Stratégie numérique de l'Ordre des avocats du Barreau de Paris
« *Vers un barreau souverain* »

CONFIDENTIALITÉ : Public

MOTS CLÉS : Stratégie numérique, souveraineté, cloud, intelligence artificielle, RGPD, cybersécurité, conformité.

RAPPORTEUR(S) :

Nicolas Mahassen, Raphaël Dana, MCO

Julia Nioré, Directrice Stratégie Numérique

BÂTONNIER ET VICE-BÂTONNIÈRE EN EXERCICE :

Louis DEGOS et Carine DENOIT-BENTEUX

DATE DE LA REDACTION :

07/05/2026

DATE DE PRESENTATION AU CONSEIL :

19/05/2026

RESUME :

Le numérique constitue désormais un enjeu structurant pour la profession d'avocat, à l'intersection de considérations de souveraineté, de compétitivité et d'indépendance.

Dans un environnement marqué par l'accélération des transformations technologiques, par l'émergence de nouveaux acteurs et par une dépendance accrue à des infrastructures majoritairement extra-européennes, le Barreau de Paris, premier barreau d'Europe et composante essentielle de l'État de droit, est conduit à définir une stratégie numérique à la fois ambitieuse, cohérente et pragmatique.

Il ne s'agit pas, dans cette perspective, de rompre brutalement avec les usages existants, ni d'adopter une approche de principe qui conduirait à exclure certaines solutions technologiques. L'enjeu consiste davantage à organiser, dans la durée, une montée en puissance progressive de la maîtrise des outils, des données et des dépendances.

La stratégie proposée vise ainsi à positionner l'Ordre comme un acteur de référence, capable d'accompagner les avocats dans leurs usages, tout en contribuant à structurer un cadre de confiance et à orienter, de manière mesurée, les évolutions technologiques de la profession.

Parallèlement, le renforcement des exigences en matière de cybersécurité et l'accompagnement des cabinets dans leurs obligations de conformité s'imposent comme des priorités opérationnelles.

TABLE DES MATIERES

TEXTE DU RAPPORT

I. Le constat : entre tradition d'innovation et perte de repères

❖ **L'Ordre des avocats de Paris est la première *legaltech* historique française.**

L'Ordre des avocats de Paris s'inscrit dans une tradition ancienne et continue d'innovation technologique appliquée au droit.

- Pionnier en matière de numérique, il a su anticiper dès le début des années 2000, sous l'impulsion de bâtonniers visionnaires, les transformations à l'œuvre en structurant ses données et en développant des outils numériques propres (gestion de l'annuaire, de la déontologie) conçus en interne par la direction des systèmes d'information et enrichis en lien étroit avec les services au fil des années.

- La Base Déontologique et Professionnelle (BDP), créée en 2002 à l'initiative du bâtonnier Iweins, s'inscrivait dans une ambition structurante : rendre accessible à l'ensemble des avocats la matière déontologique, dans un souci de transparence et de bonne diffusion des règles professionnelles.

- Cette capacité d'anticipation s'est confirmée plus récemment avec le développement d'applications structurantes, telle que e-MDF[1], aujourd'hui en cours de déploiement dans l'intégralité des CARPA de France.

Cette capacité de pionnier en matière d'innovation technologique constitue un marqueur fort de l'identité de l'Ordre qui a su, à plusieurs reprises, se positionner en précurseur dans la mise en œuvre d'outils au service de la profession, et représente à ce titre la première *legaltech* historique française.

Au-delà de cette dimension technologique, l'Ordre des avocats de Paris s'impose comme un véritable **tiers de confiance numérique**. Il constitue à la fois une **boussole pour les avocats parisiens** dans leurs choix technologiques, une référence pour les autres barreaux et un acteur structurant au sein de l'écosystème juridique.

Véritable « **aimant à innovations** », l'Ordre des avocats de Paris fédère et catalyse en effet un écosystème technologique particulièrement dynamique et favorise l'émergence de solutions innovantes au service des avocats et des justiciables.

❖ **L'Ordre des avocats de Paris n'est pas une société de services numériques.**

Si l'Ordre des avocats de Paris a su historiquement développer des outils propres, il ne saurait pour autant être assimilé à un prestataire ou distributeur de services numériques. Il ne lui appartient en effet pas d'organiser une intermédiation entre les avocats et les prestataires, ni de se substituer aux acteurs privés.

La vocation de l'Ordre des avocats de Paris consiste, de manière plus fondamentale, à **informer, orienter et accompagner** les avocats, à structurer un **cadre de confiance** et, lorsque cela apparaît nécessaire, à développer des **outils propres** répondant à des **besoins stratégiques** insuffisamment couverts par des acteurs privés.

