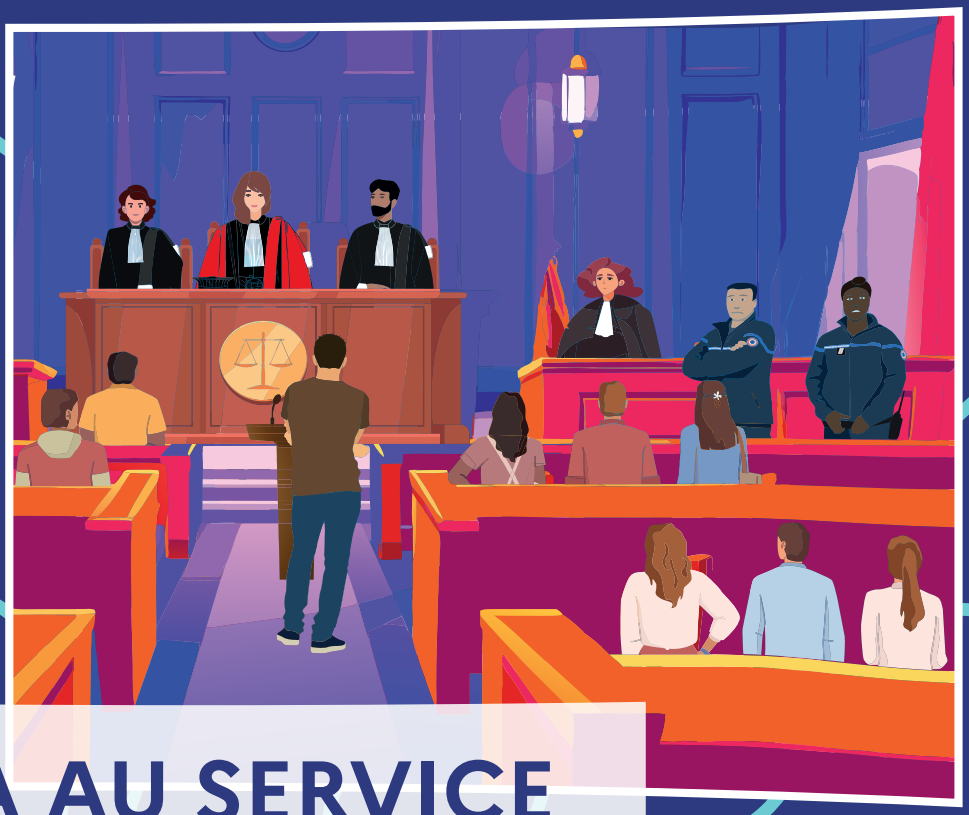


L'IA AU SERVICE DE LA JUSTICE : STRATÉGIE ET SOLUTIONS OPÉRATIONNELLES

Composition du groupe de travail

Haffide BOULAKRAS, directeur adjoint de l'école nationale de la magistrature (ENM)

Élise FARGE DI MARIA, cheffe de projet IA au secrétariat général du ministère de la Justice (SG)

Cécile CAPEAU, Inspectrice générale de la Justice (IGJ)

Benoît CHAMOUARD, 1er vice-président adjoint au tribunal judiciaire de Paris

Géraud DE-LA-BROSSE, chef de section innovation & bonnes pratiques, direction de l'administration pénitentiaire (DAP)

Julien FAROBBIA, sous-directeur de l'évaluation et du numérique de la direction des affaires criminelles et des grâces (DACG)

Mehidine FAROUDJ, sous-directeur des missions de protection judiciaire et d'éducation de la direction de la protection judiciaire de la jeunesse (DPJJ)

Aude GROUALLE, vice-procureur chargé du secrétariat général, parquet national antiterroriste

Albin HEUMAN, chargé de mission au secrétariat général du ministère de la Justice (SG)

Tarik LAKSSIMI, professeur agrégé des universités et sous-directeur en charge de la recherche à l'école nationale de la magistrature (ENM)

Emmanuelle LAUDIC-BARON, magistrat chargée de mission au département international de l'école nationale de la magistrature (ENM)

Pierre LECHANTEUX, directeur de programme dématérialisation des parcours métiers du secrétariat général du ministère de la Justice (SG)

Hugues MARTIN, directeur de programme de convergence des outils pénaux au secrétariat général du ministère de la Justice (SG)

Yannick MENECEUR, Inspecteur général de la Justice (IGJ)

Loïc POIRIER, chef de bureau conduite du changement du programme Procédure Pénale Numérique au secrétariat général du ministère de la Justice (SG)

Vincent SALAFA, adjoint au chef de bureau du droit processuel et du droit social, direction des affaires civiles et du sceau (DACS)

Philippe SILVAN, premier président de chambre à la cour d'appel d'Aix-en-Provence

Agnès TALON, chargée de mission auprès du sous-directeur de l'organisation judiciaire et de l'innovation de la direction des services judiciaires (DSJ)

Haï-Ha TRINH-VU, chef du Lab Data Justice, Direction du numérique (DNUM)

Alexandre VERNEY, procureur de la République adjoint près le tribunal judiciaire de Meaux

Avec le soutien de la direction interministérielle de la transformation publique (DITP)

Dalhia CHEKAOUI, directrice de projet

Quentin HEMONT, chef de projet

Raymane DOGHRI, consultant interne

Avant-propos

Monsieur le garde des Sceaux,

Conformément à la mission que vous m'avez confiée, le présent rapport expose une stratégie d'intégration de l'IA au bénéfice de l'ensemble des magistrats et agents du service public de la Justice.

Les enjeux majeurs liés à la modernisation de la Justice restent incontestables. Toutefois, le terme « modernisation », longtemps valorisé, me semble par moments perdre de sa portée, car il peut évoquer un processus long et progressif. Or, les opportunités offertes par l'IA exigent une mobilisation rapide et concrète afin que le ministère de la Justice réussisse ce tournant décisif.

C'est dans cet esprit que la mission a choisi d'adopter une approche résolument pragmatique et opérationnelle, visant à permettre à l'institution judiciaire de tirer pleinement parti, sans délai, des bénéfices concrets de l'intelligence artificielle (IA).

En nous appuyant sur des échanges fructueux avec de nombreux professionnels et experts, nous avons pu, dans le délai de trois mois imparti à la mission, concrétiser des propositions ambitieuses mais parfaitement réalisables dans un environnement contraint.

Ce rapport ne prétend pas à l'exhaustivité, ni à une approche académique. Il évacue la question, galvaudée, de la justice prédictive, dont certains opérateurs privés ont commencé à s'emparer mais sur laquelle il n'apparaît pas pertinent que le ministère s'engage à ce jour si ce n'est pour en démontrer les limites et en combattre les éventuels effets néfastes. Ce rapport se concentre sur des cas d'usage concrets, susceptibles d'améliorer rapidement l'efficacité du travail des agents et la qualité du service rendu aux usagers. Il propose une stratégie « clé en main », réaliste, sécurisée, tenant compte des contraintes juridiques, budgétaires et techniques, à déployer sur les trois prochaines années. Cette stratégie est conçue pour produire des résultats accessibles dès 2025, tout en orientant de manière cohérente et durable l'action en matière d'intelligence artificielle.

Remis également à un Observatoire de l'IA, qui aura pour mission d'en assurer la mise en œuvre, ce rapport synthétise les recommandations clés et la feuille de route préconisée, avec un calendrier de déploiement prévisionnel des différentes fonctionnalités pour chaque catégorie d'usagers. Nous avons veillé à ce que cette feuille de route soit progressive, réaliste et adaptable, afin de permettre un déploiement rapide des outils les plus utiles, tout en assurant une montée en compétences progressive des agents.

Je suis convaincu que les opportunités offertes par l'IA pouvant bénéficier à la Justice sont considérables, comme l'attestent les nombreux cas d'usage recensés auprès des agents du ministère. En saisissant cette opportunité unique, nous pourrons répondre aux attentes des usagers en matière d'accessibilité et d'amélioration de la qualité du service public et de l'activité juridictionnelle, tout en améliorant l'efficacité et les conditions de travail des agents.

Haffide Boulakras

Synthèse des propositions

Dans le cadre de la présente mission, il est recommandé d'orienter prioritairement l'action ministérielle autour de trois axes stratégiques complémentaires.

Le premier ambitionne de démocratiser l'accès à l'intelligence artificielle pour l'ensemble des acteurs de la Justice, en privilégiant le développement et la diffusion d'outils opérationnels, directement intégrables aux pratiques professionnelles quotidiennes.

Le second s'inscrit dans une démarche affirmée de préservation de la souveraineté technologique en veillant à assurer la maîtrise effective des dispositifs déployés.

Enfin, la troisième orientation porte sur l'accompagnement des professionnels, et de respect des exigences éthiques, conditions indispensables à la réussite de cette transformation : il convient de garantir à chacun les moyens de se former, de s'approprier les nouveaux outils et de s'adapter avec confiance aux mutations en cours.

UNE IA POUR TOUS : DES OBJECTIFS CONCRETS AU SERVICE DES MÉTIERS DE LA JUSTICE

► **Proposition 1** : Déployer, **dès 2025, un assistant IA sécurisé et souverain** dédié à l'ensemble des magistrats et agents du ministère de la Justice, intégrant progressivement des fonctions de recherche, de synthèse, de rédaction et de retranscription.

► **Proposition 2** : Faire **l'acquisition dès 2025 de licences** permettant l'usage de solutions de recherches juridiques augmentées par l'IA.

► **Proposition 3** : Déployer, à compter de **2026, des outils dédiés** pour accompagner les **12 cas d'usage**[1] **métiers jugés prioritaires** par la mission, en raison de leur impact, de leur faisabilité et de leur alignement avec les orientations stratégiques du ministère.

[1] Voir la liste des cas d'usage priorisés en 3.B du rapport

UNE STRATÉGIE SOUVERAINE : PILOTER L'INTÉGRATION DE L'IA DANS LA DURÉE

► **Proposition 4** : Constituer une équipe en charge de la conduite opérationnelle de la stratégie IA, sous la forme d'une **direction de programme**, intégrant les expertises techniques, métier, juridiques et éthiques appliquées à l'IA et dimensionnée en fonction des cas d'usage retenus, rattachée au Secrétariat Général du Ministère.

► **Proposition 5** : Instituer auprès du Ministre de la Justice un **Observatoire de l'IA** chargé de piloter sa stratégie d'intégration, d'assurer un suivi éthique des usages, leur impact sur les métiers, ou encore de garantir une veille scientifique régulière pour actualiser la compréhension de l'IA dans la Justice.

► **Proposition 6** : En 2025, installer un environnement d'**hébergement numérique souverain** (SecNumCloud[2]) pour déployer au plus tôt les cas d'usage (dont l'assistant IA), suivi d'un **transfert progressif vers les infrastructures internes** du ministère de la Justice.

► **Proposition 7** : Engager des travaux visant à **faire évoluer le cadre réglementaire national**, en veillant à leur cohérence avec les principales normes européennes (règlement européen sur l'IA, Directive Police-Justice, RGPD).

FORMER, OUTILLER, SÉCURISER : UN ACCOMPAGNEMENT À LA HAUTEUR DES ENJEUX ÉTHIQUES, HUMAINS ET JURIDIQUES

► **Proposition 8** : Diffuser une **charte d'usage des outils d'IA** à destination des utilisateurs ainsi que des **principes directeurs éthiques**, à destination des concepteurs-développeurs des outils d'IA, et créer un **label « IA digne de confiance »** afin d'encadrer l'usage des solutions proposées par des éditeurs juridiques et « legaltech ».

► **Proposition 9** : Mettre à la disposition des magistrats et agents **l'outil d'aide à la conformité** développé par la mission, incluant notamment un arbre décisionnel juridique, afin de faciliter la compréhension du cadre juridique applicable aux projets IA

► **Proposition 10** : Créer un « **campus du numérique** » dédié à la Justice, afin de sensibiliser les magistrats et agents aux enjeux de l'intelligence artificielle, de les accompagner dans l'appropriation des outils numériques et de leur proposer des formations adaptées à l'évolution des pratiques professionnelles et aux exigences éthiques

[2] Élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique, pour les fournisseurs de services Cloud.

Feuille de route pour la mise en œuvre

2025

PHASE 1 – ÉMERGENCE ET PREMIERS DÉPLOIEMENTS

Lancement rapide de services d'IA à fort impact. Cette première étape vise à poser les bases d'un écosystème sécurisé, conforme et évolutif.

Livrables :

- Mise à disposition progressive d'un **assistant IA fondé sur un grand modèle de langage** (LLM) généraliste opérationnel pour l'extraction d'informations, la synthèse et la rédaction ;
- **Acquisition des licences** d'outils proposant de la recherche juridique augmentée par IA ;
- Mise à disposition d'un **arbre décisionnel juridique** alignant les exigences nationales et européennes (RIA, RGPD) ;
- Diffusion d'une **charte d'utilisation des outils d'IA**, des **principes directeurs de conception de l'IA** ainsi qu'un cahier des charges pour l'audit éthique des solutions.

Gouvernance et accompagnement :

- Favoriser **l'internalisation des compétences en IA** en constituant une équipe resserrée, sous la forme d'une direction de programme, composée de référents métier, chefs de produit IA, de data scientists et de spécialistes des grands modèles de langage (LLM), et en responsabilisant cette équipe en lui accordant la marge de manœuvre nécessaire pour livrer les premiers résultats dans les délais attendus ;
- Créer l'**Observatoire de l'IA pour la Justice** afin de piloter la stratégie d'intégration de l'IA, suivre les indicateurs d'impact, coordonner les acteurs concernés, et organiser une revue des avancées ;
- Lancement des premières sessions de **sensibilisation** et des modules de **formation** adaptés.

Investissements :

- Allouer un budget initial pour assurer l'**hébergement** des grands modèles de langage en source libre (open-source) sur un **serveur sécurisé et souverain**, recruter les compétences nécessaires et intégrer les premiers outils.
- Prévoir un budget complémentaire, principalement destiné à l'**achat de licences** pour des solutions disponibles sur le marché.

2026 - 2027

PHASE 2 – MONTÉE EN COMPÉTENCES ET MODULARISATION

Développement de modules métiers à forte valeur ajoutée pour renforcer l'efficacité du service judiciaire et préparation de la souveraineté technologique.

Livrables :

- Développer et livrer des **modules spécialisés d'IA** répondant aux **cas d'usage métier priorisés** par la mission (synthèse avancée de dossiers de procédure, aide à la rédaction de décisions, …) ;
- Ajouter un module généraliste de **retranscription** à l'assistant IA ;
- **Installer en interne** les infrastructures d'hébergement et la puissance de calcul requises, tout en acquérant les outils pour gérer les modèles tout au long de leur vie ;
- Mettre en place un **tableau de bord** pour mesurer les gains, la qualité et l'adoption des outils ;
- Mise en place d'un **label « IA digne de confiance »** piloté avec les partenaires professionnels (avocats notaires, commissaires de justice…), la CNIL et la DINUM, assorti d'un audit éthique et technique externe annuel.

Gouvernance et accompagnement :

- Passage à une **gouvernance pérenn**e de l'Observatoire de l'IA et intégration de la dimension IA au comité stratégique de la transformation numérique.
- **Renforcement de l'équipe** avec des *data scientists*, spécialistes de la recherche et développement, expert cybersécurité ou coordonnateur de formation, et la rattacher directement au secrétaire général à très haut niveau ;
- Déploiement du **Campus numérique Justice**, proposant des parcours experts et des modules sur l'architecture IA et le pilotage du changement.

Investissements :

- Augmenter le budget pour permettre la recherche et le développement de **nouveaux modules**, automatiser davantage les processus et améliorer l'intégration avec les outils informatiques déjà en place.
- Constitution d'une **équipe interne complète dédiée à l'IA**, qui se structure en groupes spécialisés ('squads'), réunissant des compétences en produit, métier, data science et développement, afin de répondre efficacement à des besoins et projets spécifiques.

