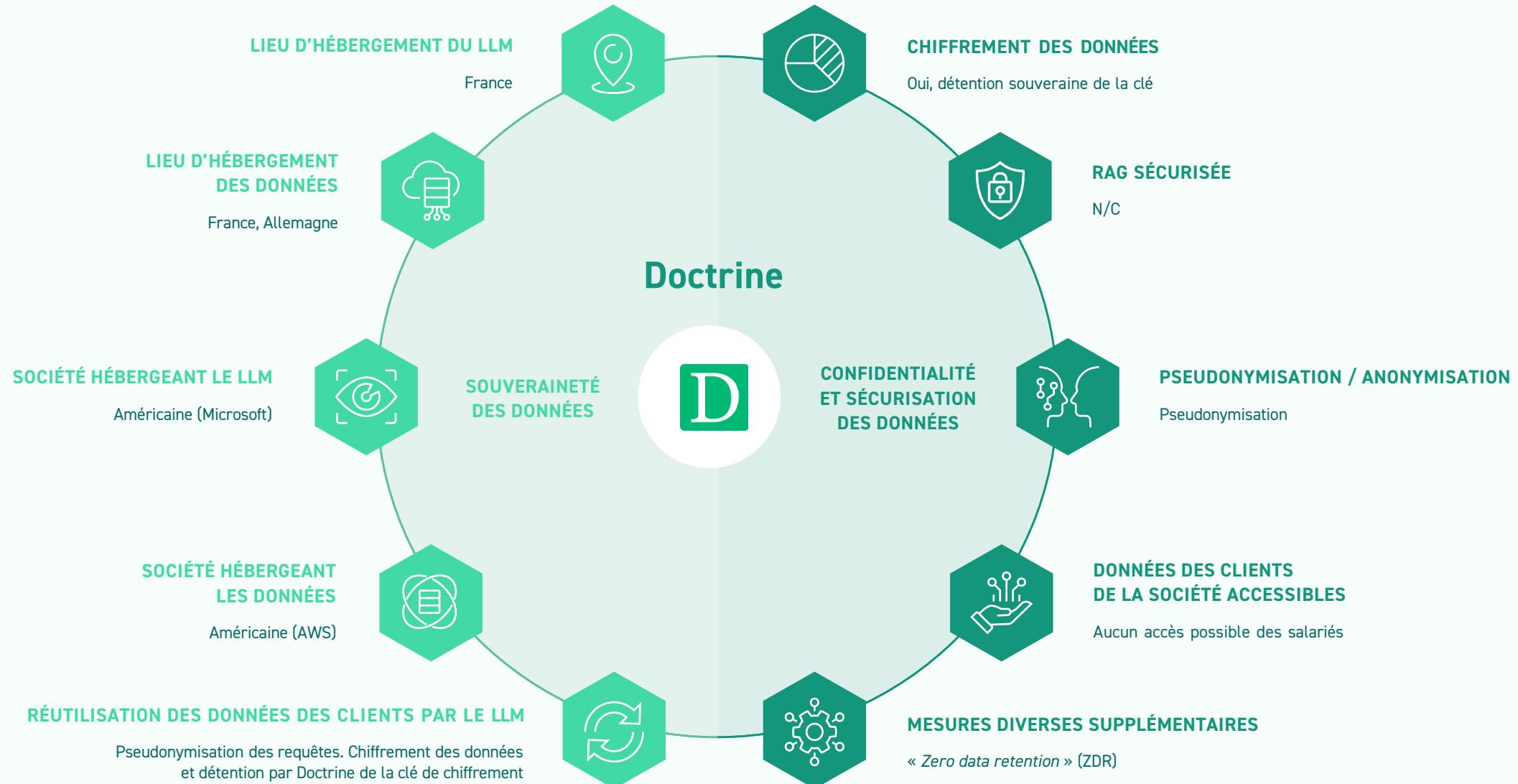
DÉPLOIEMENT

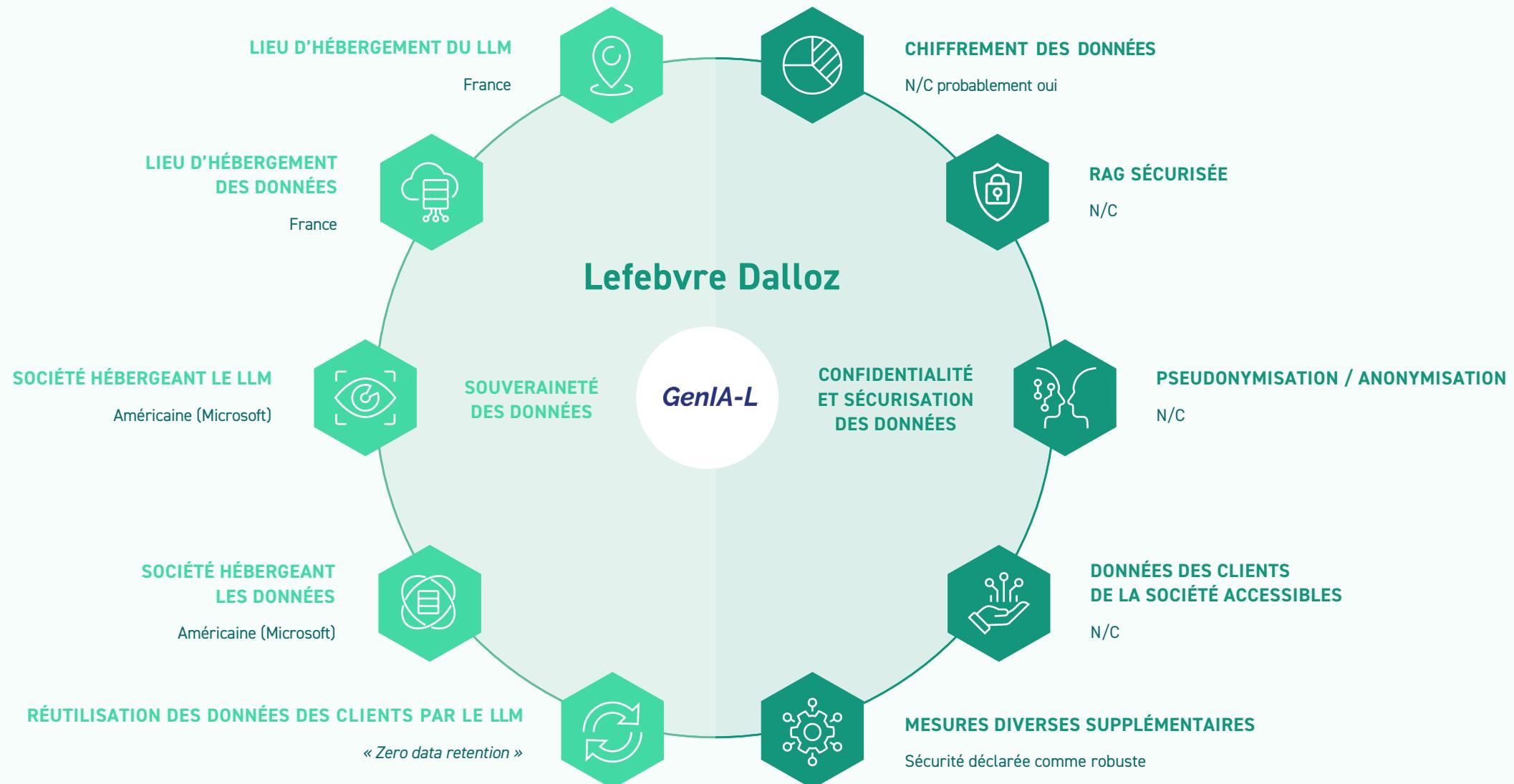
COÛT	ACCOMPAGNEMENT À LA PRISE EN MAIN	LABELS/CERTIFICATION/ CODES DE CONDUITE	REMARQUES/ OBSERVATIONS
<ul style="list-style-type: none"> À partir de 95 €/mois/utilisateur + 6 € par tranche de 10 Go pour la connexion à une GED. 	<ul style="list-style-type: none"> Formation individuelle et/ou collective incluse dans l'abonnement. Tutoriels & support client dédié. 	<ul style="list-style-type: none"> Certification ISO 27001 en cours. Code de conduite sur l'IA générative. 	<ul style="list-style-type: none"> Haiku a noué des partenariats officiels avec les principaux éditeurs de GED, notamment Secib (Septeo) et Xelya (Diapaz). Grâce à ces partenariats, Haiku est en mesure de se connecter à la GED du client, sans configuration complexe, et de valoriser la base documentaire d'un cabinet en quelques jours.