Cette ligne d'**équilibre**, parfois délicate à tracer, constitue un point d'attention majeur dans la définition de la stratégie numérique.

[1] e-MDF est le logiciel métier qui a été codéveloppé par la CARPA de Paris (précisément par les équipes de la DSI de l'Ordre des avocats de Paris) et l'UNCA, actuellement en cours de déploiement au sein de toutes les CARPA du territoire.

II. Enjeux : dépendances, innovation et croissance

A) Les cinq piliers de la stratégie numérique : souveraineté, sécurité, équité, durabilité, exemplarité

a. Souveraineté :

Les débats internes à l'Ordre des avocats de Paris ont permis de dégager une définition de la souveraineté numérique en matière d'hébergement des données proche de celle-ci :

« Souverain : désigne le fait pour un outil d'être cumulativement hébergé et opéré sur le territoire de l'Union européenne, et de faire l'objet d'un contrôle exclusif par une entité établie dans l'Union européenne, de mettre en œuvre les mesures garantissant que l'ensemble des données traitées, y compris les données d'exploitation et de support, sont stockées et traitées exclusivement au sein de l'Union européenne et, de mettre en œuvre des mesures techniques et organisationnelles appropriées assurant un niveau de sécurité et de confidentialité conforme à la réglementation européenne applicable ».

La souveraineté numérique s'est imposée en quelques années comme un enjeu politique majeur, au croisement des questions de sécurité, d'indépendance économique et de protection des libertés fondamentales. Dans le champ judiciaire, elle revêt une portée particulière : elle conditionne non seulement la garantie et la protection du secret professionnel, mais également la capacité des institutions à exercer leurs missions sans dépendance excessive à des acteurs privés, a fortiori quand ces derniers ne sont pas européens.

Au même titre que l'État a engagé une stratégie pragmatique de limitation de ses dépendances fondée sur la maîtrise des risques, l'Ordre des avocats du Barreau de Paris dispose d'une responsabilité et d'opportunités : faire de la souveraineté numérique un **levier de structuration et de protection de la profession**.

b. Sécurité :

La sécurité constitue un pilier fondamental de la stratégie numérique. Elle ne peut plus être appréhendée comme un sujet exclusivement technique, mais doit être envisagée comme un **enjeu de gouvernance** et faire l'objet d'une montée en puissance rapide au sein des cabinets.

Elle suppose, d'une part, la protection des données confidentielles de l'Ordre et des cabinets contre les risques de captation, de suppression ou de compromission et, d'autre part, une évolution des pratiques professionnelles, fondée sur une meilleure compréhension et appropriation des risques.

De manière indissociable, elle intègre les obligations spécifiques de la profession, notamment en matière de lutte contre le blanchiment, qui impliquent des exigences élevées en matière de traçabilité, de conservation des données et de sécurisation des flux d'information.

c. Equité :

La transformation numérique ne peut produire pleinement ses effets que si elle bénéficie à l'ensemble des avocats, indépendamment de la taille des structures ou des moyens dont elles disposent. A cet égard, l'Ordre des avocats de Paris a un rôle à jouer pour garantir un accès équitable aux outils et aux ressources en favorisant des mécanismes de mutualisation des coûts et des ressources et en accompagnant les avocats dans l'appropriation des technologies via des ateliers de formation.

d. Durabilité :

La stratégie numérique intègre également une exigence de durabilité, tant sur le plan environnemental qu'éthique. Le recours à des outils transparents, non discriminants et respectueux des principes fondamentaux doit être privilégié. Les choix technologiques opérés par l'Ordre des avocats de Paris doivent également tenir compte des impératifs de sobriété numérique et s'inscrire dans une logique de responsabilité.

e. Exemplarité :

Le Barreau de Paris, en raison de sa taille et de son influence, se trouve en position d'assumer un rôle d'exemplarité. Il lui revient donc de contribuer à structurer les réflexions sur le numérique juridique, à participer au débat public et à fédérer, autant que possible, les acteurs concernés.

B) La souveraineté numérique : une quête structurelle pour l'Ordre des avocats de Paris

a. Le cadre législatif et réglementaire

Le cadre applicable aux enjeux de souveraineté numérique procède d'un ensemble de normes européennes, nationales et indirectement étrangères qui, sans consacrer formellement cette notion, en déterminent les implications en matière de sécurité des systèmes d'information, de protection des données et de maîtrise des dépendances technologiques.

Au niveau de l'Union européenne, le **règlement (UE) 2016/679 du 27 avril 2016 (RGPD)** constitue le socle du dispositif. Il encadre le traitement des données à caractère personnel en imposant des obligations de licéité, de sécurité et de responsabilité, ainsi que des restrictions strictes aux transferts de données vers des États non européens. Ces transferts sont subordonnés à l'existence d'un niveau de protection adéquat ou à la mise en œuvre de garanties appropriées, ce qui participe directement à l'exigence de maîtrise des flux de données.