2028
+

PHASE 3 – CONSOLIDATION ET PÉRENNISATION

Faire de l'IA un pilier structurant de la Justice, aligné sur les standards européens et porteur d'une culture d'innovation durable.

Livrables :

- **Transfert complet des solutions vers l'infrastructure interne** avec des niveaux de service garantis ;
- Publication d'un **rapport annuel public sur l'impact de l'IA** dans la Justice (indicateurs, retours d'expérience, perspectives) ;
- **Exploration** de **nouveaux cas d'usage** et développement de solutions ;

Gouvernance et accompagnement :

- Installation d'un **comité stratégique annue**l chargé de l'évaluation des indicateurs clés, de la priorisation des projets, des arbitrages budgétaires et du suivi de la feuille de route innovation ;
- Déploiement d'un **programme d'acculturation continue** (MOOC, hackathons, laboratoire d'expérimentation).

Investissements :

- Allouer un budget pour renforcer et agrandir le **centre de données** (data center), assurer son entretien, et mettre en place un plan de continuité d'activité afin de garantir la sécurité et la disponibilité des services, même en cas d'incident.

	Émergence et premiers déploiements 2025	Montée en compétence et modularisation 2026-2027	Consolidation et pérennisation 2028 et après
Objectifs	• **Lancer des services d'IA à fort impact** • **Poser les bases d'un écosystème sécurisé, conforme et évolutif**	• **Développer des modules métiers à forte valeur ajoutée pour renforcer l'efficacité du service judiciaire** • **Préparer la souveraineté technologique**	• **Faire de l'IA un levier structurant, aligné avec les standards européens et porteur d'une culture d'innovation durable**
Actions clés	• **Déploiement d'un assistant IA (extraction, synthèse, rédaction)** • Achat de licences pour outils de recherche juridique augmentée • Mise à disposition d'un arbre décisionnel juridique alignant les exigences nationales et européennes (RIA, RGPD) • Diffusion d'une charte éthique aux usagers et aux concepteurs de solutions • Recrutement/ constitution d'une équipe projet pluridisciplinaire • Création de l'Observatoire de l'IA pour la Justice, organe de pilotage de la stratégie • Lancement des premières formations	• **Développement du module généraliste de retranscription** • **Développement de modules IA spécialisés (synthèse avancée de dossiers de procédure, aide à la rédaction de décisions, etc.)** • Investissement en infrastructures internes de calcul et d'hébergement • Création d'un label « IA digne de confiance » avec audit externe annuel pour les solutions de marché • Gouvernance renforcée et pérenne (comité stratégique trimestriel, tableau de bord) • Lancement du « Campus du numérique » Justice, commun aux quatre écoles du MJ	• **Développement de nouveaux cas d'usage** • Transfert total des solutions sur infrastructure interne • Comité stratégique annuel (pilotage et priorisation) • Rapport public annuel sur les impacts IA • Programme d'acculturation continue (MOOC, hackathons)

Sommaire

INTRODUCTION

Les positions exprimées à l'égard de l'IA dans le domaine judiciaire sont souvent portées sur le sujet de la Justice dite prédictive et sur la question, controversée, d'un éventuel remplacement du juge ou de l'avocat par la machine. Cette focalisation, conjuguée à la nouveauté de la technologie, a entretenu une attitude de réserve largement partagée au sein des milieux professionnels et académiques[3].

Une telle prudence, compréhensible à l'aune des incertitudes techniques, éthiques et juridiques qui entourent encore l'IA, a eu pour effet de restreindre la portée des réflexions engagées sur ses apports potentiels au monde de la Justice.

Alors que l'IA s'intègre déjà dans les pratiques de juridictions étrangères, d'administrations françaises et chez les auxiliaires de Justice[4], elle n'est plus un simple sujet théorique, mais un outil structurant. Selon le récent rapport du Sénat sur l'impact de l'IA dans les professions du droit[5], l'utilisation croissante de l'IA par les avocats, facilitant la production d'actes juridiques et l'engagement des procédures, devrait mécaniquement augmenter les entrées contentieuses en juridiction et le volume des écritures. Elle impose d'adapter l'organisation et les outils de la Justice pour relever ces nouveaux défis. En ce sens, le rapport de la Cour de cassation d'avril 2025 documente le bénéfice d'outils permettant d'analyser les écritures, de repérer les litiges connexes ou sériels, et d'assister la rédaction, tout en garantissant une maîtrise humaine, éthique et souveraine de ces technologies[6]. De plus, l'utilisation d'outils d'IA grand public dans un cadre professionnel par certains acteurs judiciaires, avec les facteurs de risque qu'elle comporte, est devenue une réalité qui ne peut plus être occultée et à laquelle il convient d'apporter des réponses concrètes.

Il apparaît désormais que l'IA constitue un levier majeur de transformation pour la Justice, en ouvrant des perspectives nouvelles en matière d'efficacité, d'accessibilité et de qualité du service rendu. La capacité de ces systèmes à produire et traiter de vastes volumes d'informations, à assister la rédaction ou à automatiser certaines tâches répétitives, chronophages ou à faible valeur ajoutée pour les magistrats et agents, représente un puissant vecteur d'évolution.

Cette dynamique doit impérativement s'accompagner d'une vigilance soutenue afin d'assurer la protection des droits fondamentaux et de maintenir la confiance des citoyens à l'égard de l'institution judiciaire.

Parallèlement, il est essentiel d'adopter une approche renouvelée : l'appropriation progressive de ces outils, appuyée par des expérimentations concrètes sur le terrain, doit permettre de dépasser les inquiétudes initiales et d'envisager l'IA comme une opportunité au service de la Justice. Ce n'est qu'en surmontant les réticences initiales, grâce à une mise en œuvre maîtrisée et à un accompagnement adapté, que l'IA pourra être reconnue comme une véritable opportunité au service de la Justice.

À cette condition, l'IA constituera un appui fiable pour renforcer l'efficacité, la transparence et l'accessibilité du service public de la Justice, dans le respect des principes fondamentaux de l'État de droit.

[3] V. par exemple Camille Bordère. La Justice algorithmique: analyse comparée (France/Québec) d'un phénomène doctrinal. Droit. Université de Bordeaux, 2023

[4] Le CNB et Lefebvre Dalloz lancent un plan national de formation à l'IA pour les avocats et élèves avocats | Conseil national des barreaux

[5] L'IA générative et les métiers du droit : agir plutôt que subir - Sénat

[6] Préparer la Cour de cassation de demain - Cour de cassation et intelligence artificielle - Cour de cassation, avril

Ce rapport s'inscrit donc dans une démarche résolument pragmatique et vise avant tout l'opérationnalité. Il ne cherche pas à aborder les questions théoriques autour de l'IA, mais à proposer des recommandations concrètes, directement applicables dans le contexte juridique et institutionnel actuel.

En réponse également aux défis identifiés lors des États Généraux de la Justice[7], nous analysons les moyens par lesquels l'IA peut transformer les activités judiciaires, en nous appuyant sur des exemples recueillis auprès des acteurs de terrain du ministère. Notre approche intègre les contraintes juridiques, budgétaires et techniques. La question de la qualité et de l'accessibilité des données, qui jouera un rôle croissant dans le développement futur de l'IA, est également prise en compte.

Ce rapport, destiné également à un futur Observatoire de l'IA, préconise une mise en œuvre progressive, associant le déploiement rapide d'outils généralistes, comme une plateforme de services IA, au développement de solutions métiers plus ciblées, tout en accordant une attention particulière à la gouvernance, à la formation et à l'accompagnement des magistrats et agents.

[7] Le rapport des États généraux de la Justice | Ministère de la Justice 2025

1. LES OPPORTUNITÉS OFFERTES PAR L'IA AU SERVICE DE LA JUSTICE SONT CONSIDÉRABLES, COMME L'ATTESTENT LES CAS D'USAGE RECENSÉS AUPRÈS DES MAGISTRATS ET AGENTS DU MINISTÈRE DE LA JUSTICE

A. L'IA offre une opportunité unique d'amélioration au profit des agents et des usagers

S'appuyant sur les conclusions éclairantes des **États Généraux de la Justice**[8], qui ont notamment pointé avec insistance les **difficultés d'accès au droit**, l'**engorgement des tribunaux**, la **surcharge de travail** pesant sur les magistrats et les personnels, l'**allongement des délais de jugement** ainsi que la nécessité impérieuse de **moderniser les outils** et méthodes de travail pour restaurer le sentiment de justice, le présent rapport explore le potentiel transformateur de l'IA pour améliorer concrètement et rapidement le fonctionnement du service public de la Justice.

À l'instar de ce qui a été observé dans d'autres secteurs d'activité, l'**émergence d'IA génératives**, que le grand public découvre à travers des agents conversationnels tels que ChatGPT, Gemini ou Le Chat, a suscité un vif intérêt au sein du ministère de la Justice. Si les enquêtes récentes révèlent qu'environ **13,5 % des agents de la fonction publique** déclaraient en juin 2024 **utiliser déjà ces outils** dans le cadre de leurs fonctions[9], une proportion bien plus importante a eu l'occasion d'en expérimenter les potentialités dans leur sphère privée. Cette familiarité croissante avec l'IA, bien que variable selon les profils et les métiers, constitue un atout indéniable pour faciliter son adoption dans les pratiques professionnelles, à condition d'en maîtriser les risques et d'en exploiter pleinement les avantages.

Au regard des défis considérables auxquels la Justice est confrontée, et tels qu'ils ont été clairement identifiés et débattus lors des États Généraux, l'IA se présente comme une véritable opportunité pour :

- **Améliorer l'accès au droit pour tous les justiciables :** En développant des outils d'information juridique accessibles au grand public et faciles d'utilisation, capables de présenter des textes complexes en termes simples et d'orienter les justiciables vers les services compétents (associations, consultations gratuites, etc.), l'IA peut contribuer efficacement à renforcer l'accessibilité au système judiciaire par les justiciables, y compris pour les publics suivis par l'administration pénitentiaire (AP) et la protection judiciaire de la jeunesse (PJJ).

- **Alléger la charge de travail des magistrats et des autres agents :** En automatisant les tâches répétitives et chronophages, comme la recherche documentaire, la rédaction de documents (y compris les décisions judiciaires sous le contrôle du magistrat), le tri et le classement des dossiers, ou encore la retranscription et la synthèse d'entretiens, un temps précieux est libéré. Ce temps peut alors être consacré à des activités à plus forte valeur ajoutée : analyse juridique, accueil et écoute des justiciables, tenue d'audiences, accompagnement et suivi individualisé des personnes sous main de justice. Cela permet aussi de recentrer les magistrats et agents du ministère sur l'essentiel de leurs missions mais également de réduire les délais de traitement des procédures.

- **Contribuer à une meilleure qualité et cohérence des décisions de Justice :** En fournissant aux magistrats des outils de recherche assistés par IA basés sur l'analyse rigoureuse de la jurisprudence, des données factuelles et des éléments de contexte pertinents, l'IA peut contribuer à la présélection de dossiers propices à l'amiable, à garantir une application plus uniforme et prévisible du droit, à identifier la solution la plus adaptée qu'il s'agisse d'une affaire

[8] En 2022, à l'occasion des États généraux de la Justice, près de 50.000 citoyens, acteurs et partenaires de la Justice ont formulé des propositions pour bâtir la Justice de demain. Le comité indépendant chargé de synthétiser ces propositions a remis son rapport au président de la République le 8 juillet 2022. Consulter le rapport des États généraux de la Justice | Ministère de la Justice

[9] Source : Sondage réalisé par Acteurs Publics sur 2064 agents publics en mai 2024, partagé lors de l'édition spéciale « Les agents publics face à la vague de l'IA », Acteurs Publics, juin 2024 Édition_spéciale_numérique.pdf

civile (résolution du litige) ou pénale, tout en laissant au juge le soin d'apprécier la situation particulière de chaque justiciable.

- **Optimiser l'organisation et le fonctionnement des services :** L'IA peut être mise à profit pour améliorer la gestion des flux de dossiers, anticiper les besoins en ressources (humaines, matérielles, financières), faciliter la gestion des plannings des personnels (dont leurs astreintes, temps de formation…), des salles d'audiences, des places en détention et des parcours de personnes sous mains de Justice, faciliter la communication et la coordination entre les différents acteurs au sein des juridictions, de l'administration pénitentiaire ainsi qu'avec leurs partenaires (force de sécurité intérieure, services de Santé et autres service de l'État, collectivités, monde associatif…).

- **Accompagner la formation continue et le développement des compétences des magistrats et agents :** En proposant des modules d'apprentissage personnalisés, des simulations de situations professionnelles plus complètes et réalistes, des outils d'aide à la traduction et à la documentation juridique et administrative, l'IA peut soutenir la montée en compétence de tous les métiers judiciaires, de la PJJ et pénitentiaires et ainsi faciliter l'adaptation aux évolutions constantes de leurs fonctions tout en favorisant une culture professionnelle innovante, centrée sur la qualité du service rendu[10].

L'expérience internationale offre des repères précieux pour bâtir une Justice numérique à la fois performante, éthique et humaine. Longtemps cantonnée à la sphère théorique, l'IA judiciaire est désormais une réalité opérationnelle dans certains pays. Plusieurs États ont franchi le pas en intégrant l'IA dans le fonctionnement quotidien de leurs juridictions, avec des approches encadrées et progressives.

Les expériences étrangères démontrent que l'IA dans le domaine de la Justice n'est plus une expérimentation marginale, mais une **composante structurante du service public de la Justice**. Ce mouvement mondial, bien que non coordonné, repose sur des principes partagés : maîtrise des risques, transparence des algorithmes, respect des droits fondamentaux et supervision humaine systématique, qui peuvent utilement éclairer la réflexion sur l'usage de l'IA au sein du système judiciaire français.

10 S'appuyant sur les travaux de la CEPEJ, il est désormais acquis que l'IA offre des perspectives considérables pour optimiser le fonctionnement de la Justice. Ces outils, qui couvriraient un large spectre d'applications, de la gestion des documents à l'aide à la décision, en passant par l'anonymisation et la traduction, viseraient à améliorer l'efficacité, la précision et la rapidité des processus judiciaires, tout en facilitant l'accès au droit pour les citoyens.

Encadré – Les exemples étrangers d'usage de l'IA en matière judiciaire

Si des pays comme la Chine, les États-Unis ou les Émirats arabes unis illustrent des cas d'usage avancés de l'IA dans le domaine judiciaire, leurs approches demeurent relativement éloignées du contexte français.

Le Canada, en revanche, s'est doté de lignes directrices spécifiques pour encadrer l'usage de l'IA par ses tribunaux, fondées sur la vigilance algorithmique, la supervision humaine et la transparence des décisions assistées par IA.

Au Brésil, où la justice fait face à une surcharge chronique, l'intelligence artificielle est déployée à grande échelle pour optimiser les flux judiciaires, automatiser le tri et la classification des dossiers, et assister la rédaction des jugements, tout en préservant pleinement l'autorité du juge. Le pays constitue un exemple inspirant pour la justice française, car il a su conjuguer une politique ambitieuse de développement technologique avec une réglementation et un contrôle éthique rigoureux. La stratégie brésilienne privilégie le développement internalisé des outils d'IA, chaque tribunal disposant de ses propres ressources et collaborant parfois avec des universités, dans une logique d'interopérabilité et de partage des bonnes pratiques. Parmi les solutions déployées, on trouve Victor, un système d'aide à la décision du Tribunal suprême fédéral qui automatise la conversion, la classification et l'organisation des documents, ainsi que de nombreux outils pour l'accueil du public (chatbots comme « o Judi »), la gestion administrative (ATHOS, LARRY) ou le regroupement d'affaires similaires. Ces technologies permettent d'accélérer le traitement des procédures, de réduire les délais et de désengorger les tribunaux, tout en assurant une supervision humaine et le respect strict des principes éthiques et juridiques.