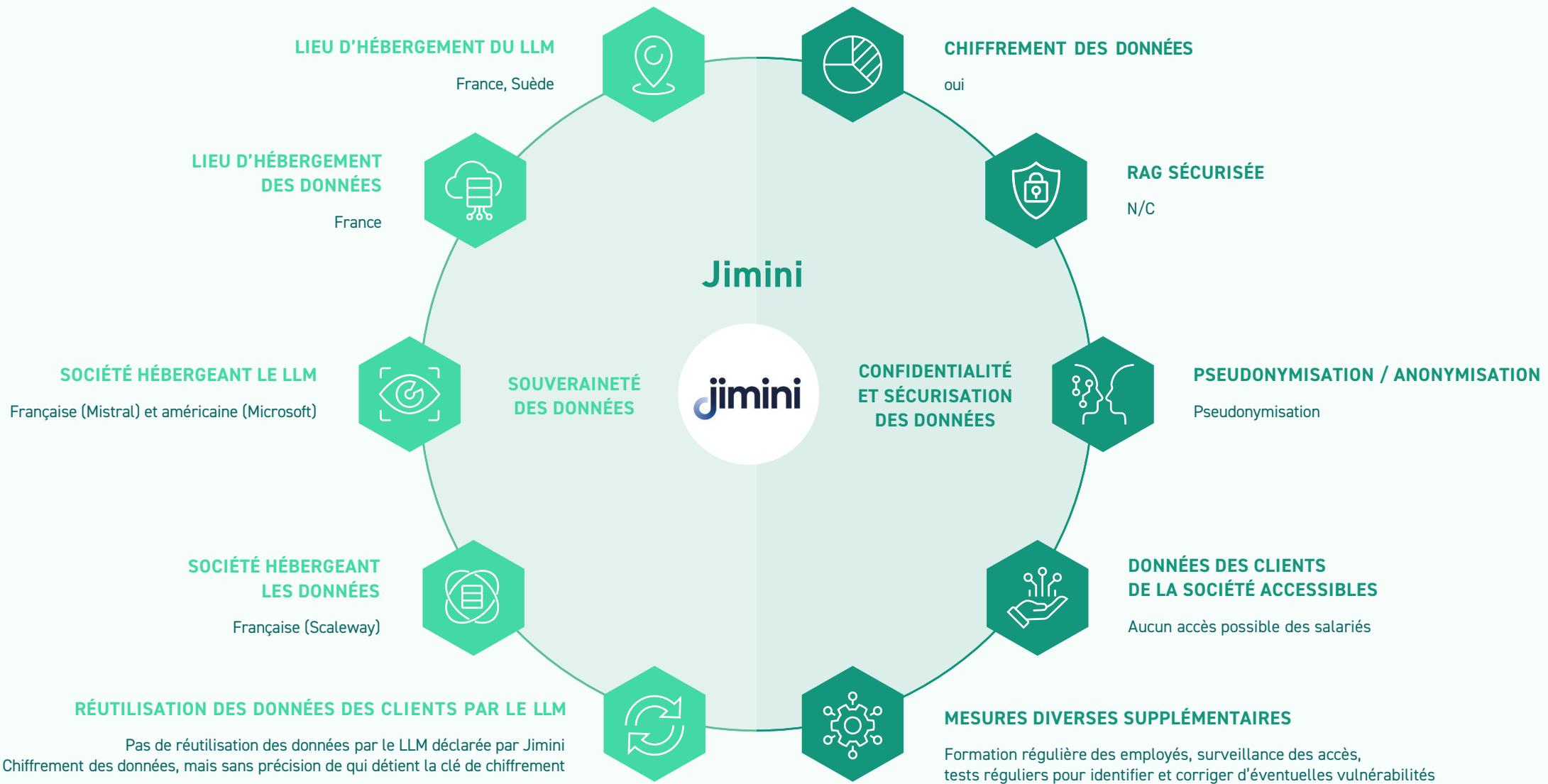
SYNTHÈSE

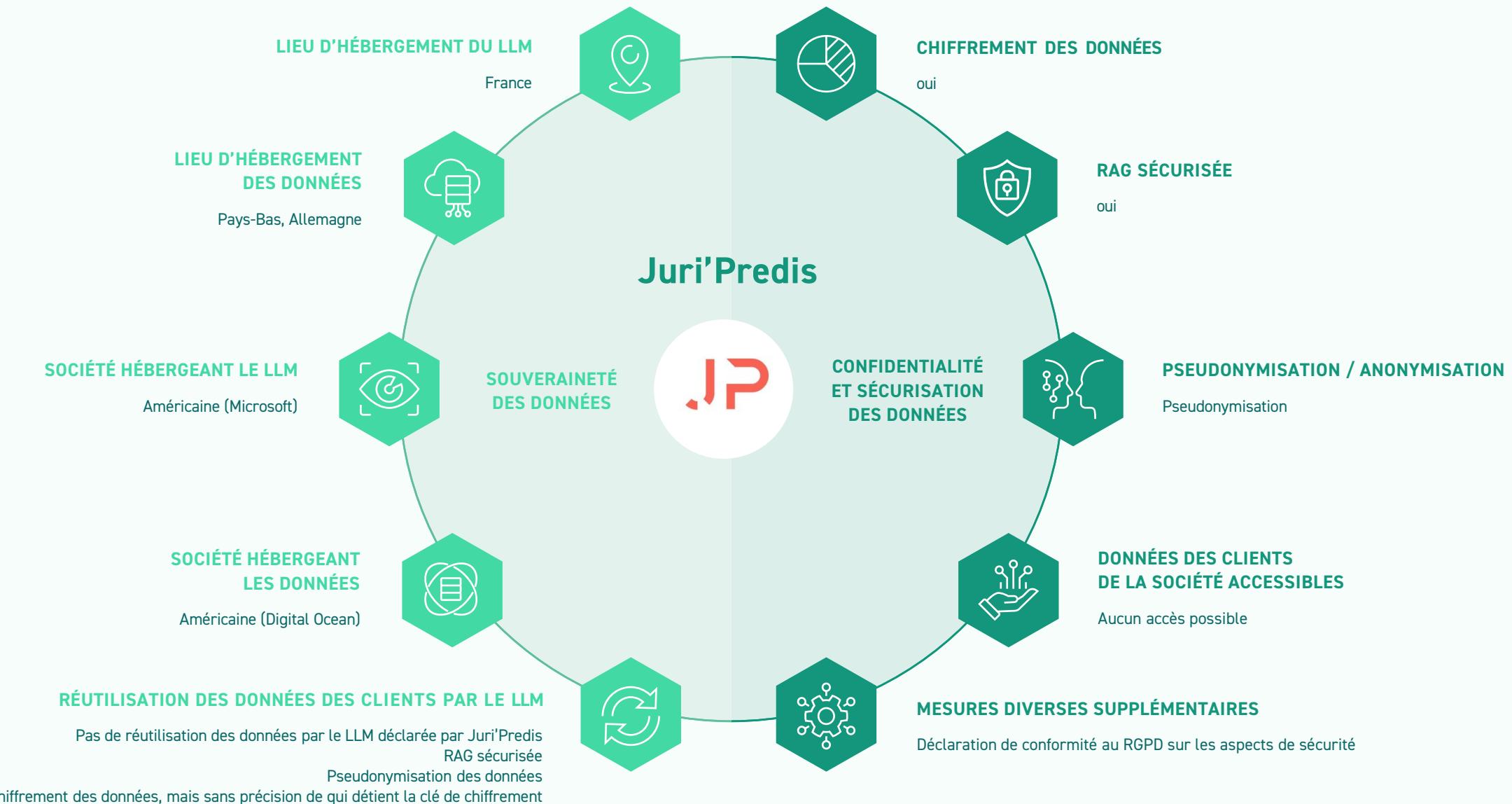
(sous couvert d'évolution et en fonction des éléments déclarés, trouvés et/ou transmis par les sociétés)