La **directive (UE) 2022/2555 du 14 décembre 2022 dite NIS 2** renforce substantiellement le cadre applicable en matière de cybersécurité. Elle impose aux entités relevant de son champ d'application la mise en place de mesures techniques et organisationnelles appropriées et proportionnées destinées à gérer les risques pesant sur la sécurité des réseaux et des systèmes d'information. Elle prévoit notamment l'instauration de politiques de gestion des risques, de dispositifs de gestion des incidents, de mécanismes de continuité d'activité et de procédures de gestion de crise. Elle consacre, en outre, une responsabilité directe des organes dirigeants, chargés d'approuver, de superviser et de contrôler les mesures mises en œuvre.

Le **règlement (UE) 2022/2554 du 14 décembre 2022 (DORA)** s'inscrit dans une logique comparable, en instituant un cadre harmonisé de gestion des risques liés aux technologies de l'information et de la communication. Il impose aux entités financières concernées des obligations structurées portant sur l'identification des actifs critiques, la prévention des incidents, la détection des anomalies, la gestion des crises, la continuité des services et la supervision des prestataires tiers de services numériques.

Ces instruments convergent vers un renforcement des exigences juridiques relatives à la sécurité des systèmes d'information, à la gouvernance des risques numériques et à l'encadrement des dépendances technologiques.

b. Risques et menaces : géopolitique et lois extraterritoriales

L'appréhension des enjeux de souveraineté numérique implique de prendre en compte un ensemble de risques juridiques et politiques affectant la maîtrise des données et l'accès aux technologies. Ces risques s'inscrivent dans un contexte marqué par l'extraterritorialité de certaines législations, la structuration mondiale des chaînes technologiques et une dépendance significative à des fournisseurs non européens.

En premier lieu, les législations étrangères, en particulier américaines, sont susceptibles de produire des effets extraterritoriaux. Le ***Cloud Act*** et le ***USA Patriot Act*** permettent aux autorités américaines d'avoir accès à des données détenues par des opérateurs relevant de leur juridiction, indépendamment du lieu de stockage. Ces mécanismes peuvent entrer en conflit avec les exigences du droit de l'Union européenne, notamment en matière de protection des données et de confidentialité.

En deuxième lieu, les mesures techniques de protection, y compris le chiffrement, présentent des limites au regard de ces enjeux. Elles ne font pas obstacle aux obligations légales de **communication de données imposées** aux prestataires.

En troisième lieu, la dépendance à des technologies et services numériques non européens expose à des **risques de rupture d'accès**. À cet égard, les autorités nationales françaises compétentes en matière de cybersécurité ont souligné que l'hypothèse d'une restriction ou d'une suspension d'accès à certaines technologies, parfois désignée sous le terme de « *kill switch* », ne relève pas d'une hypothèse théorique.

Dans un contexte marqué par le retour de tensions commerciales, politiques et juridiques, notamment entre les États-Unis et l'Union européenne, de telles mesures pourraient résulter de **décisions unilatérales, de sanctions ou de mécanismes de rétorsion**. Elles pourraient affecter non seulement l'accès aux services, mais également la continuité des mises à jour logicielles, avec des conséquences directes sur le niveau de sécurité des systèmes d'information.

En outre, ces dépendances doivent être appréciées au regard de la **complexité des chaînes de sous-traitance.** Les services numériques reposent sur des architectures imbriquées, au sein desquelles l'origine des composants logiciels et des infrastructures est souvent difficile à tracer. Cette situation limite la capacité à identifier précisément les dépendances et à en mesurer les implications juridiques.

Enfin, la coexistence de cadres juridiques distincts est susceptible de générer des situations de **conflit de normes**, en particulier entre les obligations issues du droit de l'Union européenne et celles résultant de législations étrangères. Ces situations peuvent créer des incertitudes quant au régime applicable aux données et aux conditions de leur accès.

c. Synthèse comparée

i. L'Etat

La stratégie portée par l'État en matière de souveraineté numérique est celle d'un rééquilibrage. L'État reconnaît sa dépendance actuelle à des fournisseurs internationaux, mais cherche à en limiter les effets en renforçant sa capacité de négociation, de contrôle et, à terme, de substitution. Il s'agit d'une **stratégie complexe de réduction des dépendances numériques**, menée ministère par ministère, sans rupture immédiate.

Dans ce cadre, la Direction interministérielle du Numérique (DINUM), prochainement fusionnée avec la Direction interministérielle de la Transformation publique (DITP) pour créer une **Autorité nationale du numérique et de l'IA**, joue un rôle structurant en définissant une doctrine interministérielle de réduction des dépendances numériques[2]. Cette doctrine repose sur plusieurs axes : promotion du cloud de confiance, mutualisation des solutions numériques, et développement de capacités internes (ex : abandon de Windows par la DINUM qui équipe ses 234 postes par Linux).