En Espagne, la modernisation numérique de la Justice s'est accompagnée d'une politique volontariste d'intégration de l'IA, soutenue par des textes législatifs récents. Les outils déployés permettent notamment d'automatiser la transcription des débats, d'accélérer le traitement des antécédents judiciaires ou d'anonymiser les décisions, le tout dans un cadre éthique rigoureux et transparent. Au niveau européen, la Charte éthique de la CEPEJ rappelle que l'IA doit demeurer un outil au service de l'intérêt général, utilisé dans le respect des droits fondamentaux et sous contrôle humain effectif.

B. Les acteurs de terrain et les directions d'administration centrale, consultés dans le cadre de la mission, ont exprimé leurs attentes vis-à-vis de l'IA à travers 60 cas d'usage, reflétant des besoins métiers à forts enjeux tant pour les magistrats et agents que pour les justiciables

Dans le cadre de la présente mission, des acteurs de terrain, les directions du ministère de la Justice et leurs services déconcentrés ont été sollicités pour identifier des « cas d'usage ». Ces « cas d'usage » désignent des « situations » rencontrées par les magistrats et agents dans l'exercice de leurs métiers (magistrat, greffier, équipe juridictionnelle - attaché de Justice, assistant de Justice ou assistant spécialisés-, cadre et surveillant pénitentiaire, acteur de la protection judiciaire de la jeunesse, agent d'administration centrale, etc.), soulevant des irritants ou des besoins spécifiques (perte de temps, risque pour la qualité de service, tâche à faible valeur ajoutée) et **face auxquels une solution IA pourrait apporter une amélioration significative.**

Une soixantaine de cas d'usage a été recensée dans le cadre de cet exercice. Malgré la diversité des acteurs sondés, des besoins convergents ont émergé exprimant notamment **des besoins d'appui aux tâches d'analyse, de synthèse, de recherche, de retranscription et de traduction -** des tâches répétitives et chronophages susceptibles de ralentir le traitement des affaires dans les tribunaux et l'avancement des dossiers au sein des administrations centrales. Des **besoins plus spécifiques à certaines réalités métiers** ont également été exprimés dans 60% des cas, notamment dans les réseaux de l'administration pénitentiaire et ceux de la protection judiciaire de la jeunesse. Une attention particulière a également été portée **aux besoins d'information et d'orientation du justiciable**. Enfin, d'autres cas d'usage ont concerné des besoins organisationnels, visant principalement à **mieux optimiser les ressources et les compétences notamment dans les tribunaux**.

1.B.1. Mieux collecter, analyser et traiter un large volume d'informations dans des délais resserrés

La Justice est confrontée à des situations où elle doit traiter une **masse importante d'informations** ou de **dossiers**. Ce besoin de gestion à grande échelle se manifeste dans plusieurs contextes majeurs : le traitement des contentieux dits de masse, l'analyse de nombreux documents dans les dossiers et la recherche juridique.

1.B.2. L'aide au traitement des contentieux de masse

Les **contentieux de masse**, se caractérisant par un important flux entrant de dossiers judiciaires aux attributs similaires, sont de nature à **engorger les juridictions** et à entraîner des délais de traitement conséquents des procédures. Une **aide à l'orientation de ces procédure**s, à la **détection des séries et des doublons de saisines** et à leur traitement permettrait de diminuer les délais dans lesquels les décisions sont rendues et d'harmoniser les décisions. Le ministère de la Justice français a obtenu en 2025 un appui technique de la Commission européenne[11] concernant le traitement du contentieux de masse, dont le contentieux aérien, démontrant ainsi l'actualité et l'importance du sujet.

1.B.3. Une aide à l'analyse, la synthèse et la comparaison d'un volume important de pièces de procédures afin de garantir un traitement plus efficace et accéléré des affaires

Les magistrats et les professionnels qui les entourent (attachés de Justice, assistants de Justice, assistants spécialisés) font face à **des volumes importants et croissants de documents, pièces et actes de procédure** qu'ils doivent analyser, synthétiser et comparer afin de recouper des éléments susceptibles d'éclairer la résolution d'un dossier. À ce jour, ce travail repose pour partie sur une démarche manuelle, fondée sur les synthèses individuelles et les prises de notes réalisées par les acteurs au fil de leur consultation des différentes pièces du dossier. Les solutions d'IA pourraient renforcer de manière significative la capacité d'action des magistrats et ceux qui les assistent, notamment pour :

- **prendre rapidement connaissance** d'une procédure grâce à une description objective de ses éléments clés ;
- **analyser la complétude et la régularité procédurale** d'un dossier et détecter de potentielles carences ou nullités ;
- **examiner les convergences et divergences** entre différentes pièces du dossier (constatations, témoignages, auditions, documents divers) ;
- **rapprocher des éléments clés entre eux** (par exemple, mettre en relation un numéro déclaré par une personne et l'exploitation de factures détaillées) ;
- **identifier rapidement un élément précis** au sein d'un dossier volumineux.

1.B.4. Un accès facilité aux jurisprudences et aux textes juridiques permettant d'éclairer les décisions de Justice

L'aide à la recherche juridique pour les magistrats et les membres de l'équipe juridictionnelle est un besoin identifié par la mission, notamment la recherche de précédents et de blocs de motivation dans des dossiers similaires. Actuellement, les magistrats doivent effectuer des recherches manuelles et chronophages à travers divers moteurs de recherche, bases de données privées (Dalloz, Lexis Nexis…) et bases de la Cour de cassation (Jurica, Jurinet) ainsi que sur le site internet de la Cour de cassation Judilibre concernant les décisions de justice en open data. Cette multiplicité de sources à consulter entraînant une **longue recherche est particulièrement problématique dans les contentieux techniques** nécessitant des **recherches rapides et décisions urgentes et pour les magistrats généralistes**. Cette situation est gérée de **manière artisanale**, avec des bibliothèques de motivation personnelles, non partagées et non pérennes. La résolution de ce problème permettrait un gain de temps significatif, une meilleure qualité et harmonisation des décisions, et une réduction de l'aléa judiciaire, bénéficiant ainsi aux magistrats

[11] Automation of routine tasks in judicial proceedings (ARTJP) site de la Commission européenne France - European Commission

civilistes et pénalistes et, *in fine*, aux justiciables. Une solution basée sur l'IA **pourrait accélérer cette recherche juridique**. Elle pourrait par ailleurs proposer des blocs de motivation adaptés et personnalisés selon les préférences du magistrat.

1.B.5. Accélérer la mise en texte et la traduction de tous les entretiens et documents utiles aux métiers de la Justice

La retranscription écrite et automatisée des propos tenus oralement constitue une attente forte des magistrats et agents du ministère de la Justice, au niveau central comme local. Elle est utile dans différents contextes administratifs et judiciaires pour les comptes-rendus de réunion, les comptes-rendus d'entretien, d'audition et d'audience. La retranscription « manuelle » est en effet perçue comme particulièrement chronophage, entravant la spontanéité des échanges. Par exemple, plusieurs étapes de la procédure pénale nécessitent la retranscription fidèle des déclarations, qu'il s'agisse de la phase d'instruction (interrogatoires, confrontations) ou de la phase d'audience (déclarations du prévenu ou de l'accusé, témoignages, interventions des victimes et des avocats) ; de même en est-il pour les audiences de cabinet en matière civile (devant le juge des enfants ou devant le juge des tutelles). L'automatisation de la retranscription des échanges contribuerait également à garantir une meilleure continuité dans la prise en charge de certains publics. C'est notamment le cas des jeunes suivis par la Protection judiciaire de la jeunesse (PJJ), dont les dossiers pourraient être enrichis des comptes rendus d'entretiens et d'audiences, offrant ainsi aux référents (éducateurs, psychologues, assistants de service social, cadres) une vision plus complète pour accompagner au mieux chaque situation.

Par ailleurs, au-delà des besoins de retranscription, les magistrats et agents du ministère ont également exprimé le besoin de disposer **d'outils de traduction** permettant de convertir à l'écrit, en français, les propos tenus oralement dans une langue étrangère.

1.B.6. Soutenir des réalités métiers fortes : le cas de l'administration pénitentiaire et les enjeux de surveillance des personnes détenues

Les retours de l'administration pénitentiaire mettent en lumière le potentiel qu'offre l'intelligence artificielle pour renforcer les **capacités d'analyse au sein des établissements pénitentiaires** afin de permettre une **meilleure gestion des risques** et ainsi contribuer à la p**rotection et à la sécurité des personnes**, tout en rappelant l'importance de respecter scrupuleusement le cadre juridique et éthique en vigueur. Plusieurs exemples d'application ont ainsi été identifiés tels que la vidéosurveillance intelligente pour détecter les comportements suspects, la surveillance des conversations téléphoniques des personnes détenues, l'interprétariat instantané hors connexion pour surmonter la barrière linguistique entre les agents pénitentiaires et les détenus étrangers ou encore la détection vidéo-intelligente pour renforcer la lutte anti-drônes.

1.B.7. Renforcer l'efficacité de l'accueil et orientation des justiciables via une assistance IA

Afin de **mieux orienter les justiciable**s, en particulier les plus vulnérables, les agents du ministère de la Justice expriment le besoin d'être mieux outillés et informés. Ils sont en effet confrontés à la nécessité d'**expliquer des procédures nombreuses et complexes**, de **clarifier des décisions écrites** dans un langage juridique souvent difficile d'accès, et de **maîtriser un volume important de normes et de procédures**, dont l'**intelligibilité** n'est pas toujours assurée. Ainsi, une solution IA pourrait être mise à la disposition des agents du SAUJ (service d'accueil unique du justiciable) de chaque tribunal, chargés notamment de délivrer de l'information générale et particulière sur les procédures à tous les justiciables qui en expriment le besoin au guichet physique, dans les tribunaux, ou par voie téléphonique. Les professionnels de terrain de la PJJ expriment également le souhait de bénéficier d'un agent conversationnel juridique afin de mieux appréhender le volume croissant de normes encadrant leurs missions.

1.B.8. Renforcer les capacités d'organisation au sein des juridictions afin d'optimiser les ressources et les compétences dans un contexte RH contraint

Plusieurs cas d'usage recensés traduisent les **difficultés d'organisation interne des tribunaux**, dans un contexte marqué par l'augmentation des stocks d'affaires et l'allongement des délais de procédure. Il s'agit plus particulièrement de mieux orienter les dossiers au sein des juridictions et d'optimiser les plannings en veillant à répartir équitablement la charge de travail et à tenir compte de la durée anticipée des procédures.

C. Pour éclairer la stratégie IA du ministère de la Justice, les cas d'usage ont été priorisés en croisant trois dimensions : l'impact, la faisabilité et l'alignement avec les priorités stratégiques du ministère

Pour orienter efficacement les choix d'investissement en matière d'IA, la mission a élaboré une **méthode de priorisation** permettant d'ordonner les cas d'usage identifiés selon **leur potentiel de transformation** (impact), leur **faisabilité** et leur **pertinence stratégique**. L'objectif est de concentrer les efforts sur les cas d'usage les plus impactant pour les agents et/ou les usagers, les plus rapidement déployables et les mieux alignés avec les priorités politiques du ministère.

Encadré – Méthode de priorisation des cas d'usage

La priorisation des cas d'usage repose sur une analyse croisant l'impact potentiel, la faisabilité technique, juridique, et financière et le caractère stratégique du projet pour le ministère.

L'impact potentiel repose sur l'estimation des bénéfices attendus, qu'ils touchent les **magistrats et agents** ou les **justiciables**.

- **Pour les magistrats et agents**, les gains attendus comprennent l'amélioration de l'efficacité par des économies de temps, le renforcement de la fiabilité de leurs actions par une réduction des erreurs, ainsi que l'amélioration des conditions de travail et donc de l'attractivité des fonctions par l'allègement des tâches répétitives, pénibles et sans forte plus-value.
- **Pour les justiciables**, les avantages potentiels concernent la réduction des délais des procédures judiciaires et du traitement des demandes à l'administration, l'amélioration de l'accessibilité au service de la Justice et de sa transparence.

La faisabilité intègre trois dimensions : les efforts techniques, les coûts tant sur le plan budgétaire qu'environnemental pour assurer une utilisation frugale et responsable de l'IA visant à maximiser l'impact tout en minimisant les coûts, et la charge de mise en conformité juridique.

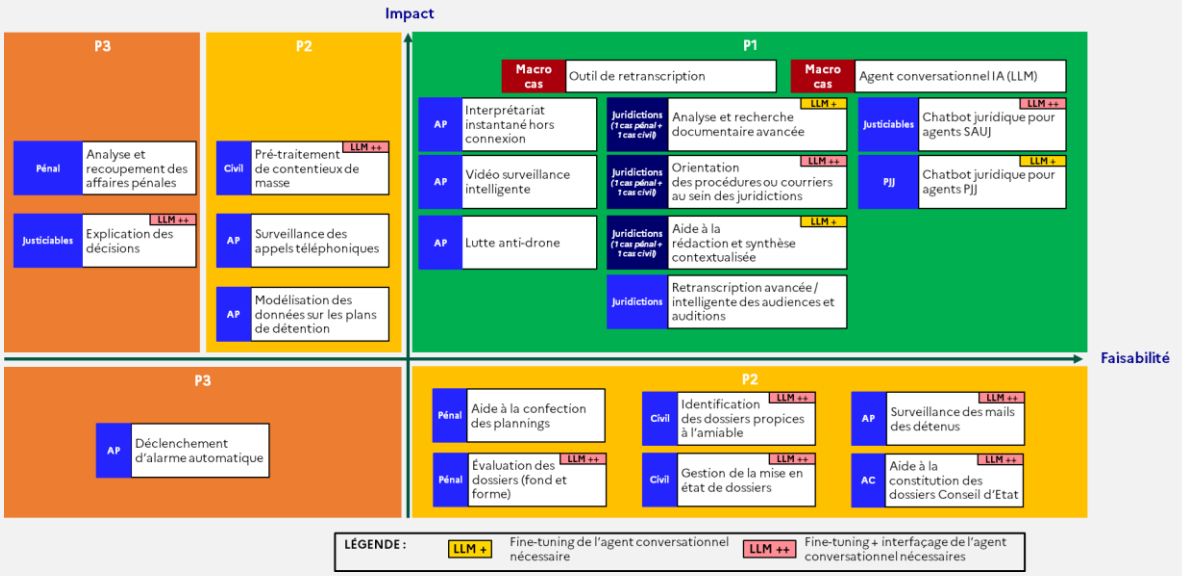
La dimension stratégique du projet reflète l'importance accordée au projet par les différents échelons décisionnels, depuis l'absence de priorité particulière jusqu'à l'inscription dans une politique prioritaire du gouvernement (PPG).

Cette méthode structurée a permis notamment de catégoriser des projets à **plusieurs niveaux de maturité** :

- **Des briques technologiques transverses à impact fort**
- **Des projets spécifiques à fort impact et faisabilité élevée, à prioriser**
- Des projets à fort impact mais plus complexes, à planifier dans le temps
- Des projets à impact plus limité mais faciles à réaliser, à temporiser

Encadré – Matrice de priorisation des cas d'usage

Grâce aux différentes informations remontées, la mission a pu évaluer l'impact et la faisabilité des cas d'usage remontés et les prioriser dans la matrice suivante :



Un **contrôle de la pertinence** des projets au regard du périmètre de la présente mission IA a également été réalisé et a conduit à écarter environ un tiers des cas d'usage remontés pour les raisons suivantes : des besoins qui ne relèvent pas de l'IA mais qui peuvent être adressés par des solutions numériques simples, des problèmes utilisateurs et leur mesure d'impact associée trop imprécis, un nombre d'utilisateurs potentiel trop faible au vu des coûts et efforts nécessaires à la mise en place de la solution.