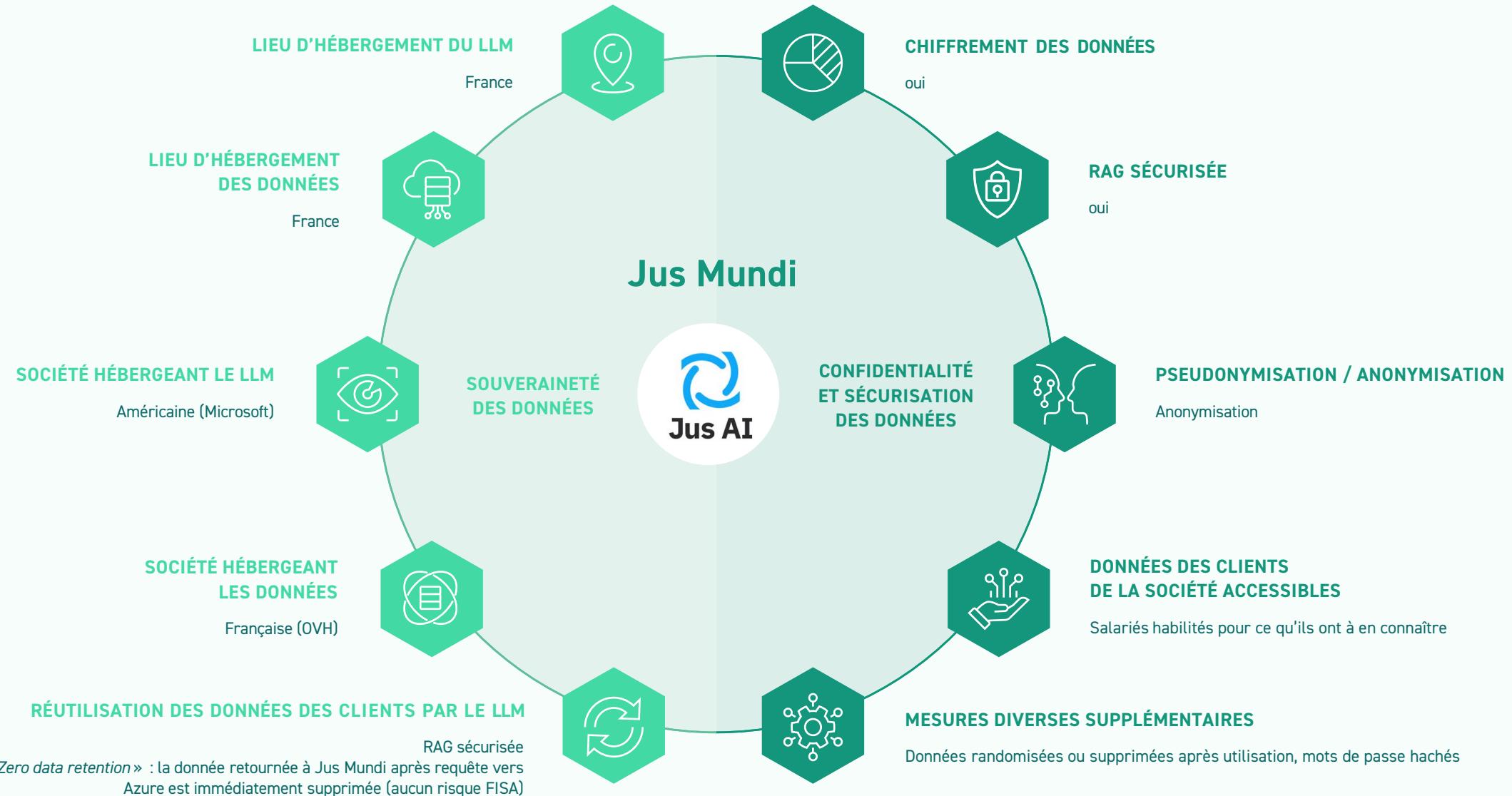


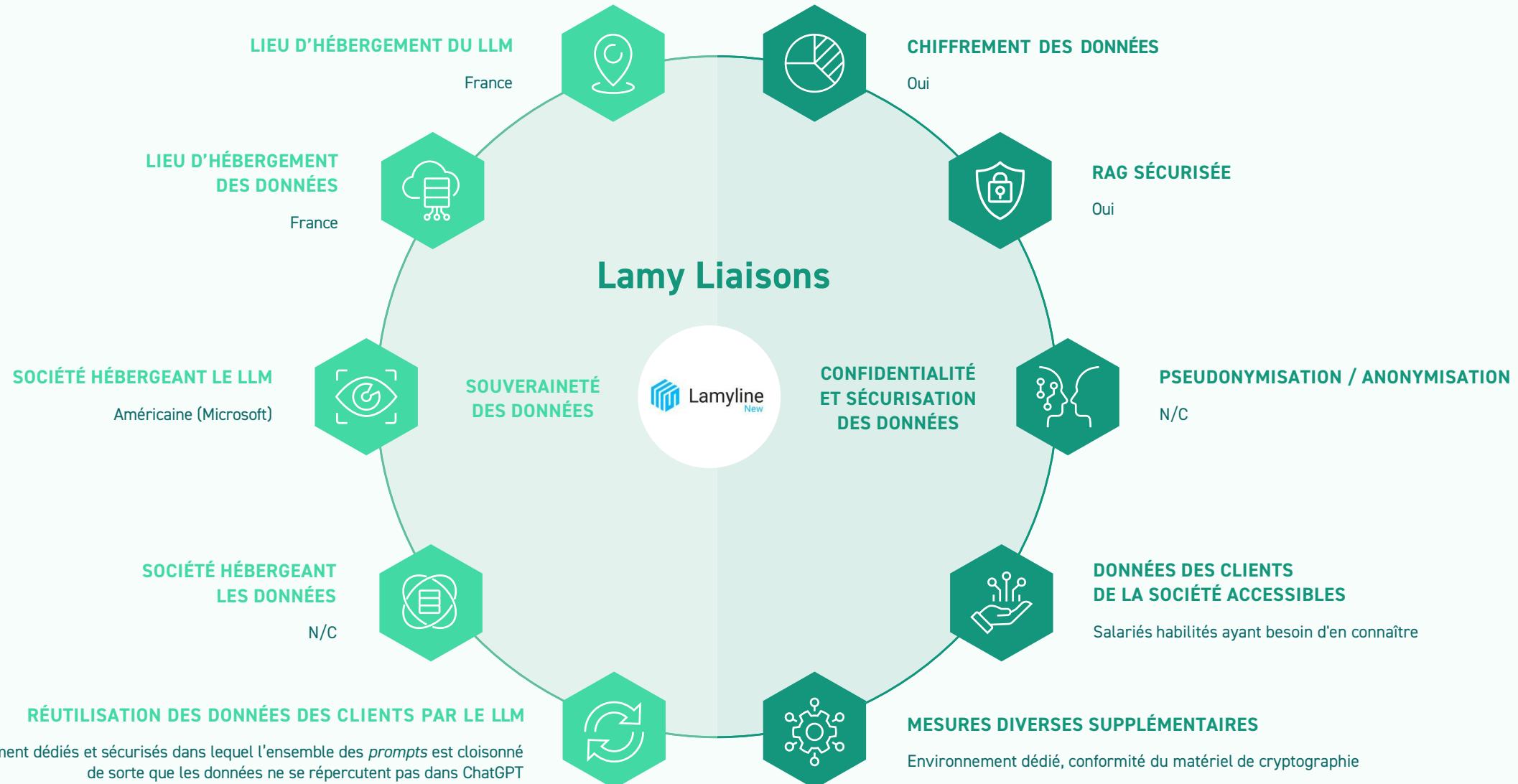




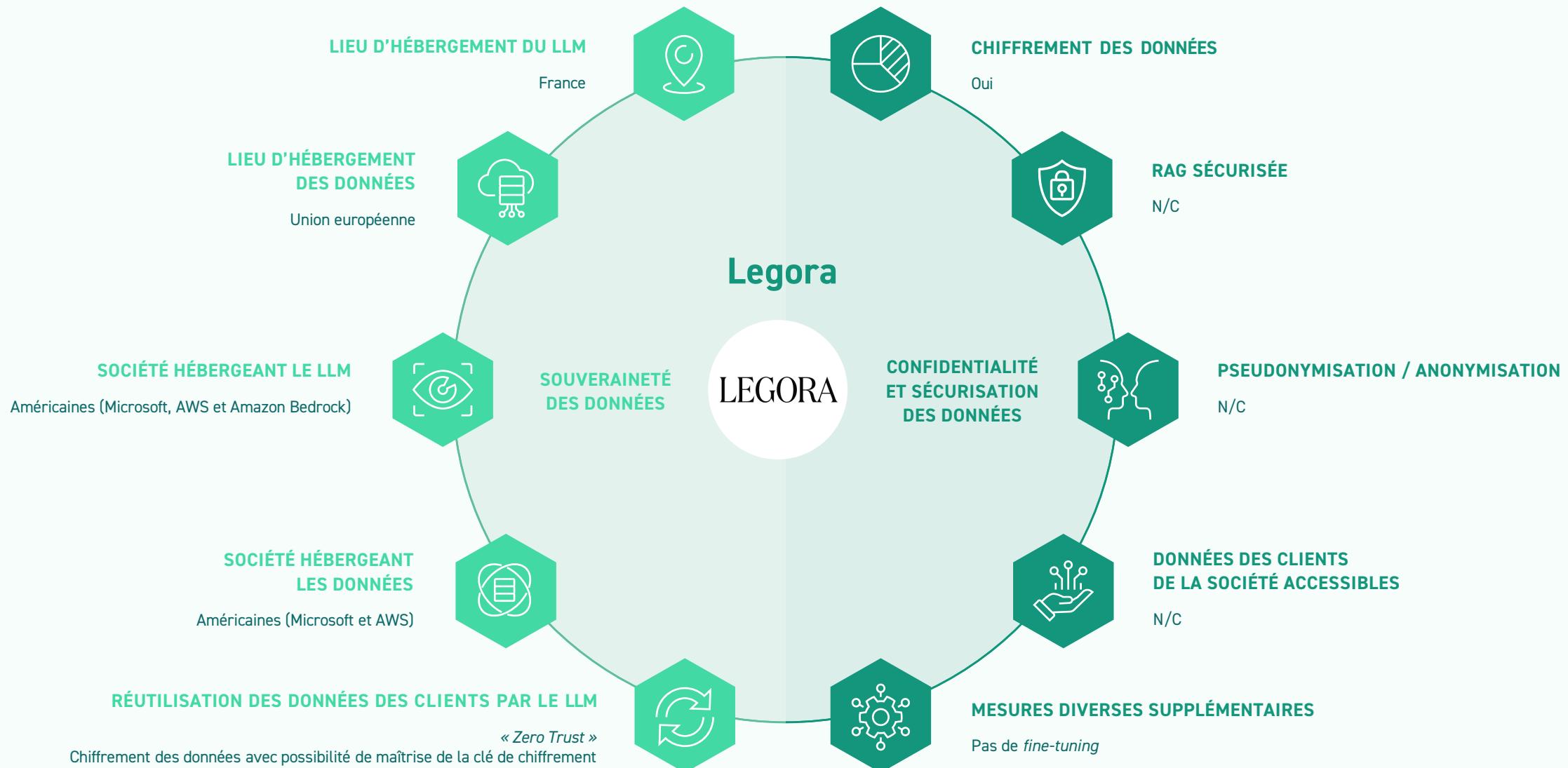