Le cas du Health Data Hub (Plateforme des données de santé) constitue une autre illustration éclairante de la nouvelle doctrine de l'Etat : si le recours à un hébergement opéré par Microsoft (Cloud Azure) a été jugé conforme au RGPD par le Conseil d'État[3], notamment en raison des garanties contractuelles, de la pseudonymisation des données et de l'absence de transfert direct de données de santé vers les États-Unis, il n'en révèle pas moins une

[2] « 234 postes : la DINUM sort de Windows, pas l'Etat », IT for Business, 15 avril 2026.
[3] https://www.conseil-etat.fr/actualites/health-data-hub-le-traitement-automatise-des-donnees-de-sante-autorise-par-la-cnil-est-conforme-au-rgpd

dépendance persistante à des infrastructures extra-européennes. Une tension qui conduit aujourd'hui à des évolutions structurelles : la migration à compter de 2027 des données de la plateforme vers la solution de cloud souverain Scaleway[4] (filiale du groupe Iliad en attente de certification SecNumCloud[5])[6].

Par ailleurs, les travaux conduits par **l'École nationale de la magistrature et le ministère de la Justice** traduisent une approche particulièrement structurée, où la souveraineté technologique est indissociable de l'État de droit. Concernant le ministère de la Justice, le déploiement d'outils d'intelligence artificielle est assumé comme une nécessité immédiate pour répondre aux besoins des juridictions, tout en s'accompagnant d'une exigence forte en matière de souveraineté. Tel que prévu par le rapport sur « L'IA au service de la justice »[7], un assistant IA civil et pénal a été déployé auprès des magistrats, adossé à un environnement d'hébergement souverain, avec un objectif à terme d'internalisation progressive des infrastructures et des compétences. Plus largement, la doctrine française en matière d'IA judiciaire insiste sur un point central : ces technologies doivent rester des outils d'assistance, sous contrôle humain permanent, afin de préserver l'indépendance de la justice et la confiance des citoyens.

Ces exemples illustrent une ligne de crête assumée par l'État : sécuriser dans l'immédiat, transformer dans la durée.

ii. Le CNB

Du côté « national » de la profession, la position portée par le CNB s'inscrit dans une **logique de vigilance renforcée** même si à date, aucune doctrine n'a été formellement adoptée. L'usage des outils numériques, et en particulier de l'intelligence artificielle, ne peut être envisagé sans garanties strictes en matière de confidentialité, de sécurité et de respect du secret professionnel.

A ce titre, d'importantes difficultés ont été relevées concernant une nouvelle version à venir du logiciel d'email client « Outlook » proposée par Microsoft qui imposera un transfert systématique des données par les serveurs de Microsoft, y compris pour les utilisateurs de comptes de messagerie non-Microsoft. Cette obligation qui concerne notamment les identifiants de connexion, les courriels envoyés et reçus ainsi que leurs pièces jointes constitue une évolution notable qui soulève de graves préoccupations en matière de confidentialité, de sécurité et de conformité juridique, notamment pour les professionnels soumis au respect du secret professionnel.

Cette position traduit une conception exigeante de la « souveraineté numérique » : il ne s'agit pas seulement de protéger des données, mais de préserver l'indépendance même de l'avocat dans l'exercice de sa fonction. Position qui a incité le CNB à promouvoir des dispositifs comme le Legal Data Space[8] dans le cadre d'un partenariat[9] dont les contours restent à clarifier.

iii. Le CCBE

[4] https://www.health-data-hub.fr/actualites/la-plateforme-des-donnees-de-sante-engage-sa-migration-vers-un-cloud-souverain-avec
[5] Elaborée par l'ANSSI, la qualification SecNumCloud permet de reconnaître des offres cloud « de confiance » dont l'utilisation est préconisée pour la protection des données sensibles.
[6] La France retire ses dossiers médicaux à Microsoft pour les confier au groupe Iliad
[7] https://www.justice.gouv.fr/sites/default/files/2025-08/rapport_ia_au_service_de_la_justice.pdf
[8] LDS : intermédiaire de données permettant un partage contrôlé et sécurisé de données juridiques par un hébergement français et européen.
[9] Rapport de la Commission Prospective et Innovation du CNB présenté à l'AG du 6 février 2026.

Les lignes directrices du CCBE[10] rappellent que le recours aux services numériques, et en particulier au cloud, ne modifie pas les **obligations fondamentales de l'avocat,** notamment en matière de secret professionnel, de confidentialité et de compétence.