2. PRÉREQUIS AU DÉVELOPPEMENT DE L'IA DANS LA JUSTICE : EXPLICITATION DU CADRE RÉGLEMENTAIRE, ÉLABORATION D'UN CADRE ÉTHIQUE ET CONSTRUCTION D'UN SOCLE DE DONNÉES FIABLES ET STRUCTURÉES

Reprenant à notre compte une thèse développée par Simon Bernard[12], il nous semble que **l'Europe ne doit pas choisir entre innovation et régulation, mais articuler les deux** pour faire du droit un levier stratégique de souveraineté et de compétitivité. A cette fin, le droit doit être pensé avec l'IA et dans une perspective d'usage réel. La règle de droit doit donc être rendue lisible, harmonisée et activable, afin qu'elle protège, légitime et accélère l'innovation européenne dans l'ère de l'intelligence artificielle.

A. Les difficultés actuelles à appréhender le cadre juridique et les enjeux éthiques

1. Les difficultés juridiques sont nombreuses : enchevêtrement des textes, notamment supranationaux, définitions floues, incertitudes réglementaires

L'**encadrement juridique des solutions d'IA est complexe** car il dépend à la fois des fonctionnalités de l'outil, des types de données traitées et des finalités poursuivies par leur traitement. **Plusieurs textes nationaux et européens s'appliquent**, mais la plupart ne visent pas spécifiquement l'IA, ce qui complique leur interprétation face aux innovations technologiques.

Le règlement (UE) 2024/1689 du 13 juin 2024, qui instaure des **règles harmonisées en matière d'IA** (dit « règlement IA » ou « RIA »), constitue à ce jour le **socle du dispositif européen**. Ce texte, premier cadre juridique complet de portée internationale, vise à garantir une **utilisation de l'IA respectueuse des droits fondamentaux**, en particulier face aux risques de discrimination, d'atteinte à la vie privée ou de remise en cause des processus démocratiques. Sa mise en œuvre suppose la clarification de notions essentielles, telles que celle de **« système d'IA à haut risque »**, notamment dans le contexte de l'administration de la Justice. L'absence de définitions précises laisse subsister des zones d'incertitude quant aux obligations à respecter dans certains cas d'usage.

Par ailleurs, dès lors qu'une solution d'IA implique le **traitement de données à caractère personnel**, que ce soit pour son entraînement ou dans le cadre de son utilisation, le **règlement général sur la protection des données** (RGPD)[13], la directive « Police-Justice[14] », ainsi que la **loi « Informatique et libertés** (LIL) »[15] ont vocation à s'appliquer, selon les finalités poursuivies.

Enfin, il convient de prendre en compte les règles relatives à l'**hébergement souverain des données sensibles** (loi n° 2024-449 sur la sécurisation et la régulation de l'espace numérique, doctrine « cloud au centre »), ainsi qu'à la **communicabilité des documents administratifs** (loi n° 2016-1321 pour une République numérique). Ces exigences s'ajoutent au cadre général et doivent être intégrées dans l'analyse de conformité des solutions d'IA.

En résumé, la construction d'un cadre juridique adapté à l'IA requiert une veille constante, une analyse au cas par cas des usages et une **coordination étroite entre les différentes sources normatives**, afin de garantir la sécurité juridique et la conformité des projets innovants.

[12] In « AI is law, le droit bouclier et lance d'une IA européenne »
[13] Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[14] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données
[15] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

B. Les enjeux éthiques propres à la Justice

Il n'existe pas à proprement parler de « cadre éthique » parfaitement circonscrit de l'IA. La production des organisations intergouvernementales (OCDE, UNESCO, Conseil de l'Europe, Union européenne et, dans une moindre mesure, G7, G20, GPAI[16]) peut toutefois éclairer la réflexion. Le terme d'éthique[17], par ailleurs, ne peut être appliqué pour désigner une réglementation juridiquement contraignante (règlement européen et convention-cadre).

La **régulation des systèmes d'IA** s'est initialement construite autour d'une **démarche d'auto-régulation**, mobilisant l'ensemble des parties prenantes et **s'inscrivant dans une perspective dite « éthique »**.

Dans le secteur de la Justice, cette orientation a notamment pris forme avec l'adoption, en 2018, par la **Commission européenne pour l'efficacité de la Justice** (CEPEJ) du Conseil de l'Europe, d'une **charte éthique** encadrant l'usage de l'IA dans les systèmes judiciaires et leur environnement. Toutefois, la portée de cette approche s'est rapidement révélée limitée : son caractère essentiellement déclaratif et l'absence de dispositifs de sanction ou de contrôle effectif ont mis en lumière ses insuffisances face aux enjeux soulevés par le développement rapide de ces technologies.

Dès 2019, avec la création d'un **comité *ad hoc* sur l'IA** (CAHAI) au **Conseil de l'Europe** et en 2020, avec la publication par la **Commission européenne** d'un **livre blanc**, l'Europe a replacé le **droit contraignant** au cœur de la gouvernance de cette technologie. Ainsi, en 2024, ont été adoptés d'une part, le RIA au sein des 27 États de l'Union européenne, établissant un régime juridique de sécurité des produits avec un niveau de contrainte proportionné aux risques créés et d'autre part, une convention-cadre par les 46 États du Conseil de l'Europe et 11 États non-membres, incluant une **série de principes de haut niveau visant à protéger les droits fondamentaux, la démocratie et l'État de droit**.

La **coexistence de normes éthiques et de règles juridiques contraignantes** dans le domaine de l'IA n'est ni redondante ni accessoire : elle répond à des **besoins complémentaires et reste essentielle**, même dans un contexte de régulation renforcée.

Les règles juridiques, comme le RIA, imposent des **obligations précises et sanctionnables**, notamment pour les usages à risque élevé (recrutement, Justice, santé, etc.), afin de garantir la sécurité, la transparence, la robustesse et la protection des droits fondamentaux. Cependant, la seule existence d'un cadre légal ne suffit pas à anticiper l'ensemble des situations inédites ou à **répondre à des enjeux qui évoluent plus vite que la législation elle-même**.

Les normes éthiques jouent un rôle essentiel : elles **apportent des repères là où la loi est absente ou insuffisante**. Ces normes se traduisent généralement par des principes fondamentaux à respecter, tels que **la transparence, la non-discrimination, le respect de la vie privée, le contrôle humain, la sécurité et l'inclusion**. Elles inspirent et orientent l'élaboration des futures normes juridiques, comme cela a été le cas pour le RIA, qui s'appuie sur les **lignes directrices en matière d'éthique pour une IA digne de confiance**, élaborées par un groupe d'experts indépendants de haut niveau, il est essentiel de garder une réflexion éthique, car respecter la loi ne suffit pas toujours à garantir un usage juste de l'IA. Par exemple, certains outils d'IA comme l'algorithme COMPAS (Correctional offender management profiling for alternative sanctions) dans la justice américaine, instrument d'évaluation du risque de réitération de l'infraction, ont renforcé des **biais raciaux**, même en étant légaux.

[16] Global Partnership on Artificial Intelligence ou partenariat mondial pour l'IA, initiative internationale et multipartite visant à guider le développement et l'utilisation responsables de l'IA

[17] Éthique de l'intelligence artificielle | UNESCO -L'éthique en matière d'intelligence artificielle (IA) désigne l'ensemble des principes, valeurs et règles qui guident la conception, le développement et l'utilisation de l'IA afin qu'elle respecte la dignité humaine, les droits fondamentaux, la justice, la transparence et le bien commun. En résumé, il s'agit de s'assurer que l'IA soit utilisée de façon responsable, équitable et bénéfique pour la société, tout en minimisant les risques comme les discriminations, les atteintes à la vie privée ou la perte de contrôle humain.

De plus, beaucoup de systèmes d'IA sont **opaques** (« boîtes noires »), ce qui rend leurs décisions difficiles à comprendre et **peut nuire à l'équité et à la confiance**, même s'ils respectent la loi.

En résumé, les **normes éthiques sont indispensables** pour accompagner le développement de l'IA, prévenir les dérives et renforcer la confiance du public, au-delà du simple respect des règles juridiques. Elles forment une base commune pour une IA responsable et adaptée aux évolutions rapides du secteur.

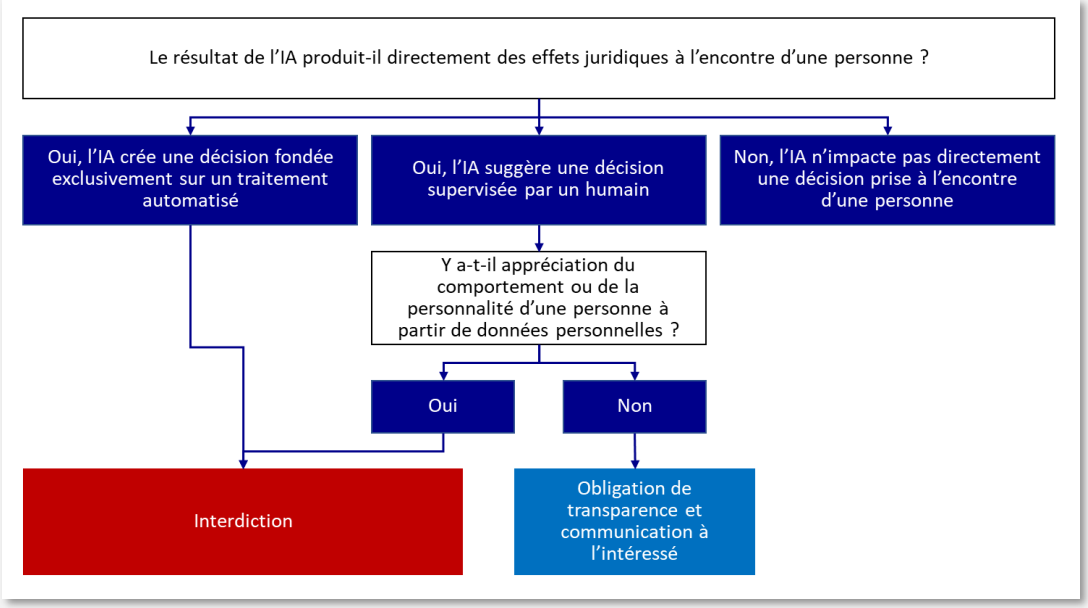
C. Les outils proposés facilitent l'appropriation du cadre juridique et des enjeux éthiques, tout en soulignant la nécessité de clarifier les règles applicables à l'IA

1. A court terme, la mission propose un outil dit « arbre décisionnel juridique » pour accompagner les porteurs de projets IA

Compte-tenu de la complexité du cadre juridique précédemment décrit, la mission a élaboré un **arbre décisionnel** permettant aux porteurs de projets d'**identifier les dispositions légales et réglementaires applicables** dans le cadre de la mise en œuvre d'un système d'IA (SIA). Il est constitué d'une suite de questions que devront se poser les porteurs de projets (ex. quelles données sont utilisées dans la phase d'utilisation et d'entraînement du SIA ? Quelle est la finalité du SIA ? Quel est le degré de proximité avec la décision judiciaire ? etc.) et dont la réponse permettra d'**affiner le cadre juridique applicable**. Cet arbre décisionnel est complété par une note plus globale présentant de manière exhaustive le cadre juridique applicable.

Encadré – Arbre décisionnel juridique

Exemple de question juridique soulevée par l'arbre décisionnel juridique à destination des concepteurs et utilisateurs de système d'IA en Justice



2. A moyen terme, le cadre juridique devra évoluer pour permettre la généralisation des solutions IA au service de la Justice dans le respect des droits fondamentaux

La **loi informatique et libertés** et les normes supranationales applicables en matière de **protection des données personnelles** imposent la **détermination préalable d'une ou de plusieurs finalités** précises à chaque traitement de données à caractère personnel. La majorité des SIA ayant vocation à traiter des données personnelles dans le cadre d'un usage par les magistrats et agents du ministère de la Justice, ce cadre leur est applicable. Or, beaucoup d'outils d'IA, dont les agents conversationnels, ont pour **objectif de répondre à de nombreux cas d'usage**, non déterminés à l'avance, ce qui rend complexe, si ce n'est impossible, la définition en amont des finalités précises de ces traitements.

En outre, l'**absence de cadre légal au niveau national permettant d'expérimenter l'usage d'un SIA**, de constater les usages métier qui en sont faits et de déterminer sur cette base l'encadrement informatique et libertés nécessaire est un véritable frein au développement de tels outils. Or, l'article 57 du RIA prévoit expressément la mise en place de « **bacs à sable réglementaires en matière d'IA** » afin d'encourager l'innovation et faciliter le développement, la formation, l'essai et la validation de SIA innovants pendant une période limitée avant leur mise en service. Ces bacs à sable peuvent inclure des essais dans des conditions réelles supervisées. Il serait pertinent d'**adapter notre droit national à ces exigences** afin de permettre la mise en œuvre d'expérimentations en matière d'IA, incluant le traitement de données à caractère personnel, de manière encadrée mais sans avoir à respecter au préalable les exigences de la loi informatique et libertés.

Une **évolution de la loi informatique et libertés**, afin de l'adapter au développement et au fonctionnement des SIA apparaît donc nécessaire à la mission. Ces aménagements du cadre juridique national de la protection des données personnelles mériteraient d'être entrepris rapidement.

Par ailleurs, les travaux engagés par les autorités de protection des données et les instances européennes compétentes en matière d'IA[18]afin de développer une **doctrine d'interprétation des textes** permettant le développement de systèmes d'IA à droit constant pour aboutir à des **lignes directrices** dans les mois à venir pourraient être l'occasion de porter le sujet de l'**articulation entre la réglementation européenne relative à la protection des données personnelles et les SIA**, et d'obtenir des interprétations concrètes, pratiques et constructives.

S'agissant plus spécifiquement des SIA développés **en appui des fonctions pénales**, une réflexion pourrait être amorcée d'une part sur d'éventuelles adaptations de la **directive « police-Justice »** que rendrait nécessaire la généralisation de solutions d'IA en matière pénale et d'autre part sur l'éventuelle « surtransposition » dont a pu faire l'objet cette directive dans notre droit national. À ce titre, le niveau de norme requis pour la mise en œuvre d'un traitement de données par l'État n'est pas un frein en soi. Cependant, son **inadéquation avec les technologies et les besoins actuels** montre qu'il est nécessaire de le faire évoluer afin d'assurer un encadrement plus adapté et efficace. Il conviendrait donc de repenser ce cadre réglementaire.

Enfin, s'agissant de la conception de **SIA nécessitant un entraînement sur la base de données spécifiques** à l'activité concernée, par exemple des dossiers civils ou des dossiers de procédures pénales, se pose la question de **l'application des règles de confidentialité des procédures**, propres à chaque domaine. Que ce soit en matière civile ou en matière pénale, aucun texte ne permet d'alimenter un SIA sur la base de toutes les procédures qui seraient agrégées pour affiner ou entraîner un modèle. Pour ce faire, la création de règles spécifiques serait à envisager.

[18] Travaux du comité IA européen et comité européen de la protection des données pour interprétation à la fois du RIA + RGPD et directive police Justice (Law Enforcement Directive)

Proposition : Mettre à la disposition des magistrats et agents l'outil d'aide à la conformité développé par la mission, incluant notamment un arbre décisionnel juridique, afin de faciliter la compréhension du cadre juridique applicable aux projets IA.

Proposition : Engager des travaux visant à faire évoluer le cadre réglementaire national, en veillant à leur cohérence avec les principales normes européennes (règlement européen sur l'IA, Directive Police-Justice, RGPD).

3. Des « principes directeurs d'utilisation de l'IA » et une labellisation « IA digne de confiance en Justice »

Il est important de clarifier d'une part, les **obligations pesant sur les concepteurs et les usagers**[19] de systèmes d'IA employés dans le cadre des missions du service public de la Justice et d'autre part, de proposer une **méthode d'évaluation de la performance des systèmes**, objectivant leur valeur ajoutée.