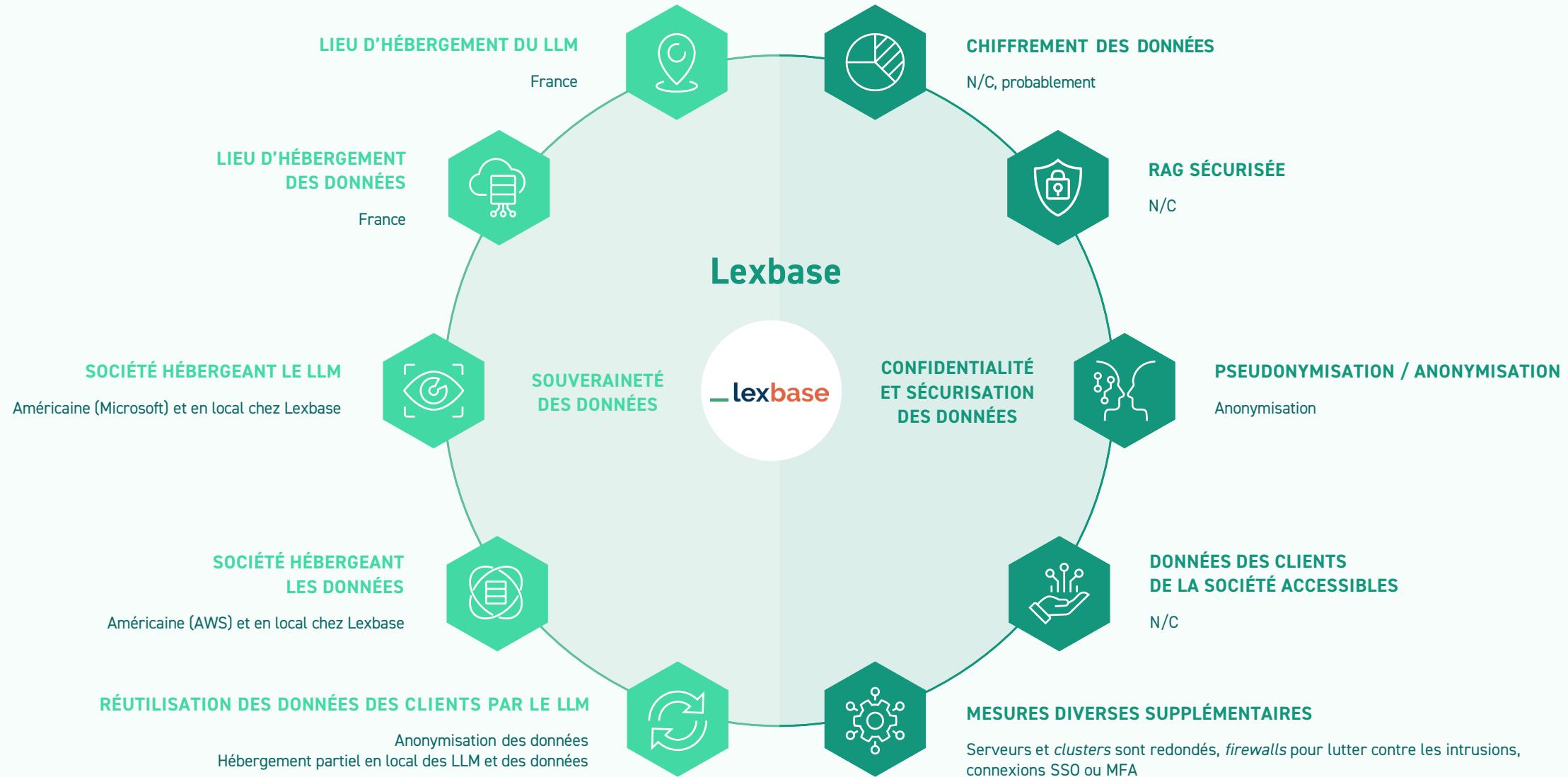




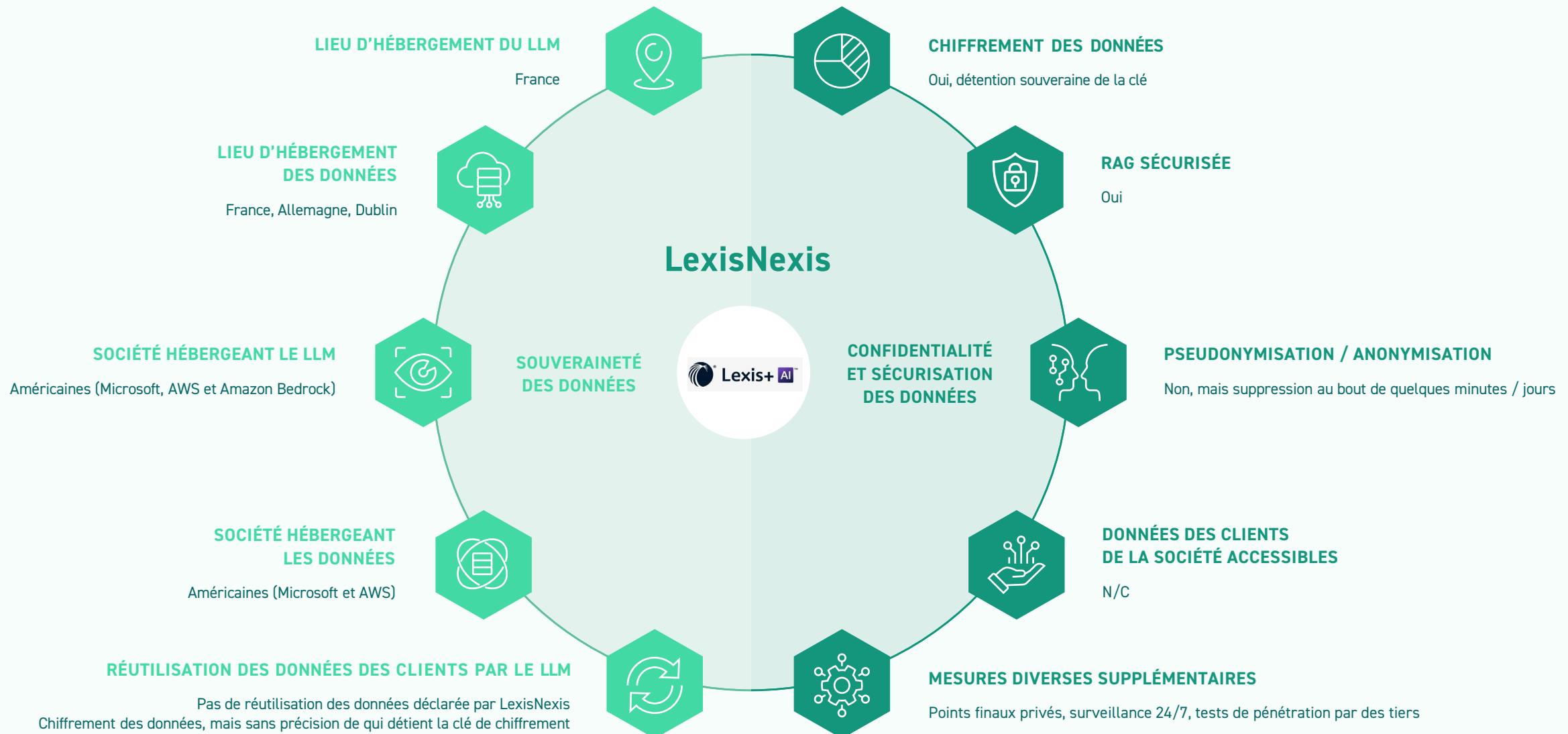


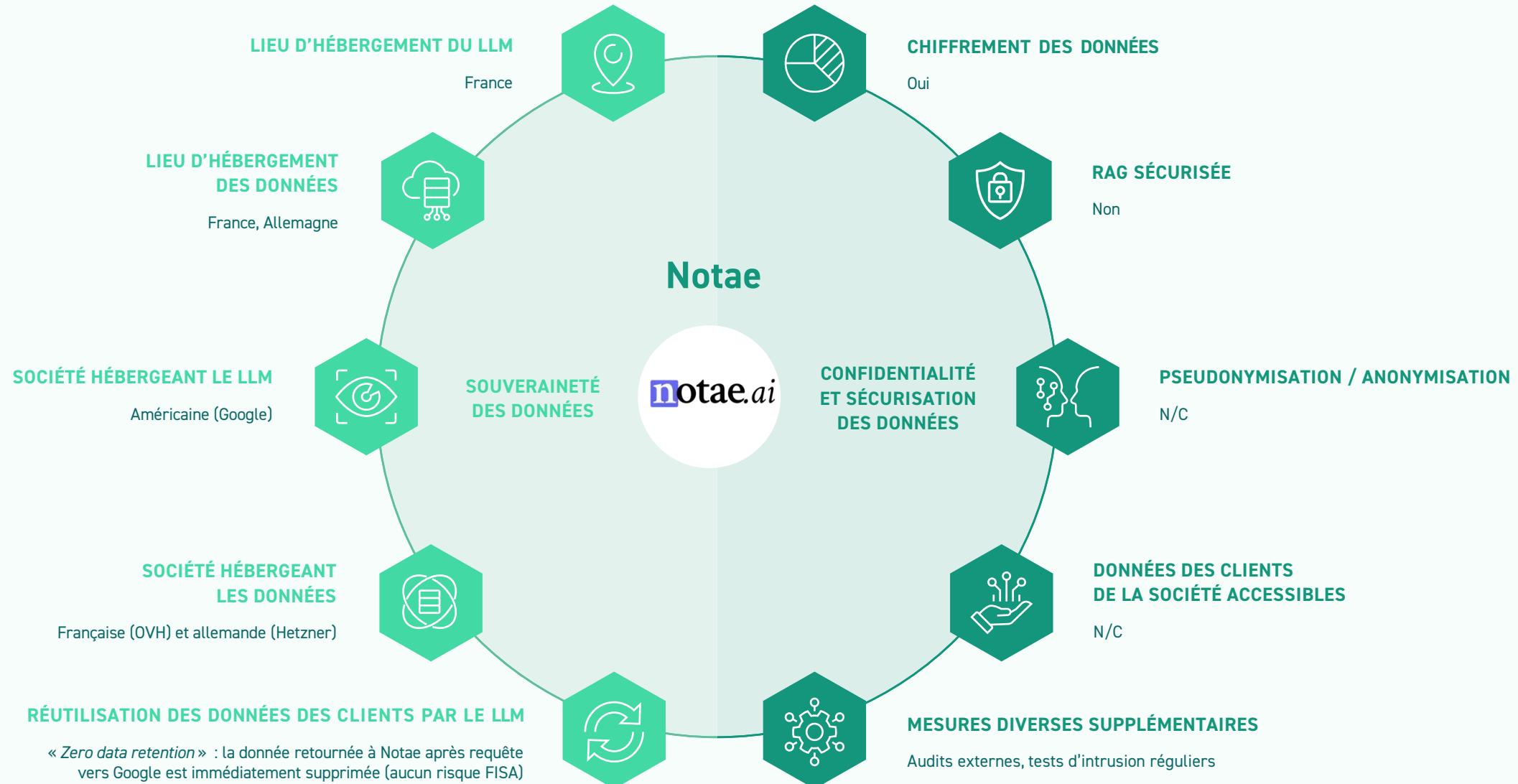
RAG et environnement dédiés et sécurisés dans lequel l'ensemble des *prompts* est cloisonné de sorte que les données ne se répercutent pas dans ChatGPT