Elles mettent en évidence plusieurs points structurants :

- L'avocat demeure responsable des données, y compris lorsqu'elles sont traitées par des prestataires tiers. Cette externalisation est susceptible d'entraîner une perte de contrôle et une exposition à des législations étrangères.

- Les transferts internationaux de données et l'application de législations extraterritoriales sont identifiés comme des facteurs de risque, en particulier lorsque les fournisseurs sont soumis à des obligations d'accès aux données par des autorités publiques.

- La complexité des chaînes de sous-traitance limite la visibilité sur les flux de données et les responsabilités associées.

Dans ce contexte, le CCBE structure une exigence de maîtrise fondée sur la connaissance des prestataires et de leurs sous-traitants, l'identification des lieux de traitement des données, l'analyse des conditions contractuelles et la garantie de la disponibilité et de la réversibilité des données.

La souveraineté numérique est ainsi appréhendée comme une **condition de l'effectivité du secret professionnel et de la maîtrise des données par l'avocat**.

d. La souveraineté numérique de l'Ordre des avocats de Paris : une opportunité stratégique à préempter et à structurer

Gage **d'indépendance, d'exemplarité et de confiance**, la souveraineté numérique doit être abordée de façon pragmatique, dans le temps long : une **quête,** un **horizon stratégique**, une **capacité de choix**, de **maîtrise** et de **réversibilité**. Dans cette perspective, l'Ordre des avocats du Barreau de Paris se trouve dans une position singulière.

L'accélération des transformations numériques rend en effet incontournable une réflexion approfondie sur la souveraineté de ses outils et de ses infrastructures, au service de la protection du secret professionnel et de l'indépendance de la profession.

Elle suppose **d'identifier les points de dépendance critiques**, de **sécuriser les infrastructures** essentielles et de privilégier, chaque fois que cela est possible, des **solutions européennes**. Elle impose également d'anticiper dans la mesure du possible les **évolutions géopolitiques et réglementaires**, dans un contexte marqué par une intensification des tensions de toutes natures, notamment technologiques.

Par ailleurs, **la directive NIS 2[11] change l'approche en matière de cybersécurité**, en faisant de la gestion des risques numériques une responsabilité directe des organes dirigeants et en imposant des exigences élevées en matière de gouvernance, de continuité d'activité et de maîtrise des prestataires.

Dès lors, la question n'est plus celle de l'applicabilité formelle de la directive NIS 2 mais de son appropriation stratégique : pour l'Ordre des avocats de Paris comme pour la CARPA, **l'adoption volontaire de ces standards apparaît comme un levier de sécurisation** des infrastructures, de maîtrise des dépendances et de crédibilité

[10]https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/FR_ITL_20250227__CCBE-guidelines-on-the-use-of-cloud-computing-by-lawyers.pdf
[11] https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/

institutionnelle, dans un contexte de montée des risques cyber et de judiciarisation croissante des obligations de sécurité.

Comme vu précédemment, dans l'attente de la définition de la doctrine par le Conseil de l'Ordre en cette matière, il convient de préciser que les débats internes ont permis de dégager une **définition de la souveraineté en matière d'hébergement des données dans des termes proches de ceux-ci** :

« Souverain : désigne le fait pour un outil d'être cumulativement hébergé et opéré sur le territoire de l'Union européenne, et de faire l'objet d'un contrôle exclusif par une entité établie dans l'Union européenne, de mettre en œuvre les mesures garantissant que l'ensemble des données traitées, y compris les données d'exploitation et de support, sont stockées et traitées exclusivement au sein de l'Union européenne et, de mettre en œuvre des mesures techniques et organisationnelles appropriées assurant un niveau de sécurité et de confidentialité conforme à la réglementation européenne applicable ».

La question de la souveraineté numérique ne peut toutefois être abordée de manière isolée. Elle doit s'inscrire dans une stratégie globale, conciliant plusieurs impératifs parfois contradictoires : sécuriser les usages sans freiner l'innovation, garantir l'indépendance sans isoler la profession, maîtriser les outils sans renoncer à leur performance.

Dans cette perspective, le Barreau de Paris a un rôle particulier à jouer. Par sa taille, son influence et sa capacité d'initiative, il peut contribuer à structurer une voie française de la souveraineté numérique appliquée aux avocats parisiens.

III. Propositions d'actions pour l'Ordre des avocats de Paris et pour les cabinets parisiens

A) Actions prioritaires pour l'Ordre des avocats de Paris :

a. Procéder à un audit des dépendances de l'Ordre

Dans le cadre de la définition de la stratégie numérique de l'Ordre des avocats de Paris, la question de l'identification et de la maîtrise des dépendances technologiques revêt un caractère central.