S'agissant des obligations pesant sur les concepteurs, il sera distingué les obligations résultant de cadres juridiques impératifs (RIA, RGPD notamment) des obligations supplémentaires que le ministère voudra établir (tant à destination du secteur public que du secteur privé) pour renforcer le cadre de confiance. La mission propose ainsi d'établir **des principes directeurs**[20], inspirés notamment de la Charte éthique de la CEPEJ, qui pourront notamment concerner des mesures particulières prises par les concepteurs pour s'assurer de la qualité des données d'entraînement, de la mesure des biais ou encore de la pertinence de la documentation établie. Le respect de ces principes directeurs, vérifié par des organismes tiers et sous l'autorité de l'Observatoire de l'IA du ministère, permettra d'attribuer une label d'« *IA digne de confiance en Justice* » (IADCJ) (cf.infra).

Encadré – Le label « IA digne de confiance en Justice (IADCJ) »

La mission propose de créer un label « IA digne de confiance en Justice » (IADCJ), qui n'a pas vocation à se substituer aux certifications obligatoires sur le fondement du RIA pour les systèmes « à haut risque », mais intéressera les applications n'étant pas qualifiées à « haut risque » et pour lesquelles l'autorité publique ou les opérateurs privés considéreront comme une valeur ajoutée l'attribution d'un tel label.

Ce label, non obligatoire, pourra s'appuyer sur des principes directeurs établis à l'attention de ceux qui fournissent et déploient des systèmes d'IA (cf.supra) et attester que ceux-ci ont respecté, tant durant la phase de conception que tout au long du cycle de vie, un certain nombre de mesures éthiques et techniques à même de prévenir les principaux risques et dérives (sécurité des données, discriminations illégitimes, biais algorithmiques et cognitifs, atteintes à l'intégrité du système par des attaques cyber, etc.).

[19] Concepteurs de systèmes d'IA : acteurs internes (direction du numériques du ministère de la Justice) ou externes (prestataires, legaltechs) responsables de la conception, du développement et de la mise en œuvre des solutions d'IA.
Usagers : magistrats, personnels administratifs, auxiliaires de Justice et justiciables qui utilisent ou bénéficient des outils d'IA dans le cadre des activités judiciaires.

[20] Principes qui imposent le respect des droits fondamentaux, la non-discrimination, la qualité et la sécurité des systèmes, la transparence, ainsi que la maîtrise et le contrôle par l'utilisateur

S'agissant des obligations pesant sur les utilisateurs, le **projet de charte établi par le Service de l'expertise et de la modernisation (SEM)** du ministère de la Justice devra être diffusé pour accompagner la mise en service d'une IA générative « Justice » et **prohiber l'utilisation de systèmes tiers avec des données d'une sensibilité particulière issues de l'activité judiciaire** tout particulièrement. Cette charte établit des principes et conduites à tenir, cohérent avec les obligations déontologiques reposant sur les magistrats et agents. Elle promeut un **usage responsable, raisonné et fruga**l de l'IA, au vu des coûts environnementaux engendrés par son utilisation, et tout particulièrement de limiter son usage dans les situations où une alternative moins consommatrice existe tel qu'une recherche web classique. La **formation sur l'IA générative** déjà proposée sur la **plateforme MENTOR**[21], pourrait être, dans le même temps, rendue obligatoire pour les magistrats et agents ne l'ayant pas déjà suivie.

Proposition : Diffuser une charte d'usage des outils d'IA à destination des utilisateurs ainsi que des principes directeurs éthiques, à destination des concepteurs-développeurs des outils d'IA, et créer un label « IA digne de confiance » afin d'encadrer l'usage des solutions proposées par des éditeurs juridiques et « legaltech ».

D. La qualité et l'accessibilité des données : un préalable essentiel à toute démarche d'intelligence artificielle

La majorité des cas d'usage de l'intelligence artificielle repose sur l'**exploitation de données judiciaires** déjà **intégrées aux logiciels métiers** ou issues des documents produits par le ministère. L'accès à ces données, qu'elles soient structurées ou non, constitue un **prérequis incontournable** pour le développement de SIA capables de répondre aux besoins spécifiques des métiers judiciaires.

Le ministère produit en continu un **volume important de données originales, fiables et pertinentes**, essentielles à la conduite de ses missions. La circulation et la valorisation de ces données, dans le respect des exigences de confidentialité et de sécurité, sont déterminantes pour **garantir la qualité** et la pertinence des solutions d'IA déployées.

Afin d'assurer une exploitation optimale de ces ressources informationnelles, il convient d'organiser, en amont de tout projet d'intelligence artificielle, les actions suivantes :

- **Ouverture et accessibilité des données** : Veiller à ce que les données nécessaires soient aisément accessibles, dans un cadre sécurisé, pour les équipes en charge du développement et de l'intégration des solutions d'IA.
- **Mise en qualité et structuration des données** : Intégrer dès la collecte ou la création des données, au sein des applicatifs métiers, des processus de structuration et d'assurance qualité. Selon les cas d'usage, les données devront ensuite être nettoyées, annotées ou labellisées. Ce travail sémantique, à forte dimension juridique, est indispensable pour prévenir les risques d'erreurs ou d'« hallucination » lors de l'utilisation des SIA.

En définitive, la valorisation et la gestion rigoureuse des données produites par le ministère constituent le socle sur lequel reposent la fiabilité, l'efficacité et l'adaptation des solutions d'intelligence artificielle au service de la Justice.

[21] Découvrir les IA génératives | Mentor - formation d'1 heure approximativement

3. DÈS 2025, DOTER LES MAGISTRATS ET AGENTS D'UN ASSISTANT IA GENERALISTE, PUIS DÉPLOYER PROGRESSIVEMENT DES FONCTIONNALITÉS MÉTIERS SPÉCIFIQUES

A. Développer, dès 2025, une solution transverse sous la forme d'un assistant IA pour couvrir de larges usages de façon sécurisée (analyse, synthèse, extraction d'information)

1. Lancement en 2025 d'une plateforme IA évolutive, avec de nouveaux services dès le premier semestre 2026

Les deux tiers des cas d'usage recensés par la mission relèvent de besoins de technologies transverses (LLM et retranscription) :

- **50%** reposent sur une base technologique de **grand modèle de langage** (LLM)[22], telles que l'analyse, la synthèse, l'extraction d'information.

- **13%** sont fondés sur une base technologique de **retranscription** (speech-to-text)[23], exprimant des attentes fortes de l'ensemble des directions et métiers du ministère.

La mission préconise ainsi le développement d'un assistant IA souverain, capable de traiter ces besoins de façon progressive à travers des fonctions mutualisées de langage (analyse, recherche documentaire, rédaction assistée, synthèse, etc.) et un outil de retranscription.

Un premier outil prêt à l'usage (encore appelé « produit minimum viable » ou PMV[24]), dont la mise en service pourrait intervenir d'ici la fin d'année 2025, permettra de répondre à plusieurs besoins identifiés, à travers l'exploitation de grands modèles de langage (LLM) en source ouverte (open-source)[25]. Une dizaine de cas d'usage communs à plusieurs métiers (administratif, civil, pénal, AP, PJJ) pourront être en partie couverts dès la mise en production de la première version minimale de cet assistant IA. L'assistant IA offrira notamment des capacités de :

- **Transformation de contenu textuel** : mise en forme automatique des textes, reformulation pour améliorer la clarté ou l'accessibilité, traduction multilingue, et correction orthographique et grammaticale.

- **D'aide à la rédaction** : génération de modèles de documents (courriers, rapports, notes), suggestion d'idées ou de formulations, adaptation des textes à différents contextes ou publics, et personnalisation selon les besoins de l'utilisateur.

[22] *Large Language Model* (LLM) ou grand modèle de langage est un modèle de langage possédant un grand nombre de paramètres (généralement de l'ordre d'un milliard ou plus) constitués de réseaux de neurones profonds entraînés sur de grandes quantités de texte non étiqueté. Ces modèles sont apparus dès 2018 sous la forme d'agents conversationnels. Ils sont entraînés à prédire une suite probable de mots à partir d'une entrée donnée (*prompt*), permettant d'effectuer diverses tâches liées au traitement du langage naturel, telles que de la rédaction, de la synthèse, des réponses à des questions etc.

[23] La technologie *speech to text*, également connue sous le nom de reconnaissance automatique de la parole ou retranscription, est un processus qui permet de convertir la parole humaine captée au moyen d'un microphone en texte écrit. Cette technologie utilise des algorithmes de traitement du signal et d'apprentissage automatique pour analyser les sons de la voix, les décomposer en éléments linguistiques, et les transcrire en mots écrits.

[24] Un *minimum viable product* (MVP) ou produit minimum viable, est une version simplifiée d'un produit numérique avec les fonctionnalités essentielles pour satisfaire les premiers utilisateurs. Il permet de tester une idée de produit avec un investissement minimal. L'objectif est de recueillir des retours pour guider les développements futurs en délivrant de la valeur aux utilisateurs en continu tout en s'adaptant à leurs besoins. Il s'agit d'un concept lié au mode produit ou *product management*.

[25] Un modèle *open-source* ou en source ouverte, est un modèle publié dans le cadre d'une licence libre et ouverte, dont le code source est librement accessible, distribuable et modifiable par tous.

- **D'une première version d'analyse documentaire** : lecture automatisée de documents, extraction rapide des informations clés, synthèse de contenus, comparaison de plusieurs documents pour repérer similitudes et différences, et création de résumés ou de tableaux comparatifs.

Des versions ultérieures, qui pourraient intervenir dès 2026, **viendront élargir le périmètre fonctionnel de l'assistant pour couvrir davantage de cas d'usage et de manière plus performante**. Tout d'abord, l'amélioration continue permettra d'**affiner la précision et la pertinence** des réponses en spécifiant le grand modèle de langage au contexte du ministère. Par ailleurs, l'assistant sera ainsi progressivement renforcé dans sa capacité à **traiter des volumes documentaires complexes et variés**, assurer la **retranscription** de réunions ou échanges simples, **transformer en plein texte des documents** images ou scannés.

En revanche, pour les cas d'usage requérant une solution spécifique ou une adaptation de l'assistant IA, une priorisation des efforts a été nécessaire. À ce titre, 12 cas d'usage ont été priorisés au sein d'un portefeuille évolutif ; ils feront l'objet de développements adaptés, qu'il s'agisse d'une personnalisation du grand modèle de langage ou d'une solution technique autonome (**voir section IIIB**).

Encadré – Typologie des cas d'usage recensés et correspondance technologique

Les cas d'usage recensés dans le cadre de la mission peuvent correspondre à des technologies d'IA distinctes. Cette caractérisation permet de repérer les similitudes et synergies possibles entre les différents cas d'usage et d'envisager des solutions technologiques communes. Ainsi, la création de composants technologiques mutualisables peut optimiser l'impact d'un développement de manière transversale.

Fonctionnalité	Description	Technologie principale	Proportion parmi les cas d'usage identifiés
Génération de contenu	Production assistée de contenus textuels, incluant notamment la synthèse documentaire, la rédaction structurée, la production de code informatique et la traduction écrite	LLM	27%
Retranscription	Traitement d'échanges oraux en documents textuels exploitables	Speech-to-text	13%
Interprétariat	Traduction orale en temps réel	LLM, Speech-to-text	5%
Recherche	Exploration contextuelle de vastes corpus documentaires et extraction d'informations pertinentes	LLM, IA analytique, NLP[26]	20%
Analyse de données	Identification des corrélations, prévision des tendances et appui à la prise de décision	IA analytique, Data science, ML[27]	23%
Analyse d'images	Traitement et interprétation d'images et de flux vidéo	Computer vision[28]	3%
Automatisation de tâches	Systèmes d'automatisation des processus métiers répétitifs ou standardisés	IA analytique, Data science, RPA[29]	9%

[26] Le *Natural Language Processing* (NLP) ou traitement automatique du langage naturel (TAL), est un domaine multidisciplinaire impliquant la linguistique, l'informatique et l'intelligence artificielle. Il vise à créer des outils de capable d'interpréter et de synthétiser du texte pour diverses applications.

[27] Le *Machine Learning* (ML) ou apprentissage automatique, est une branche de l'intelligence artificielle qui utilise des méthodes mathématiques et statistiques pour permettre à un modèle d'apprendre à partir de données. Il vise à améliorer les performances des systèmes sur des tâches spécifiques sans programmation explicite pour chacune. Les modèles d'apprentissage automatique s'ajustent et optimisent leurs résultats en fonction des données d'entrée.

[28] La *computer vision* ou vision par ordinateur est un domaine de l'intelligence artificielle qui vise à permettre aux machines de comprendre et d'interpréter le monde visuel. Elle utilise des algorithmes et des modèles pour analyser et traiter des images et des vidéos, afin d'extraire des informations significatives.

[29] Le *Robotic Process Automation* (RPA) ou automatisation robotisée des processus, est une technologie qui s'appuie sur des "logiciels robots" qui permettent d'automatiser des tâches bien précises effectuées sans réflexion ou avec des logiques très simples.

3. De nombreux bénéfices sont attendus de la mise à disposition d'un assistant IA, comme l'illustrent les retours d'expérience des autres ministères en matière d'IA

La mission recommande au ministère de la Justice, à l'instar du ministère des Armées ou de l'Intérieur, de développer une plateforme d'IA générative, souveraine et sécurisée. Cette priorisation se fonde sur les objectifs suivants :

- **S'aligner avec la stratégie du gouvernement** visant à mettre à disposition des outils d'IA générative à l'ensemble des magistrats et agents d'ici la fin de l'année 2025. Déployer une solution unique d'IA à grande échelle, plutôt qu'une multitude d'outils spécialisés afin de permettre à tous les professionnels de la justice d'accéder rapidement à des outils d'IA, favorisant l'harmonisation des pratiques, la mutualisation des ressources et un gain de temps sur l'ensemble des tâches courantes.

- **Éviter le phénomène d'utilisation cachée de l'IA (shadow AI)** et de fuite de données d'une sensibilité particulière en proposant une alternative sécurisée. Aucun agent conversationnel grand public n'est aujourd'hui souverain et sécurisé au sens de la doctrine « Cloud au centre »[30] et de la loi SREN[31], y compris Le Chat de Mistral. Les données sont hébergées sur des serveurs d'entreprises de nationalité américaine soumises au Cloud Act[32], Foreign Intelligence Surveillance Act (FISA)[33] et un ensemble de décrets permettant aux instances de Justice ou de renseignement américains de contraindre ces fournisseurs de services à fournir les données stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers même en France. L'hébergement ou le traitement de données judiciaires par un système d'IA ouvre ainsi un risque d'ingérence.

- Développer **une plateforme dont les fonctionnalités pourront être intégrées dans les applications métiers via des API** ce qui permettra aux magistrats et agents de bénéficier d'outils d'analyse, de recherche et de synthèse directement intégrés à leurs logiciels habituels, facilitant ainsi la préparation des dossiers, la prise de décision et l'accès à l'information juridique.

Encadré – La stratégie IA du ministère de l'Intérieur

Confronté à des enjeux similaires à ceux du ministère des Armées, le ministère de l'Intérieur a développé son propre **portail d'outils d'IA généraliste**, fondé sur des solutions open source. Aujourd'hui opérationnel, ce portail met à disposition des agents quatre outils conçus pour répondre à des besoins concrets du quotidien :

- Un agent conversationnel
- Un outil de synthèse de texte
- Un outil d'extraction de texte d'un document (océrisation)
- Un outil de transcription de réunions en visioconférence

Source :Mission - Entretien avec la délégation ministérielle à l'IA du ministère de l'Intérieur

[30] Circulaire n° 6404/SG du 31 mai 2023, actualisant la doctrine et précisant les règles d'hébergement des services numériques de l'État
[31] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (dite « loi SREN »)
[32] Clarifying Lawful Overseas Use of Data Act ou Cloud Act (H.R. 4943), loi fédérale américaine adoptée en 2018
[33] Foreign Intelligence Surveillance Act (FISA), loi fédérale américaine adoptée en 1978, codifiée principalement au titre 50 du Code des États-Unis (§ 1801 et suivants)

Encadré – Le ministère des Armées et la plateforme GenIAI

Dans le cadre de ses travaux sur l'IA, **le ministère des Armées avait initialement adopté une approche fondée sur les cas d'usage**, en recensant plus de 200 besoins exprimés par les agents. Si cet inventaire offrait un premier panorama des attentes, il ne permettait ni de hiérarchiser les priorités, ni de concentrer les ressources sur les cas à fort impact. Par ailleurs, le ministère observait une utilisation croissante d'outils d'IA grand public, non sécurisés et non souverains, l'incitant à proposer rapidement une alternative interne et mieux maîtrisée.