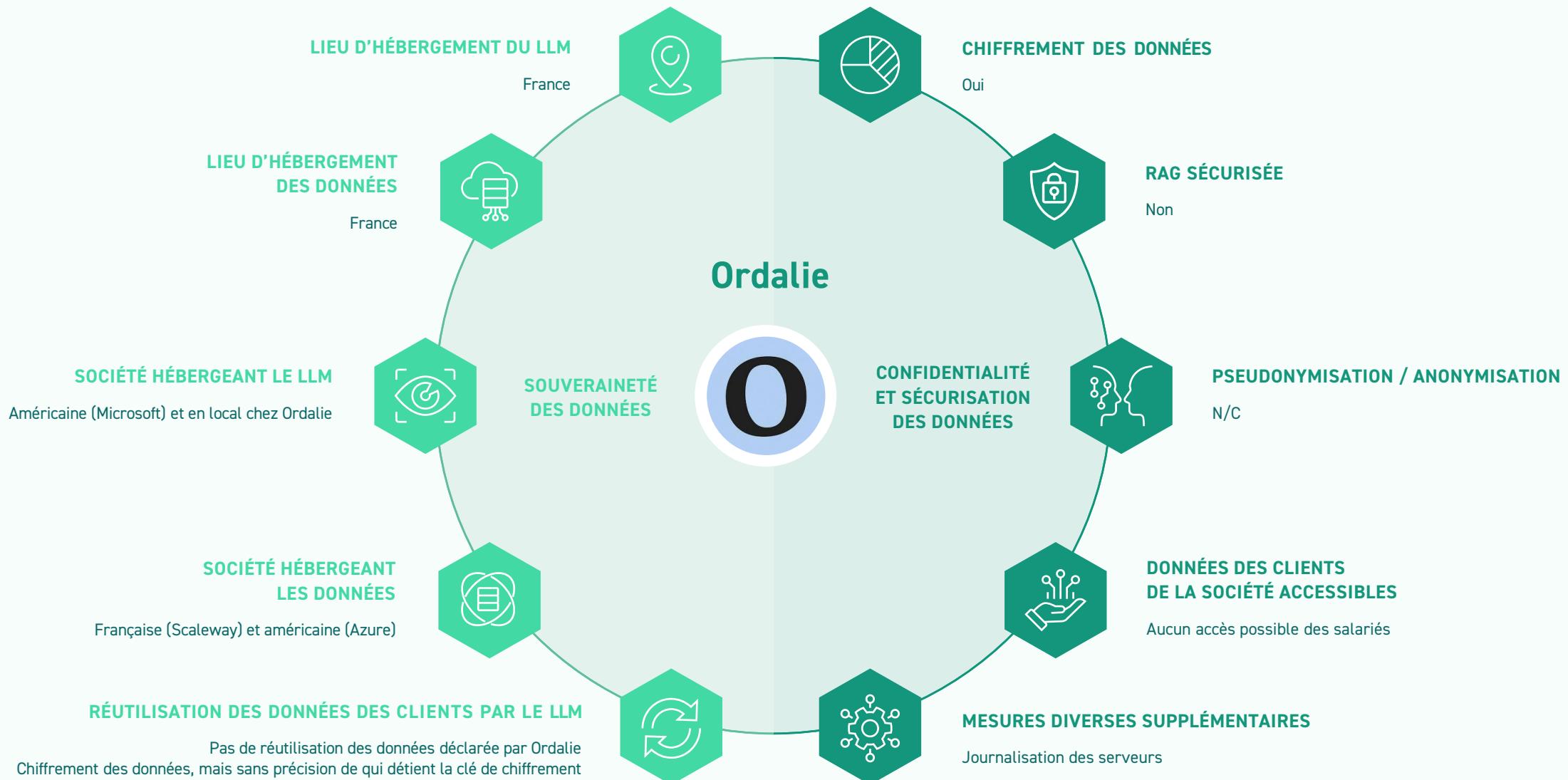


SYNTHÈSES

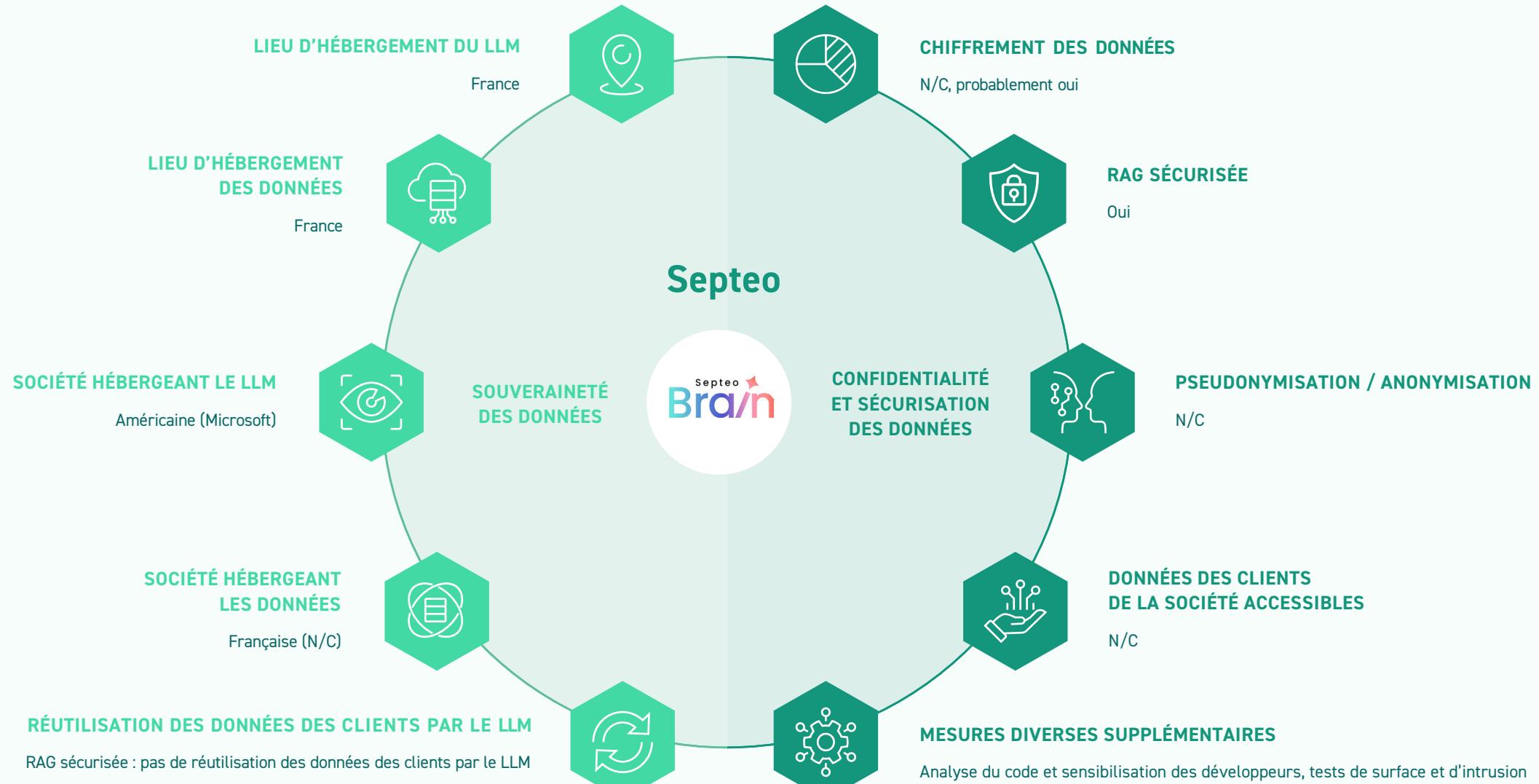


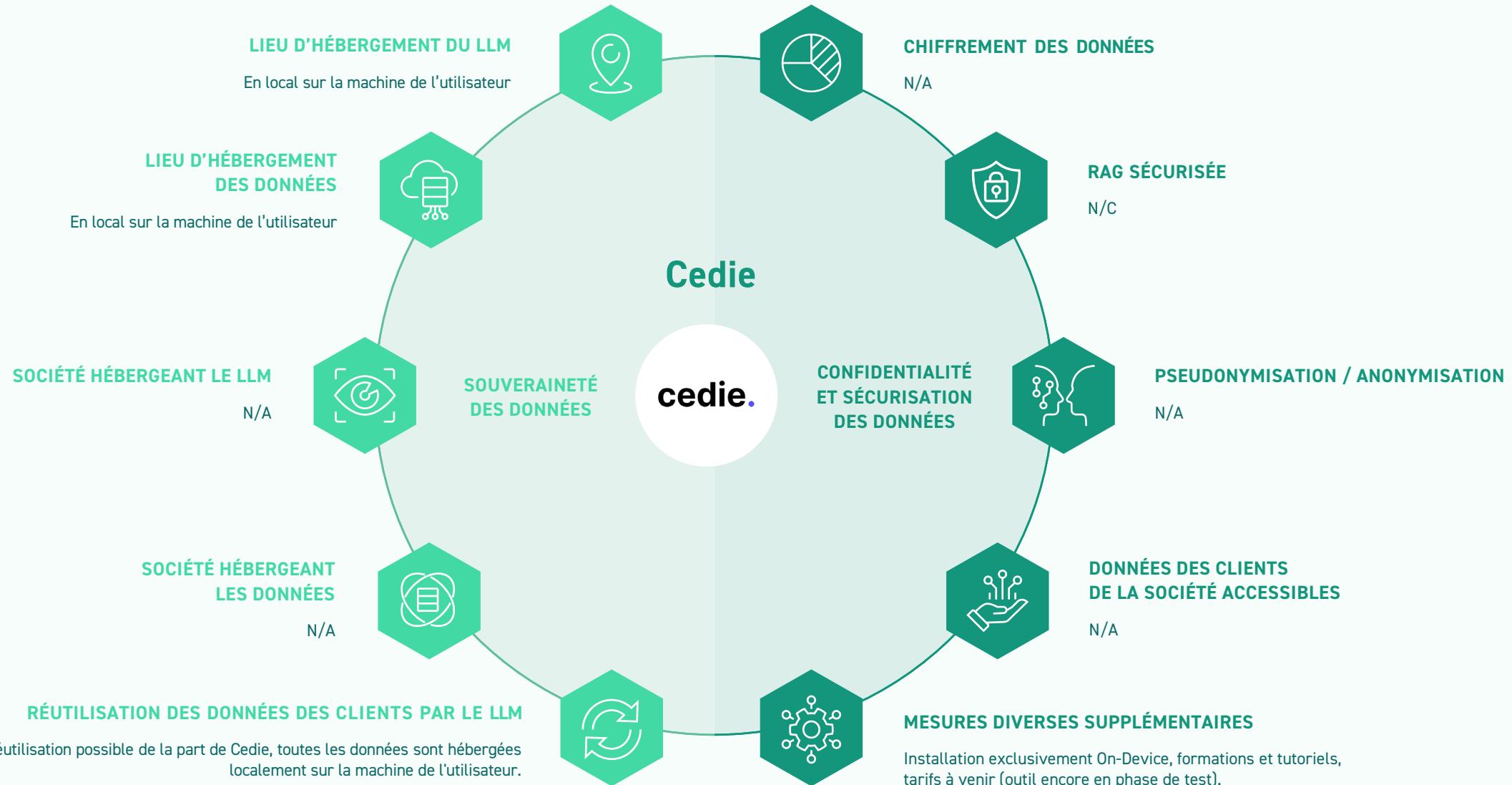