Cette démarche suppose d'engager un audit structuré des dépendances de l'Ordre, afin d'identifier de manière précise les **points d'exposition, qu'ils soient d'ordre technique, juridique, opérationnel ou financier**. Cet audit vise à déterminer les risques, à qualifier leur criticité et à définir des moyens de les circonscrire.

Cet enjeu ne se limite pas à une dimension technique. Il engage la capacité du Barreau de Paris à garantir à ses membres un environnement numérique conforme aux exigences déontologiques et réglementaires, notamment en matière de confidentialité et de sécurité des données, et à préserver son autonomie dans ses choix technologiques.

Dans un contexte marqué par une utilisation significative de solutions proposées par des acteurs non européens, et principalement américains, cette analyse apparaît nécessaire pour éclairer les décisions à venir.

L'audit devra notamment porter sur les infrastructures, les prestataires, les conditions contractuelles, les flux de données et les engagements financiers associés. Il pourra utilement intégrer une analyse des contraintes issues du cadre réglementaire, notamment en lien avec les exigences issues de la directive NIS 2.

b. Définir la doctrine de l'Ordre des avocats de Paris en matière de souveraineté

Au regard de ce qui précède, et compte tenu du grand mouvement porté par l'Etat et les institutions européennes de réduction des dépendances, il apparaît nécessaire de formaliser la doctrine de l'Ordre en matière de souveraineté numérique au travers d'un **cadre cohérent, prescripteur pour l'ensemble des confrères parisiens**, permettant d'assurer une **meilleure lisibilité des choix opérés**.

Cette doctrine aura vocation à constituer un cadre de référence permettant d'orienter les choix technologiques, en **tenant compte de la diversité des situations et des contraintes opérationnelles évolutives.** Elle devra également préciser les critères de recours aux solutions technologiques, en tenant compte de la nature des données, des risques identifiés, des garanties offertes par les prestataires et des contraintes économiques associées. Elle pourra, le cas échéant, intégrer une **réflexion sur le recours à des solutions françaises ou européennes**, ainsi que sur les conditions dans lesquelles ces solutions peuvent être mises en œuvre.

c. Intégrer l'intelligence artificielle dans les services de l'Ordre

L'intégration de l'intelligence artificielle constitue un levier de transformation important pour l'Ordre qui appelle une mise en œuvre progressive, encadrée et maîtrisée. L'IA représente en ce sens une opportunité, un outil au service des missions de l'Ordre et de son fonctionnement.

i. L'intelligence artificielle au service du Pôle déontologie de l'Ordre : sécuriser, enrichir et valoriser notre corpus juridique.

Dans le cadre du positionnement du Barreau de Paris en matière de stratégie numérique, cet atout majeur que constitue la donnée déontologique se trouve à la croisée des initiatives. Précisément, l'intelligence artificielle apparait comme une opportunité à **deux niveaux** :

1. Intégration de l'intelligence artificielle en interne : l'IA au service de la mission régalienne de l'Ordre

L'activité du Pôle Déontologie implique une gestion complexe et chronophage des dossiers pour les salariés, les avocats missionnés et les MCO en charge de la déontologie, dont le quotidien est notamment marqué par le traitement d'un nombre considérable de pièces, par l'analyse des dossiers et la rédaction d'avis.

Face à l'augmentation du nombre de saisines du Pôle et à la complexification des dossiers, les outils numériques constituent un levier d'optimisation du fonctionnement du service. L'intégration d'un outil d'intelligence artificielle souveraine contribuerait à la **rationalisation du traitement des dossiers** en permettant un **accès plus fluide et plus pertinent à la doctrine déontologique, et à renforcer la diffusion des règles professionnelles**, tout en tenant compte des plus hautes exigences en matière de sécurité et de confidentialité.

2. Intégration de l'intelligence artificielle en externe : L'IA au service des avocats parisiens

L'Ordre des avocats de Paris met à la disposition des avocats parisiens via leur « espace pro » une base de données déontologiques structurée, la « Base Déontologique et Professionnelle » (BDP) dont la gestion est assurée par l'équipe du Centre de Documentation.

Ce corpus comporte notamment des avis déontologiques, décisions disciplinaires et productions ordinales structurantes sélectionnés par le service du Pôle déontologie et ayant fait l'objet d'une anonymisation préalable. Il s'agit d'une **véritable source du droit, précieuse, spécifique aux avocats parisiens.** Une source normative au service des avocats, des élus et de la sécurité juridique de la profession, qui suscite également l'intérêt de plusieurs autres barreaux de France.

Dans ce contexte, la vision portée consiste à faire de ce corpus un levier structurant d'accès à la doctrine déontologique.

⇒ Concrètement, cette plateforme revisitée grâce à l'intelligence artificielle devrait offrir aux avocats parisiens :

- un accès simplifié à la doctrine déontologique,
- une aide à la compréhension des règles professionnelles,
- un appui dans la sécurisation de leurs pratiques quotidiennes.