Inspiré des pratiques de certains grands groupes privés, ayant opté pour une approche plus resserrée autour de grands piliers, le ministère a alors changé de stratégie. Une analyse des usages réels a été menée, permettant notamment de quantifier les requêtes adressées à des outils comme ChatGPT ou Mistral, et d'objectiver ainsi la pertinence de ce virage. Le ministère a dès lors adopté une **approche « produit »**, **centrée sur le développement d'outils généralistes répondant à une forte demande**, et déclinables selon des cas d'usage spécifiques.

C'est dans cette logique qu'est née la **plateforme GenIAl,** dont un premier prototype a été développé en août 2023. Depuis, la plateforme s'est progressivement consolidée. Ouverte à l'ensemble des agents, GenIAl propose aujourd'hui **plusieurs briques technologiques :**

- Agent conversationnel pour l'assistance à la rédaction et aux questions générales
- Outil de synthèse de documents
- Système de traduction de textes et de messages
- Transcription automatique d'enregistrements audios
- Océrisation (conversion de texte contenu dans des images)
- Génération d'images

Plébiscitée par les agents, la plateforme compte désormais **35 000 utilisateurs**. Son adoption s'explique notamment par les **gains d'efficacité et de productivité** qu'elle permet. Ces bénéfices ont été confirmés par un sondage réalisé auprès d'un panel représentatif d'agents, qui estime les **gains de temps entre 50% et 70%** selon les usages.

Source : Mission - Entretien avec le centre d'expertise données & IA (SGA/DTPM/MAP)

Proposition : Déployer, dès 2025, un assistant IA sécurisé et souverain dédié à l'ensemble des magistrats et agents du ministère de la Justice, intégrant progressivement des fonctions de recherche, de synthèse, de rédaction et de retranscription.

B. Des cas d'usage plus spécifiques aux métiers de la Justice ont été considérés comme prioritaires par la mission et pourront être développés progressivement au cours des trois prochaines années

1. Présentation des 12 cas d'usage « métiers » prioritaires

Dans le cadre de la mission, en complément des cas d'usage déjà couverts par le socle initial de l'assistant IA, **12 cas d'usage « métiers » ont été identifiés et considérés comme prioritaires** en fonction de leur impact potentiel, de leur faisabilité technique ainsi que de leur alignement avec les priorités stratégiques du ministère, couvrant les périmètres judiciaire (civil, pénal et accueil du justiciable en juridiction), pénitentiaire et de la protection judiciaire de la jeunesse. Une autre préoccupation de la mission a été d'assurer une représentativité de l'ensemble des directions dans les cas d'usage priorisés, afin de garantir l'engagement de l'ensemble du ministère dans cette stratégie.

Ces cas d'usage nécessitent, selon les situations, **soit des développements numériques spécifiques**, **soit un approfondissement des fonctionnalités de l'assistant IA**[34]**.**

Leur mise en œuvre sera graduelle, capitalisant sur les enseignements des outils IA déjà développés et dépendra étroitement du dimensionnement de l'équipe IA (voir partie V), qui conditionnera la capacité à les intégrer de manière plus ou moins rapide dans la feuille de route opérationnelle. A **chaque étape, un accompagnement réglementaire permettra de garantir la conformité des usages aux exigences de protection des données** et aux principes fondamentaux du droit. Cette articulation entre innovation technologique et sécurité juridique suppose une démarche pragmatique, fondée sur l'observation des pratiques effectives et l'ajustement progressif des cadres d'encadrement.

Encadré – Cas d'usage spécifiques prioritaires

Métier concerné	Cas d'usage prioritaires	LLM comme prérequis ?
Administration pénitentiaire	1 - Interprétariat instantané fonctionnant hors connexion	Oui
	2 - Vidéosurveillance intelligente dans les établissements pénitentiaires	Non
	3 - Détection vidéo intelligente pour la lutte anti-drones	Non
Protection judiciaire de la jeunesse	4 - Agent conversationnel juridique pour agents PJJ	Oui
Juridictions civiles	5 - Analyse et recherche documentaire avancée	Oui
	6 - Aide à la rédaction et synthèse contextualisée	Oui
	7 - Orientation des procédures ou courriers au sein des juridictions	Oui
Juridictions pénales	8 - Analyse et recherche documentaire avancée	Oui
	9 - Aide à la rédaction et synthèse contextualisée	Oui
	10 - Orientation des procédures ou courriers au sein des juridictions	Oui
Juridictions civiles et pénales	11 - Retranscription judiciaire des audiences et auditions	Non
Accueil du justiciable	12 – Solution d'orientation du justiciable pour les agents SAUJ	Oui

[34] Accroissement de la puissance de traitement des documents, interfaçage (APIsation) avec des applicatifs métiers, personnalisation et spécialisation d'un modèle existant (fine-tuning), RAG, etc.

2. Administration pénitentiaire : 3 cas d'usage pour sécuriser les établissements pénitentiaires et faciliter les relations avec les personnes détenues

Cas n°1 - Interprétariat instantané fonctionnant hors connexion :

La **barrière linguistique** des **détenus étrangers** (un quart de la population pénitentiaire) pose de nombreux défis aux agents pénitentiaires dans la **communication quotidienne** et la prise en charge de ces derniers. Les établissements pénitentiaires sont contraints de recourir à des **solutions non sécurisées et non encadrées** (traducteurs en ligne, intermédiation d'autres détenus) ou aux services d'interprètes professionnels ou à des associations spécialisées, ce qui représente un coût élevé pour l'administration. Pour les détenus, cette barrière linguistique **complique l'accès à leurs droits**, **nuit à leur prise en charge et fragilise leur santé psychologique**. Un outil **d'interprétariat instantané hors connexion** faciliterait la communication entre personnes détenues et agents, permettrait de réaliser des économies sur les services d'interprétariat, renforcerait la sécurité des agents et améliorerait la prise en charge des personnes détenues.

Cas n°2 - Vidéosurveillance intelligente dans les établissements pénitentiaires :

La **vidéosurveillance** dans les établissements pénitentiaires est rendue complexe par **le grand nombre de zones à surveiller**, ce qui nuit à la **détection systématique et rapide des situations à risqu**e (regroupements anormaux de personnes, présence prolongée d'un individu ou d'un objet dans une zone sensible, etc.). Un outil de vidéosurveillance intelligente, capable d'analyser les flux en continu et de générer des alertes en cas de comportement suspect, permettrait aux agents de se concentrer sur les zones critiques, de lever le doute et de **réagir rapidement**. Cette solution renforcerait la **sécurité des personnes détenues comme des agents**, améliorerait les conditions de travail des agents en réduisant leur charge de surveillance et permettrait de réduire le nombre d'incidents.

Cas n°3 - Détection vidéo intelligente pour la lutte anti-drones :

Les **survols de drones** au-dessus des établissements pénitentiaires se multiplient ces dernières années, et les moyens de les détecter et de les neutraliser se compliquent avec **l'apparition de nouvelles technologies, comme le pilotage via le 4G**. Un système de vidéo intelligente dédiée à la lutte anti-drones et fonctionnant avec l'intelligence artificielle permettrait de compléter les systèmes anti-drone de la DAP (radiofréquence et brouillage), et participerait à la réponse à une problématique commune à l'ensemble des établissements pénitentiaires : la l**utte contre l'introduction de produits** tels que drogues, cigarettes ou téléphones portables. Le suivi amélioré des vols de drones permet ainsi de **démanteler les filières d'approvisionnement** ou de **prévenir l'entrée d'objets encore plus dangereux**, comme des explosifs ou des armes.

3. Protection judiciaire de la jeunesse : 1 cas d'usage priorisé pour sécuriser la prise en charge des mineurs

Cas n°4 - Agent conversationnel juridique pour magistrats et agents PJJ :

Les professionnels de la PJJ doivent maîtriser un **nombre croissant de normes juridiques**, mais l'accès à ces informations est souvent difficile, ce qui complique leur application et consomme du temps agent. Un agent conversationnel juridique basé sur une IA, **capable de répondre aux questions des professionnels**, faciliterait l'**accessibilité et l'intelligibilité de la norme**, sécuriserait la prise en charge des mineurs et ferait gagner du temps aux professionnels.

4. Juridictions : 7 cas d'usage priorisés pour fluidifier l'activité juridictionnelle présentant de fortes similitudes entre le domaine pénal et civil

Si les domaines civil et pénal présentent des spécificités liées à la matière traitée, à l'environnement numérique de travail et aux gestes métiers attendus, il existe de **fortes synergies sur des cas d'usage** visant à **analyser et produire des documents textuels**. Les solutions envisagées devront être distinctes pour s'adapter aux spécificités métiers et s'insérer en harmonie avec des **applicatifs métiers propres** (Cassiopée, NPP ou SPS, Epopée, Portalis). Néanmoins le développement d'une solution pour un des cas d'usages permettra des apprentissages bénéfiques pour les suivantes.

Analyse et recherche documentaire avancée :

Cas n°5 - L'analyse et la recherche documentaire au civil

Les magistrats civilistes doivent traiter un **grand nombre de dossiers de nature diverse** (en particulier les contentieux de masse ou sériels), **nécessitant l'extraction manuelle d'informations clés**, par exemple, le premier impayé en matière de crédit à la consommation, les informations clés d'un bail d'habitation, les revenus des parties aux affaires familiales. Ce travail chronophage et propice aux erreurs **rallonge les délais de traitement des affaires.** Un **outil d'extraction de données**, capable d'identifier automatiquement les informations pertinentes et de **pré-remplir les trames de décisions**, permettrait de gagner du temps, de limiter les erreurs et d'homogénéiser le **traitement des affaires répétitives**.

Cas n°8 - L'analyse et la recherche documentaire au pénal

Les **dossiers pénaux** sont **de plus en plus volumineux et complexes** compte tenu notamment de l'accroissement des exigences formelles et de la nécessité de recourir de plus en plus fréquemment à des investigations techniques et scientifiques, ce qui augmente en conséquence le temps devant être consacré à l'étude des dossiers par les magistrats et ceux qui l'assistent. Un outil capable d'effectuer des **recherches rapides, précises et contextuelles** au sein des dossiers (dépassant significativement ce que permet la recherche « en plein texte ») contribuerait à faciliter et **accélérer le traitement des procédures** à tous les stades (enquête, instruction, audience…)., Enfin, à l'heure de la procédure pénale numérique, ces fonctionnalités pourront permettre l'ordonnancement automatique des pièces de procédure et la génération d'alertes procédurales.

Aide à la rédaction et synthèse contextualisée :

Cas n°6 – L'aide à la rédaction et synthèse au civil

Les magistrats consacrent un temps important à des tâches répétitives sans plus-value intellectuelle liées à la **rédaction des jugements simples et répétitifs** et au travail de préparation des éléments constants des dossiers complexes. Cela **allonge les délais de traitement**, notamment dans les affaires complexes. Un outil permettant de **synthétiser automatiquement les conclusions**, de **préparer l'exposé du litige** avec, après extraction, les faits constants et pertinents, la procédure, les prétentions et moyens, de suggérer des blocs de motivation issus de la jurisprudence, et de **détecter les contentieux sériels**, contribuerait à la réduction des délais de traitement.

Cas n°9 – L'aide à la rédaction et synthèse au pénal

La majeure partie de l'activité des magistrats pénalistes, et de ceux qui les assistent, consiste à **prendre connaissance des procédures pénales**, afin d'orienter, poursuivre, instruire, renvoyer ou juger. Ce travail fondamental de **lecture, d'analyse et de synthèse** d'un même dossier mobilise fortement ces personnels, qui doivent prendre des notes, élaborer des résumés thématiques ou chronologiques et identifier les éléments structurants d'une procédure pour fonder leurs décisions. Un outil automatisé faisant appel à

l'IA est en mesure de **générer instantanément une synthèse sur-mesure du dossier**, ajustée au niveau de détail requis, et de **mettre en lumière les concordances ou contradictions** entre constatations, auditions et interrogatoires. En conséquence, il accélérerait la **prise de connaissance des dossiers** et le traitement des procédures.

Orientation des procédures au sein des juridictions :

Cas n°7 – Orientation des procédures au civil

Les juridictions font face à un volume important de **dossiers hétérogènes nécessitant une orientation majoritairement manuelle** vers les chambres compétentes, ce qui est chronophage et source d'erreurs. Ce travail est particulièrement lourd dans les tribunaux judiciaires et cours d'appel de grande taille, et **peut entraîner des retards ou des erreurs dans l'affectation** des dossiers. Un outil capable de repérer automatiquement les critères d'orientation des dossiers et de proposer une orientation vers la chambre compétente, à soumettre à la validation du magistrat ou de l'agent de greffe, permettrait de **gagner du temps de magistrat et de greffe**, de réduire les erreurs, d'**améliorer la cohérence dans le traitement** des dossiers, de **diminuer les délais d'audiencement** et de rendu de la décision.

Cas n° 10 - Orientation des procédures au pénal

Les juridictions sont **destinataires de nombreux courriers, courriels ou procédures émanant des forces de sécurité intérieure, de justiciables ou d'autres administration**s, qu'il convient d'orienter, au sein des juridictions en fonction de l'état procédural d'une procédur**e** (parquet, instruction, siège correctionnel, application des peines, juge des enfants) et, le cas échéant, du type de contentieux ou de la minorité de l'auteur. L'orientation et l'affectation des procédures en fonction de **critères de répartition des affaires** par l'intelligence artificielle est donc de nature **raccourcir les délais de traitement**.

Cas n°11 - Retranscription judiciaire des audiences et auditions

Le pénal et le civil font face à des **défis similaires** concernant la **retranscription des échanges judiciaires**. Dans les deux cas, on observe que la nécessité de **prendre des notes simultanément à l'échange crée un cercle vicieux où la qualité de l'interaction diminue**, la fiabilité des informations retranscrites s'amoindrit, et le temps consacré à cette tâche détourne les professionnels de leur **mission principale d'écoute et d'accompagnement des justiciables**.

Dans le **domaine civil**, certaines procédures exigent la réalisation de **procès-verbaux d'audition**, notamment devant le juge des enfants en assistance éducative, devant le juge des tutelles, ou au juge aux affaires familiales pour l'audition des mineurs. Parallèlement, lors des audiences, le greffe doit établir une **note d'audience pour chaque affaire**. En **procédure orale**, la note d'audience doit être **la plus complète possible et consigner les éléments essentiels** (notamment les prétentions des parties). L'existence d'une retranscription avec verbatim permettrait de **garantir une retranscription fidèle** de l'argumentation des parties et ainsi de prévenir tout contentieux ultérieur tiré d'un défaut de réponse de la juridiction à une argumentation, d'**aider à la rédaction et à la motivation de la décision à venir**.

Dans le **domaine pénal**, il s'agit tout comme en matière civile des procédures nécessitant la **tenue de procès-verbaux d'audition** destinés à alimenter un dossier pénal. L'exemple le plus significatif est celui de la **procédure d'instruction** où chaque **audition**, **interrogatoire** ou **confrontation** fait l'objet d'une retranscription en style direct de l'intégralité des propos tenus. Actuellement, cette retranscription, faite par le greffier d'instruction, est nécessairement un **facteur limitant la fluidité des actes d'instruction**. La possibilité d'une retranscription automatique des propos tenus et distinguant les locuteurs, **sous le contrôle d'un greffier**, serait un facteur de gain de temps dans la conduite des actes sans risque de perte en qualité, **le greffier étant ainsi réaffirmé dans son rôle de garant du respect de la procédure** et de la fidélité entre les propos tenus et les propos retranscrits.