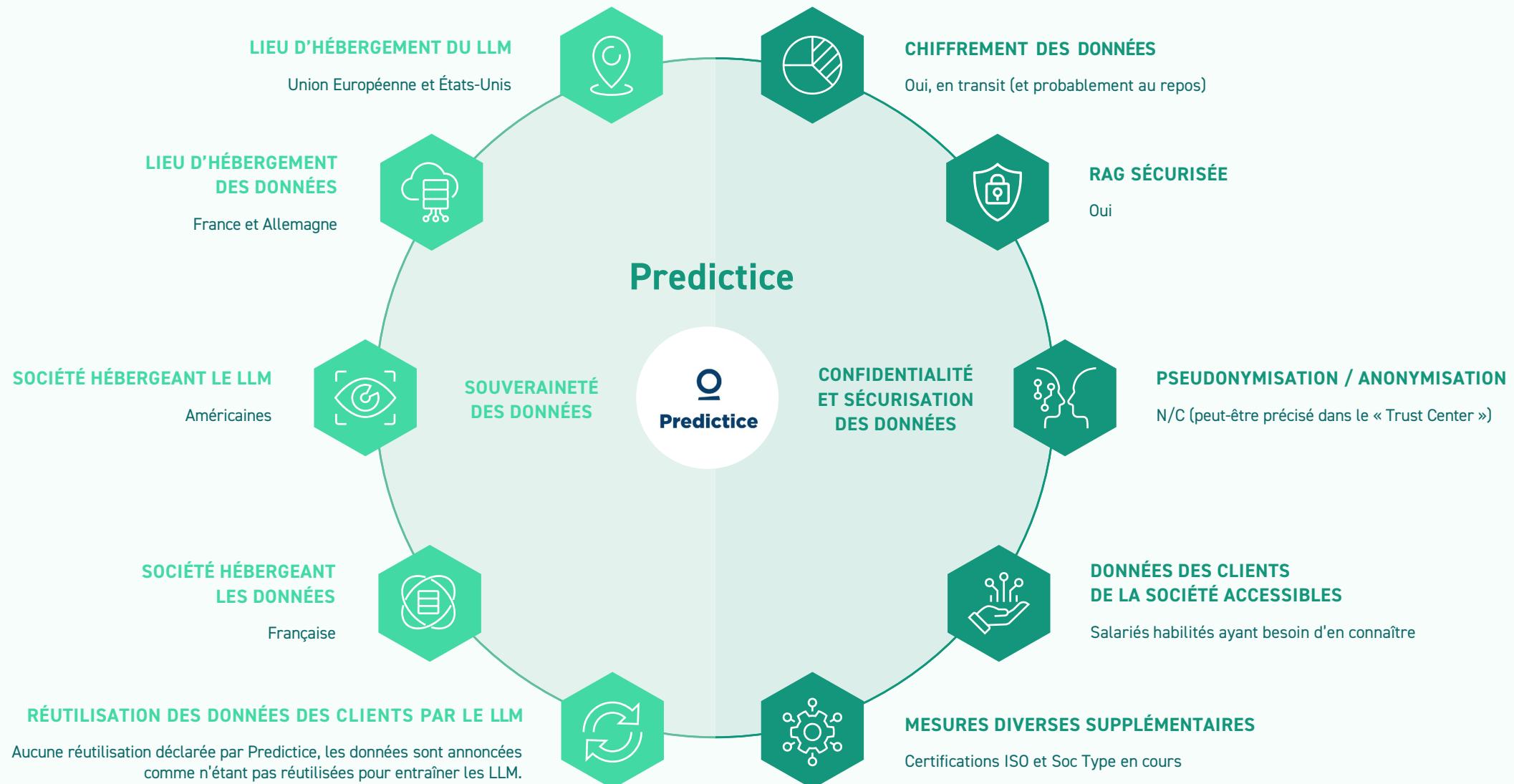
SYNTHÈSES

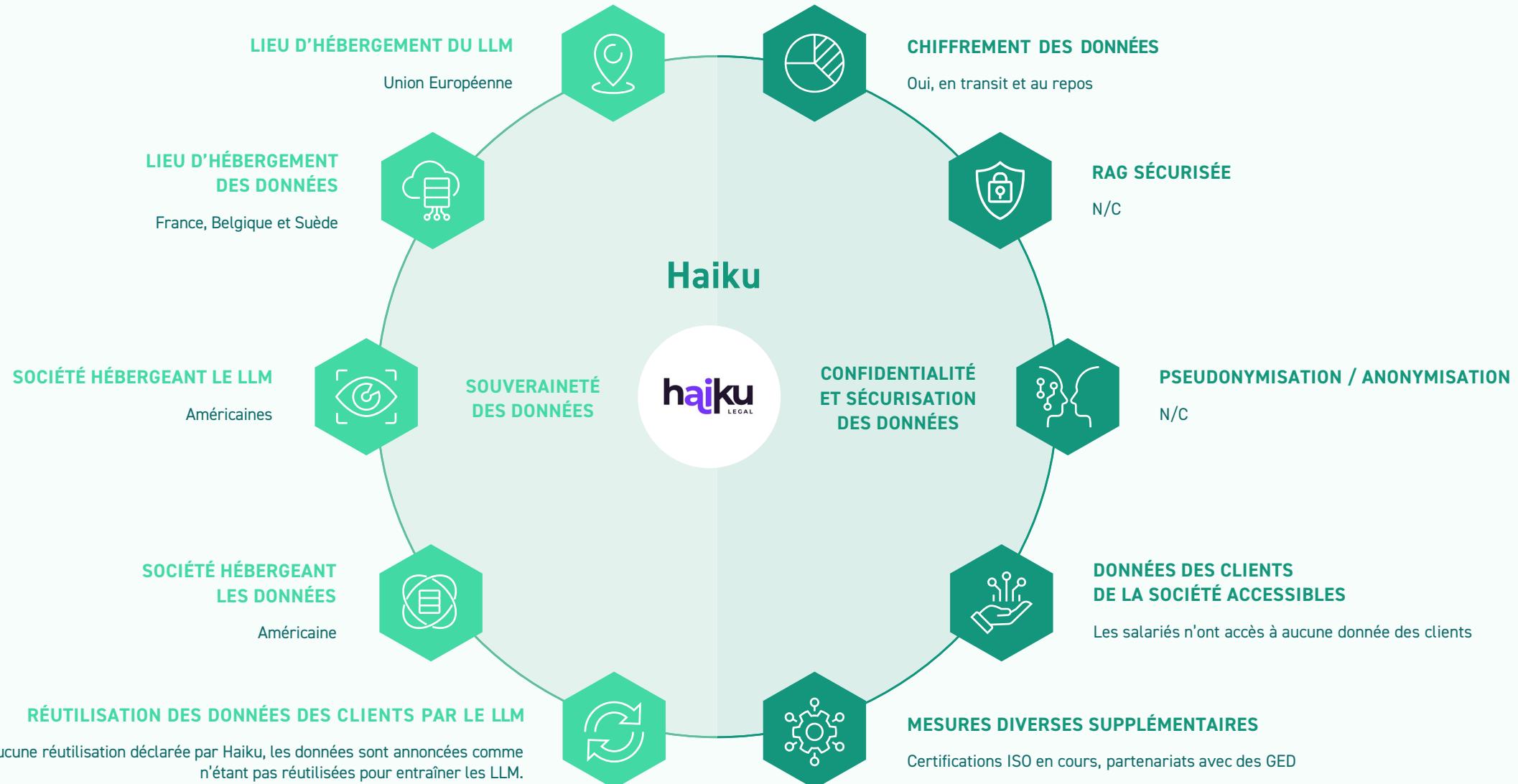


SYNTHÈSES











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

Sur les réseaux sociaux



Au siège

180 boulevard Haussmann - 75008 Paris