Le projet s'inscrit au croisement de plusieurs enjeux structurants :

- **Un enjeu de souveraineté** : la doctrine déontologique constitue un patrimoine propre à la profession. Son exploitation par des outils externes, non maîtrisés, ferait peser un risque sur le secret professionnel, la maîtrise et l'intégrité de ces données.

- **Un enjeu de sécurisation des pratiques professionnelles** : En facilitant l'accès à la règle, l'outil contribue directement à la prévention des risques déontologiques.

Ce projet d'intégration de l'IA en interne et en externe appelle enfin une vigilance particulière en matière de gouvernance, de sécurité et d'acceptabilité (formation). Précisément, le développement de ces projets appelle une attention particulière sur plusieurs points :

- La fiabilité juridique des réponses : l'outil ne peut en aucun cas se substituer à l'analyse humaine, il doit rester un outil d'assistance.
- La protection des données : les données déontologiques sont hautement sensibles et nécessitent un encadrement strict.

ii. Déployer l'intelligence artificielle dans les services de l'Ordre

Au-delà du projet d'IA au service de la déontologie, **l'intelligence artificielle a vocation à être intégrée dans l'ensemble des services de l'Ordre,** dans une logique d'amélioration des processus et de l'accès au droit. Cette démarche suppose une coordination étroite avec les services concernés et une définition claire des cas d'usage prioritaires.

iii. Structurer les projets et sécuriser leur mise en œuvre

La mise en œuvre de ces projets suppose de **structurer une démarche de sélection et de pilotage**. À cet égard, il apparaît nécessaire de :

- Formaliser l'expression des besoins,
- Elaborer des cahiers des charges adaptés,
- Définir des critères de sélection des projets,
- Organiser des phases pilotes permettant de tester les solutions avant leur généralisation.

d. Structurer la capacité d'investissement de l'Ordre pour les projets numériques

La mise en œuvre d'une stratégie numérique suppose une **capacité d'investissement adaptée aux enjeux identifiés**. Dans ce cadre, l'Ordre est conduit à structurer sa politique d'investissement, en tenant compte de ses **ressources propres**.

Les investissements dans le numérique, notamment dans un mouvement de réduction des dépendances à des solutions extra-européennes, et en particulier dans les outils d'intelligence artificielle, doivent être appréhendés dans une logique de transformation, susceptible de produire des effets en termes de **productivité, de rationalisation des coûts et d'amélioration des conditions de travail**. Ils peuvent également contribuer à **renforcer l'attractivité de l'Ordre,** notamment en matière de recrutement de profils techniques, dans un contexte de tension sur ces compétences.

B) Actions prioritaires pour les avocats parisiens :

a. Définir un plan d'action « conformité » pour les cabinets d'avocats (cyber, RGPD, souveraineté, LCB-FT)

i. Bâtir une confiance numérique structurelle au sein des cabinets

Le développement des usages numériques au sein des cabinets s'accompagne d'un renforcement des exigences en matière de conformité, notamment au regard de la cybersécurité, de la protection des données personnelles, de la souveraineté et de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

De plus en plus imbriquées, ces obligations imposent une approche globale permettant aux avocats d'identifier leurs risques, de structurer leurs pratiques et de sécuriser leur activité. Dans ce cadre, l'Ordre a vocation à **accompagner les cabinets**, en particulier les structures de petite taille, dans la **mise en conformité de leurs pratiques numériques**. Cet accompagnement doit s'appuyer sur la **mise à disposition d'outils, de référentiels et de dispositifs d'appui**, sans pour autant imposer un modèle unique.

L'ambition consiste à **faire de l'Ordre un tiers de confiance** sur ces sujets, reconnu pour sa crédibilité par les pouvoirs publics et les acteurs institutionnels, et capable de structurer une réponse adaptée aux enjeux de la profession.

ii. Structurer un dispositif d'accompagnement à l'échelle du Barreau

La mise en œuvre de cette ambition suppose de structurer un dispositif d'accompagnement à l'échelle du Barreau de Paris. Un **objectif de sensibilisation généralisée des cabinets aux risques et aux enjeux numériques** peut être fixé **à horizon 2027**, avec une montée en charge progressive des dispositifs d'accompagnement.

Dans cette perspective, il apparaît nécessaire de :

- Permettre aux avocats d'évaluer leur niveau de maturité en matière de cybersécurité et de conformité,
- Mettre à disposition des outils opérationnels facilitant la mise en conformité.