Dans les mêmes conditions, les **audiences correctionnelles**, qui supposent la **tenue de notes d'audiences** par le greffier d'audience, pourraient bénéficier d'un tel outil de retranscription qui faciliterait le travail de ce dernier en lui permettant de **se concentrer sur le respect de la procédure et la vérification de la fidélité des propos** tenus à la retranscription faite par l'IA.

La **spécificité du vocabulaire juridique** et de ses acronymes, les **différents niveaux de formalisme** au sein d'un échange, la **diversité de participants** dans une salle vaste notamment lors d'une audience, ainsi que l'exigence d'une haute fidélité des propos transposés établissent la **nécessité de spécifier un outil de retranscription** qui devra être pensé en intégration avec l'environnement numérique existant pour en assurer la supervision humaine. Il conviendra également d'assurer l'équipement matériel adéquat assurant la prise de son (microphones, insonorisation, acoustique des salles).

5. DSJ : 1 cas d'usage priorisé pour améliorer l'accueil du justiciable en juridiction

Cas n°12 - Solution d'orientation du justiciable pour agents SAUJ :

Les **services d'accueil unique des justiciables** (SAUJ) ont une **mission d'information générale et particulière vis-à-vis du justiciable**, ainsi qu'une mission de réception d'actes. Ils jouent un rôle clé en matière d'orientation du justiciable et d'accès aux droits. Cependant, les agents SAUJ font face à des difficultés : **effectifs limités, rotation importante, manque de formation et accès restreint aux outils**. Ils doivent répondre à des **demandes justiciables nombreuses et variées**, pouvant porter sur l'ensemble des procédures judiciaires. Dans ce contexte, un outil d'IA s'appuyant sur les textes juridiques, les procédures internes et les bases de données locales pour **formuler des réponses adaptées, contextualisées et sécurisées permettrait d'assister les agents d'accueil** dans leur réponse aux questions des justiciables. Une telle solution allégerait la charge des agents, permettrait de **mieux orienter les usagers** dès le premier contact, et de **renforcer la qualité perçue du service public de la Justice**.

Proposition : Déployer, à compter de 2026, des outils dédiés pour accompagner les 12 cas d'usage métiers jugés prioritaires par la mission, en raison de leur impact, de leur faisabilité et de leur alignement avec les orientations stratégiques du ministère.

4. Le plan d'approche technologique préconisé par la mission est progressif et réaliste, combinant le développement des capacités internes du ministère et un recours ciblé à certaines solutions de marché

A. Pour l'assistant IA et les usages critiques, un développement interne est recommandé afin de garantir l'autonomie technique et la sécurité des données sensibles

1. Le développement interne des solutions IA : un choix justifié par la spécificité des besoins, la souveraineté et la maîtrise des coûts

Les ministères interrogés dans le cadre des travaux de la mission IA Justice se sont engagés dans une **dynamique d'internalisation ou de ré-internalisation du développement des solutions d'intelligence artificielle**. L'arbitrage entre le développement des outils en interne ou le recours à des solutions du secteur privé dépend principalement de deux critères : la **spécificité des besoins métiers** et les **impératifs de souveraineté**. Cette démarche permet de mieux adapter les technologies aux exigences propres à chaque administration et de garantir la maîtrise des données et des outils stratégiques. Elle s'inscrit dans la stratégie nationale visant à faire de l'IA un levier d'innovation et d'efficacité pour l'action publique, tout en préservant l'indépendance technologique de l'État.

Après cette première analyse, la décision doit être affinée en tenant compte des éléments suivants :

- **Comparaison des coûts** : Évaluer le coût total d'un développement interne (salaires, infrastructure, formation, maintenance) par rapport à l'achat ou à l'abonnement à une solution du marché, en tenant compte des besoins de personnalisation, de la complexité du projet et de la durée d'exploitation envisagée.

- **Nombre d'utilisateurs concernés** : Prendre en compte la taille de la population cible (agents, magistrats, services) pour estimer la rentabilité et la pertinence de l'investissement. Un déploiement à grande échelle peut justifier un développement interne, alors qu'un usage limité privilégiera une solution existante plus économique.

- **Capacité technique et scientifique** : Analyser les compétences internes disponibles (data scientists, ingénieurs IA, chefs de projet) et la capacité à maintenir et à faire évoluer la solution. Le recrutement d'experts et la formation des équipes représentent des investissements importants, mais sont essentiels pour garantir l'autonomie et la maîtrise sur le long terme.

- **Contraintes d'intégration** : Examiner la compatibilité de la solution avec l'environnement numérique du ministère, notamment l'intégration aux systèmes existants, la sécurité des données, la conformité réglementaire (RGPD, souveraineté) et la facilité de maintenance. Une solution interne peut être plus facilement adaptée à ces exigences spécifiques, tandis qu'une solution du marché nécessitera parfois des adaptations ou des compromis.

2. La mission recommande la mise en œuvre, dès l'année 2025, d'un assistant reposant sur un grand modèle de langage (LLM) en source libre, hébergé dans une infrastructure cloud certifiée SecNumCloud

Dans l'attente du développement d'une infrastructure interne capable d'héberger un grand modèle de langage (LLM)[35] à l'échelle du ministère, il est essentiel de proposer une solution accessible à l'ensemble des magistrats et agents, soit potentiellement 91 000 personnes, dans le respect des normes les plus strictes en matière de sécurité et de protection des données.

Le scénario recommandé par la mission IA Justice repose sur le déploiement d'un assistant fondé sur **un grand modèle langage (LLM) en source ouverte**, hébergé chez un prestataire cloud disposant de la certification SecNumCloud[36]. Le choix de la source ouverte correspond à la volonté de pouvoir **maîtriser et installer les modèles sur une infrastructure propre** au ministère sans dépendre d'un éditeur tout en s'adaptant aux évolutions rapides du secteur. Par ailleurs, l'autonomie sur le choix des modèles d'IA permet de **sélectionner les modèles les plus frugaux** au vu des performances exigées, et s'assurer de la prise en compte du coût environnemental dès la conception.

De plus, le recours à une solution cloud certifiée SecNumCloud permet de garantir une **localisation exclusive des données sur le territoire national**, tout en les **protégeant contre tout accès non autorisé** ou toute **législation extraterritoriale**. Ce dispositif offre par ailleurs une sécurisation complète de l'ensemble de la chaîne de traitement, depuis la soumission des requêtes jusqu'à l'exploitation des résultats, assurant ainsi un niveau de confiance optimal pour les utilisateurs.

Pour anticiper une adoption large et répondre à la diversité des cas d'usage identifiés sur le terrain, une **montée en charge progressive** est envisagée. La mission évalue, **sur la base des retours d'expériences d'autres ministères** et d'échanges avec des fournisseurs spécialisés, un **premier dimensionnement** (détaillé en annexes). Une **mise à niveau ciblée du réseau ministériel** est également prévue pour accompagner ce déploiement, destiné à renforcer les capacités de requêtage (interrogation de données) et d'accès aux données.

En synthèse, le scénario préconisé présente plusieurs atouts :

- un **haut niveau de protection** des données et de souveraineté ;
- une mise en œuvre **rapide** et progressive ;
- une grande **flexibilité** pour ajuster les ressources GPU selon la montée en charge ;
- la possibilité de **personnaliser** le modèle via des techniques avancées telles que le pre-prompting, le fine-tuning, ou encore, à plus long terme, l'entraînement sur des jeux de données spécifiques à la Justice.

[35] *Large Language Model* (LLM) ou grand modèle de langage est un modèle de langage possédant un grand nombre de paramètres (généralement de l'ordre d'un milliard ou plus) constitués de réseaux de neurones profonds entraînés sur de grandes quantités de texte non étiqueté. Ces modèles sont apparus dès 2018 sous la forme d'agents conversationnels. Ils sont entraînés à prédire une suite probable de mots à partir d'une entrée donnée (*prompt*), permettant d'effectuer diverses tâches liées au traitement du langage naturel, telles que de la rédaction, de la synthèse, des réponses à des questions etc.

[36] Élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence. Les exigences du référentiel garantissent la protection du service cloud vis-à-vis du droit extra-européen, grâce à la combinaison de mesures techniques (étanchéité des systèmes d'information), opérationnelles (seul le prestataire peut intervenir sur les ressources supportant le service), et juridiques (application exclusive du droit européen).

3. Perspective de réinternalisation de l'hébergement des solutions d'IA au sein des infrastructures matérielles à partir de 2026

À compter de 2026, la stratégie numérique du ministère de la Justice doit prévoir **une nouvelle étape avec la réinternalisation de l'hébergement des solutions d'intelligence artificielle au sein des infrastructures ministérielles**. Cette évolution vise à renforcer la maîtrise technologique, budgétaire et sécuritaire du projet à moyen terme. L'acquisition des équipements nécessaires et leur déploiement dans les centres de données du ministère permettraient d'héberger localement les modèles d'IA, en assurant des performances comparables, voire supérieures, à celles d'une solution externalisée.

Il est essentiel de disposer d'une infrastructure matérielle performante, composée de serveurs équipés de processeurs spécialisés GPU[37], qui permettent de traiter rapidement les calculs complexes nécessaires au fonctionnement des modèles d'IA. Les coûts d'investissement, bien que significatifs, seraient **amortis dès la première année d'exploitation**. Ce choix renforcerait par ailleurs la **souveraineté numérique** en limitant l'exposition des données à des environnements tiers, tout en ouvrant la possibilité de **mutualiser ces ressources avec d'autres administrations**. Il garantirait également une **disponibilité continue** des capacités de calcul, indépendamment des tensions d'approvisionnement sur le marché des GPU.

Pour permettre cette réinternalisation, trois chantiers techniques devront être engagés :

- la **mise à niveau du réseau** historique pour absorber le volume croissant de requêtes liées aux usages IA ;
- l'installation d'un **réseau haut débit** dédié aux communications entre unités de calcul ;
- l'**adaptation physique des espaces du centre de données** aux contraintes spécifiques du nouveau matériel, ainsi que le renforcement du réseau électrique pour garantir l'alimentation et le refroidissement des serveurs.

Une fois cette infrastructure opérationnelle développée, elle couvrira la majorité des besoins quotidiens du ministère. Toutefois, afin de répondre à d'éventuels pics d'activité ou à des besoins temporaires accrus, elle pourra être complétée, de manière ponctuelle et ciblée, par un service de cloud privé certifié SecNumCloud, permettant ainsi d'accéder à des GPU supplémentaires sans recourir à de nouveaux investissements. **Ce modèle hybride permettra d'optimiser l'usage de l'infrastructure tout en garantissant la continuité et la qualité du service, y compris en période de forte sollicitation.**

Proposition : En 2025, installer un environnement d'hébergement numérique souverain (SecNumCloud[38]) pour déployer au plus tôt les cas d'usage (dont l'assistant IA), suivi d'un transfert progressif vers les infrastructures internes du ministère de la Justice.

[37] *Graphics Processing Unit* (GPU) est un processeur graphique ou carte graphique plus communément, qui permet de faire des calculs massivement parallèles et utilisé dans les calculs pour l'IA, la science des données, et la simulation. Le dimensionnement des infrastructures GPU dépend du nombre de requêtes utilisateur simultanées et donc in fine de la fréquence d'usage et du nombre de cas à développer.

[38] Élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique. Les exigences du référentiel garantissent la protection du service cloud vis-à-vis du droit extra-européen, grâce à la combinaison de mesures techniques (étanchéité des systèmes d'information), opérationnelles (seul le prestataire peut intervenir sur les ressources supportant le service), et juridiques (application exclusive du droit européen.

C. En complément du développement interne recommandé pour les cas d'usage à forts enjeux de sécurité et souveraineté, un ensemble de solutions de marché peuvent être envisagées pour les usages les moins critiques

La mission a eu le plaisir de mobiliser un **panel de magistrats civilistes et pénalistes** pour **tester plusieurs solutions d'IA issues du secteur privé**, dans le but de mieux cerner les usages potentiels de l'IA en Justice et de valider les hypothèses dans lesquelles les acquisitions de licences étaient opportunes. Cette démarche collaborative a permis d'identifier des outils particulièrement adaptés au quotidien des magistrats, notamment pour la recherche juridique et l'analyse de documents.

Trois fonctionnalités ont été plus particulièrement évaluées : **l'extraction d'information, la synthèse textuelle et la recherche juridique**. La mission a pu compter sur l'engagement et l'enthousiasme des utilisateurs volontaires, tout comme sur l'accompagnement des éditeurs qui ont participé à ces expérimentations.

Les retours sont encourageants : plus de **60 % des testeurs déclarent qu'ils utiliseraient « *assez souvent* »** les outils évalués si ceux-ci étaient déployés au sein du ministère, dessinant des perspectives prometteuses pour l'intégration de l'IA dans les pratiques judiciaires.

Cependant, à ce jour, la plupart des solutions proposées par les entreprises de legaltech **ne démontrent pas pleinement leur conformité à nos exigences en matière de sécurité et de souveraineté des données**. Cette réserve s'explique principalement par deux facteurs : d'une part, l'**hébergement** ou le traitement des données et des modèles s'effectue fréquemment sur des **serveurs appartenant à des entreprises étrangères**, notamment américaines ; d'autre part, l'utilisation de **modèles propriétaires** ne permet pas toujours de garantir l'absence de réutilisation des données transférées à des fins de ré-entraînement.

En conséquence, aucune de ces solutions ne peut actuellement prétendre à la certification SecNumCloud, conformément aux exigences de l'ANSSI et aux obligations prévues par la loi SREN. Dans ce contexte, et par mesure de précaution, il est recommandé de privilégier l'utilisation de services de legaltech qui ne nécessitent pas le versement de données de procédure non anonymisées, comme, par exemple, l**a recherche juridique assistée par l'IA** ou de solutions qui autorisent un hébergement sur nos infrastructures et l'utilisation de modèles non propriétaires

I**l demeure toutefois essentiel de poursuivre les échanges avec les éditeurs de solutions, afin d'explorer avec eux toutes les pistes d'adaptation possibles à nos exigences**. Ces discussions permettront d'identifier des évolutions techniques ou contractuelles susceptibles de garantir la conformité aux exigences de sécurité et de souveraineté. Cette démarche est d'autant plus importante que les services proposés par ces éditeurs présentent souvent une réelle valeur ajoutée et répondent à des besoins spécifiques des métiers de la Justice. Engager un dialogue constructif avec eux et en compagnie de l'ensemble des professions judiciaires nous permettra ainsi, à terme, de bénéficier de solutions innovantes tout en assurant la protection optimale des données sensibles.

Le recours à des solutions du marché demeure ainsi pertinent, mais en l'état et à défaut de démonstration tangible de mesures mises en place pour sécuriser l'hébergement des données de procédure, **la mission préconise de le limiter à la recherche juridique**. D'une part, cet usage n'implique pas la transmission de pièces de procédure ou de données personnelles, d'autre part, seules les solutions privées permettent de tirer pleinement parti de la richesse de leurs fonds doctrinaux et jurisprudentiels.

Proposition : Faire l'acquisition dès 2025 de licences permettant l'usage de solutions de recherches juridiques augmentées par l'IA.