Un réseau de référents cybersécurité pourrait être constitué, dans le cadre de travaux menés notamment par la DPO de l'Ordre avec l'ANSSI, composé de MCOs ou d'avocats volontaires formés en amont, capables d'apporter un premier niveau d'accompagnement aux cabinets. Ce réseau, fondé sur une logique de pairs, contribuerait à la diffusion des bonnes pratiques et à l'appropriation des outils.

iii. Définir un cadre commun de sécurité et de conformité

Il apparaît nécessaire de définir un cadre commun de sécurité applicable à l'ensemble des avocats. Ce cadre pourrait notamment inclure :

- Une politique de cybersécurité harmonisée,
- Des dispositifs de formation adaptés,
- **Un référencement de prestataires répondant à des exigences définies et régulièrement remis en « concurrence » et audités.**

Une réflexion pourrait également être engagée sur l'intégration d'une **charte relative à l'usage de l'intelligence artificielle et à la cybersécurité** au sein des conventions d'honoraires.

iv. Encadrer les usages de l'intelligence artificielle

Le développement des usages de l'intelligence artificielle au sein des cabinets appelle un encadrement spécifique. Dans la poursuite des travaux menés dans le cadre du Livre Blanc diffusé en fin d'année 2025 et compte-tenu de l'évolution rapide des pratiques et des technologies, il convient de définir des règles d'usage, notamment en matière de traitement des données, de confidentialité et de responsabilité professionnelle.

Une attention particulière doit être portée aux conditions d'utilisation des outils, notamment s'agissant des différences entre les offres grand public et les offres professionnelles, qui présentent des garanties distinctes en matière de traitement des données et de confidentialité. Des outils d'accompagnement peuvent être développés

afin d'aider les avocats à évaluer les solutions disponibles, notamment sous la forme de référentiels ou de dispositifs d'analyse des risques.

Par ailleurs, les évolutions technologiques, et en particulier l'intelligence artificielle, interrogent certaines règles déontologiques. Une réflexion devra être engagée afin d'en apprécier les implications, notamment en matière d'information du client, de traitement des données et de facturation.

b. Faire du numérique un levier de croissance pour les cabinets parisiens

Le numérique ne doit pas être appréhendé uniquement sous l'angle des contraintes, mais également comme un levier indispensable de développement et de compétitivité pour les cabinets.

L'Ordre a vocation à aider à un accès équitable aux outils numériques, notamment par la mise en place de **solutions mutualisées**, adaptées aux besoins de la profession. Cela peut notamment se traduire par la mise à disposition d'infrastructures sécurisées ou par la négociation d'offres adaptées.

Par ailleurs, l'accompagnement des cabinets suppose une **politique d'acculturation ambitieuse**. Dans cette perspective, le Centre de Documentation pourrait voir son périmètre élargi (« Centre de Documentation et de Technologie juridique ») et se positionner comme un lieu dédié à l'innovation juridique et à la diffusion des pratiques numériques, intégrant des actions de formation, des démonstrations et des échanges autour des outils. Cette évolution permettrait de structurer un espace de référence pour les avocats, facilitant l'appropriation des technologies et leur intégration dans les pratiques professionnelles.

c. La formation initiale et continue : un enjeu existentiel

Dans un contexte où certains cabinets réduisent la masse de leurs collaborateurs et stagiaires à l'occasion de l'intégration de l'IA dans leur structure, la formation constitue un levier central de la stratégie numérique et doit être adaptée pour intégrer les enjeux liés à l'intelligence artificielle et aux technologies numériques. Elle conditionne la capacité des avocats à appréhender les évolutions technologiques, et à en maîtriser les usages.

Cette transformation implique une évolution des contenus et des formats pédagogiques, ainsi qu'une intégration progressive des outils dans les dispositifs de formation.

PILOTAGE ET CALENDRIER :

Les orientations présentées constituent une trajectoire. Elles appellent et appelleront des ajustements et arbitrages, dans le cadre d'un dialogue régulier avec les membres du Conseil de l'Ordre.

Le calendrier de présentation a permis d'associer progressivement les différentes instances ordinales, avec une présentation au Bâtonnier, à la Vice-Bâtonnière, à la Secrétaire du Conseil et au Directeur général le 17 février 2026, puis à la sous-Commission des évolutions numériques le 19 mars 2026, avant la présentation au Conseil de l'Ordre le 19 mai 2026. Le Pôle déontologie et les MCO Secrétaires de la déontologie ont également été associés au projet de déploiement d'une intelligence artificielle en cette matière le 5 mai 2026.

Le pilotage de la stratégie numérique repose sur une gouvernance associant le Bâtonnier, la vice-Bâtonnière, les membres du Conseil de l'Ordre (MCO dédiés et Commission des finances), la Direction générale et la Direction de la stratégie numérique.

Des groupes de travail dédiés à chaque action du plan seront par ailleurs constitués et composés des services de l'Ordre concernés ainsi que les services : DSI, RSSI, DPO, Direction des affaires publiques, Centre de documentation.