Enfin, pour un **certain nombre de cas d'usage propres à l'administration centrale**, il peut être particulièrement pertinent d'envisager le recours à des solutions du marché, notamment lorsque ces usages n'impliquent pas la manipulation de données particulièrement sensibles. Cela concerne, par exemple, des domaines tels que la **communication institutionnelle**, la **gestion des ressources humaines** ou encore la **gestion immobilière**. Dans ces secteurs, les outils proposés par le marché offrent souvent des fonctionnalités éprouvées, une facilité de déploiement et une adaptabilité aux besoins des métiers concernés, tout en présentant un niveau de risque maîtrisé en matière de sécurité des données. Il convient toutefois de s'assurer, au cas par cas, que les solutions retenues respectent les exigences minimales de conformité et de protection des informations. La mission propose dès lors que le ministère de la Justice audite les solutions de marché, sélectionne les plus pertinentes et en fasse l'acquisition.

5. Pour réussir la stratégie IA, le ministère de la Justice devra internaliser les compétences en matière d'IA, se doter d'une gouvernance adaptée, dégager les ressources nécessaires et répondre aux besoins d'accompagnement et de formation des magistrats et agents dans l'intégration de l'IA

A. Poser les bases d'une nouvelle gouvernance IA permettrait d'animer la stratégie IA du ministère de la Justice et d'impulser une culture de l'évaluation des projets soutenus

1. Les principes d'une bonne gouvernance IA ministérielle

La **Cour des comptes** s'est récemment exprimée, dans un rapport consacré au déploiement de l'IA dans les politiques publiques, sur les leviers à mobiliser pour instaurer une gouvernance ministérielle de l'IA efficace. Ce rapport[39] souligne l'importance d'une **vision d'ensemble et d'une coordination efficace** à l'échelle ministérielle, ce qui freine, à défaut, la diffusion d'outils et d'expériences réussies. Si les questions de confiance – telles que la **transparence**, la **compréhension** des décisions prises par l'IA ou la **gestion des biais** – ainsi que les **enjeux environnementaux**, sont abordés de façon dispersée, sans cadre commun ni évaluation régulière des solutions mises en place, la modernisation ne peut bénéficier à tous. Le rapport recommande donc de **renforcer la coordination**, de mettre en place des outils pour mesurer la fiabilité des systèmes, d'anticiper les conséquences sur les équipes, et de privilégier des approches sobres et responsables. En définitive, il appelle à une **gouvernance transversale et prévoyante**, afin d'assurer un développement harmonieux, éthique et durable de l'intelligence artificielle dans les administrations.

2. Un Observatoire de l'IA pour la cohérence, l'éthique, l'état des connaissances scientifiques, la conformité et l'anticipation de l'impact sur les métiers

La mission propose de structurer une gouvernance adaptée aux enjeux de l'IA au sein du ministère de la Justice, avec comme mesure clé la création d'un **Observatoire de l'IA**, rattaché au Ministre de la justice.

Cet observatoire **réunirait les directions d'administration centrale, la DNUM, la CNIL, la défenseure des droits, les représentants des métiers ainsi que des experts IA issus de la recherche et du secteur privé**, pour apporter une approche pluridisciplinaire sur les sujets IA et constituerait un pilier essentiel pour garantir une gouvernance responsable et efficace de l'IA. Pour garantir la **pluralité des expertises** et des points de vue, il est essentiel d'intégrer à un comité permanent un **collège métier**, représentant les différents acteurs de la Justice, ainsi qu'un **collège éthique et scientifique**. L'ensemble de ces instances formerait ainsi l'Observatoire, assurant une supervision globale, équilibrée et éclairée du déploiement de l'IA dans le secteur de la Justice.

Cet Observatoire aurait pour missions clés :

- **Veiller à la cohérence stratégique et à l'efficacité des initiatives IA**, en assurant l'alignement des projets avec les priorités nationales et les besoins exprimés par les services. Il jouerait un rôle clé dans le pilotage « orienté résultats » et la maîtrise des risques, en s'appuyant sur des indicateurs d'impact opérationnel (par exemple : temps gagné sur la retranscription, amélioration de l'accès à la jurisprudence, diminution des délais de traitement des procédures, satisfaction des magistrats et agents) et en intégrant une gestion proactive des risques (biais, sécurité, conformité). En favorisant le partage des retours d'expérience et des bonnes pratiques entre

[39] Rapport de la Cour des Comptes, « L'intelligence artificielle dans les politiques publiques : l'exemple du ministère de l'économie et des finances », 18 juillet 2024

administrations, chercheurs et acteurs privés, l'Observatoire stimulerait l'innovation tout en sécurisant les usages.

- **Animer la réflexion relative à l'impact sur les missions et métiers des magistrats et agents du ministère de la Justice à l'ère de l'IA**, en anticipant les transformations induites par l'automatisation et l'assistance numérique, et en accompagnant les magistrats et agents dans l'adaptation de leurs pratiques professionnelles. Depuis 2017, l'actualité de l'IA a considérablement évolué, soulignant la nécessité de confronter régulièrement les prédictions à la réalité. On garde le souvenir de l'étude de Frey et Osborne[40] qui a marqué les esprits en estimant que 47 % des emplois américains étaient menacés d'automatisation d'ici 2033, en évaluant pour chaque métier la probabilité d'être informatisé sur la base d'avis d'experts et de modèles de machine learning. Quatre ans plus tard, une analyse de Fabernovel[41] montre que, contrairement à ces prédictions alarmistes, les métiers identifiés comme les plus menacés ont vu leur nombre d'emplois augmenter de 4,4 %, soulignant que l'impact de l'IA sur l'emploi est souvent surestimé à court terme. Les choix en matière d'IA relèvent ainsi d'enjeux politiques, éthiques et philosophiques, et appellent à une réflexion collective que l'Observatoire de l'IA pourrait contribuer à nourrir.

- **Promouvoir une culture de la transparence autour des usages de l'IA**, en informant régulièrement les magistrats et agents et les usagers sur les finalités, les limites et les garanties associées aux nouveaux outils.

Proposition : Instituer auprès du Ministre de la Justice un Observatoire de l'IA chargé de piloter sa stratégie d'intégration, d'assurer un suivi éthique des usages, l'impact sur les métiers, ou encore de garantir une veille scientifique régulière pour actualiser la compréhension de l'IA dans la Justice.

3. Une direction de programme chargée de l'IA

A ce jour, le ministère de la Justice **ne dispose pas d'une structure effective et industrialisée** spécifiquement dédiée à la production et au déploiement de l'intelligence artificielle à grande échelle. Les initiatives actuelles relèvent principalement de travaux exploratoires ou de projets pilotes, comme celui lancé au sein de la cour d'appel de Paris, en collaboration avec le parquet général de la cour d'appel et la DINUM. Si ces démarches témoignent d'une volonté d'innovation, elles restent **fragmentées** et **ne s'appuient pas sur une organisation pérenne**, dotée de moyens humains et techniques suffisants pour développer, déployer des outils IA et garantir leur conformité.

Les retours d'expérience d'autres ministères ainsi que les recommandations de la Cour des comptes et de la DINUM, soulignent pourtant **l'importance de structurer la gouvernance de l'IA autour d'une équipe dédiée, pluridisciplinaire et rattachée à un haut niveau hiérarchique**. Cette absence de structure freine la capacité du ministère à passer du stade de l'expérimentation à celui de la production à grande échelle, alors même que la sensibilité des données justifie un pilotage fort et une maîtrise de bout en bout des outils.

La Cour des comptes[42] préconise à ce titre explicitement la structuration de la gouvernance via des **instances de pilotage et la centralisation des compétences**. La DINUM encourage la **constitution d'équipes pluridisciplinaires** et dédiées à des produits pour accélérer et sécuriser les projets IA.

[40] Frey C. B. , Osborne M.A., Le futur de l'emploi « The future of employment : How susceptible are jobs to be computerisation ? » Oxford Martin School – Université d'Oxford, 2013
[41] Analyse par Fabernovel « Métiers menacés par l'IA : 4 ans après l'étude d'Oxford, le verdict », 2017
[42] Rapport de la Cour des Comptes « Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique », 8 avril 2024

Dans ces circonstances **la création d'une direction de programme dédiée à l'IA** au ministère de la Justice, rattachée à un haut niveau hiérarchique est un levier essentiel pour garantir la cohérence, la robustesse et la conformité des projets IA.

Proposition : Constituer une équipe en charge de la conduite opérationnelle de la stratégie IA, sous la forme d'une direction de programme, intégrant les expertises techniques, métier, juridiques et éthiques appliquées à l'IA et dimensionnée en fonction des cas d'usage retenus, rattachée au Secrétariat Général du Ministère.

4. Des partenariats institutionnels, avec les autres ministères ainsi qu'avec le secteur privé, renforceraient la capacité à relever les défis communs en matière de réglementation et d'éthique

La mise en œuvre efficace des initiatives d'IA au sein du ministère de la Justice repose sur une logique de collaborations et de partenariats stratégiques, tant au niveau ministériel qu'interministériel, ainsi qu'avec le secteur privé et le monde académique

5.A.1.1. Des partenariats interministériels pour soutenir le partage de bonnes pratiques et engager une réflexion sur des enjeux communs, notamment la protection des données personnelles

La multiplication des initiatives en matière d'IA au sein des ministères témoigne d'un réel dynamisme. Toutefois, cette effervescence demeure trop souvent marquée par une approche en silo, peu favorable au partage de bonnes pratiques sur des enjeux pourtant transversaux. Dans le cadre de ses travaux, la mission IA justice a engagé des discussions avec les équipes IA de plusieurs ministères ainsi qu'avec la DINUM afin d'identifier les pistes de mutualisation des efforts. Plus généralement, il conviendra donc de :

- **Encourager la mutualisation des outils IA ou les retours d'expérience des ministères ayant développé leurs propres outils pour répondre à des besoins partagés par l'ensemble des ministères**, tels que l'analyse documentaire, la recherche d'informations ou la rédaction de notes.

- **Partager les bonnes pratiques en matière d'actions d'accompagnement / formation** : **formations, webinaires, supports pédagogiques ou autres actions d'acculturation se multiplient localement** et gagneraient à être davantage diffuser afin de bénéficier à l'ensemble des ministères. Soutenir la création d'un **groupe de travail interministériel spécifiquement dédié aux enjeux réglementaires, en lien avec la CNIL**. Une telle coordination, qui pourrait être **pilotée par la DINUM**, favoriserait l'émergence d'une stratégie unifiée, accélérerait la mise en œuvre des projets et appuierait les prises de décision au sein des différents ministères.

5.A.2. Des partenariats avec le secteur privé et le monde académique

Les collaborations avec le secteur privé, notamment les **entreprises innovantes spécialisées dans l'IA**, permettent de tirer parti des expertises et des technologies avancées développées par ces acteurs. Parallèlement, la création de **partenariats avec des institutions académiques**, telles que l'INRIA et le CNRS, offre l'opportunité de bénéficier des travaux de recherche de pointe et de contribuer activement à l'innovation dans le domaine de l'IA, tout en favorisant un échange mutuellement bénéfique entre théorie et pratique.

B. Des ressources humaines et budgétaires à calibrer en fonction de l'ambition retenue au sein d'une direction de programme dédiée

La création d'une direction de programme IA, positionnée à haut niveau, composée d'une équipe pluridisciplinaire, constituée pour partie de ressources déjà existantes et renforcée par des recrutements complémentaires, permettra de répondre efficacement à l'ambition de transformation numérique de la Justice, d**'assurer la qualité, la sécurité et l'appropriation des produits IA**

L'équipe intégrée IA créée en 2024 est **actuellement sous-dimensionnée** en nombre (4 ETPs) et ne rassemble pas l'ensemble des compétences nécessaires pour passer à l'échelle. Ces compétences sont pourtant essentielles dès la première phase de la création et du déploiement de l'assistant IA en 2025. Selon les meilleurs standards observés dans les secteurs publics innovants, une structure efficace dédiée à la construction de produits IA doit impérativement reposer sur une **équipe pluridisciplinaire**, combinant :

- Des **scientifiques** et **ingénieurs** (data scientists, chercheurs appliqué IA, développeurs) capables de concevoir, déployer et sécuriser des solutions robustes et adaptées aux enjeux spécifiques de la Justice.
- Des **chefs de produits** (*product managers*) et **designers** assurant la coordination, la gestion agile des cycles de développement et l'alignement des livrables avec les attentes métiers et institutionnelles.
- Des **experts juridiques et éthiques** pour assurer la mise en conformité des solutions et leur respect des recommandations éthiques.
- Des **chargés d'accompagnemen**t en lien avec les référents métiers également issus des directions du ministère, chargés de faire remonter les besoins du terrain, de valider la pertinence des solutions, d'en mesurer l'impact sur les processus et chaînes métier et de faciliter leur appropriation par les magistrats et agents.

L'exemple de la Direction de la transformation numérique (DTNUM) du **ministère de l'Intérieur** illustre la pertinence de ce modèle : en s'appuyant sur un **réseau de référents métiers et techniques** présents dans la police, la gendarmerie et les services centraux, la DTNUM garantit la pertinence opérationnelle des solutions IA et leur appropriation rapide par les magistrats et agents. Cette organisation **favorise la remontée des besoins, l'adaptation des produits aux réalités du terrain et une dynamique d'innovation continue**. De même, l'Agence ministérielle pour l'IA de défense (AMIAD) au **ministère des Armées** s'appuie sur un **réseau de centres de la donnée et de l'IA implantés au plus près des opérationnels**, accélérant ainsi le déploiement des solutions et leur intégration dans les processus métier.

Le **dimensionnement** des effectifs à recruter pour la direction de programme IA du ministère de la Justice **dépend directement des missions identifiées**. **Le nombre de personnes à recruter croit proportionnellement au nombre de cas d'usage à traiter**. La structuration de la direction de programme sera également décisive. La mission préconise de constituer un état-major pour piloter la création et le déploiement de produits, une **équipe socle dotée de compétences transverses** (conformité, sécurité, mise à l'échelle), et une **équipe d'accompagnement au changement** pour anticiper l'adoption métier. L'essentiel des effectifs sera cependant déterminer par **le nombre de « squads », petites équipes pluridisciplinaires et autonomes**, chacune dédiée à un cas d'usage précis. Cette structuration, conforme aux standards des administrations les plus avancées, favorise la construction de produits IA utiles, robustes et alignés avec les priorités stratégiques et opérationnelles du ministère.

Encadré – Les éléments indispensables à la constitution de la future équipe IA

Pour assumer efficacement la construction, le déploiement et la gouvernance des outils d'IA au sein du ministère de la Justice, il est indispensable de constituer une équipe atteignant une masse critique et animant un réseau fonctionnel et matriciel au sein des différentes directions du ministère. Plusieurs arguments militent en faveur d'une telle intégration, du positionnement à haut niveau par un rattachement direct à la secrétaire générale et à ses adjoints et de ce dimensionnement minimal :

Pluridisciplinarité : Pour disposer de la capacité à développer et déployer les outils IA priorisés, pour en garantir la robustesse, l'éthique et la conformité juridique comme la sécurité, il est indispensable de réunir des compétences techniques, juridiques, métiers, éthiques et en gestion de produit, en nombre et en qualité adaptés au respect des jalons techniques, budgétaires et calendaires définis.

Complexité : à la fois technique et organisationnelle requérant des connaissances pointues, une capacité à anticiper et intégrer les avancées technologiques, à en mesurer les impacts sur les processus et les chaînes métier, à concevoir la conduite du changement qui en résulte.

Transversalité : l'activité à conduire tout autant que la gouvernance du dispositif dépassent la compétence d'une unique direction, que ce soit celle du numérique ou des directions dites « métier ». Une organisation fonctionnelle, sans intégration au sein d'une structure *ad hoc* rendrait difficile la préparation et la prise des arbitrages stratégiques pouvant surpasser des enjeux sectoriels plus immédiats. Par ailleurs, les synergies entre des cas d'usage issus de différents métiers sont fréquentes et fortes, et la centralisation des compétences permet donc un développement plus efficace et rapide.

Visibilité : la concentration des ressources et des compétences sur des sujets à fort enjeu est un facteur d'efficacité, d'innovation et de cohérence. Elle offre par ailleurs la possibilité d'une identification forte par l'ensemble des acteurs de l'écosystème IA, .

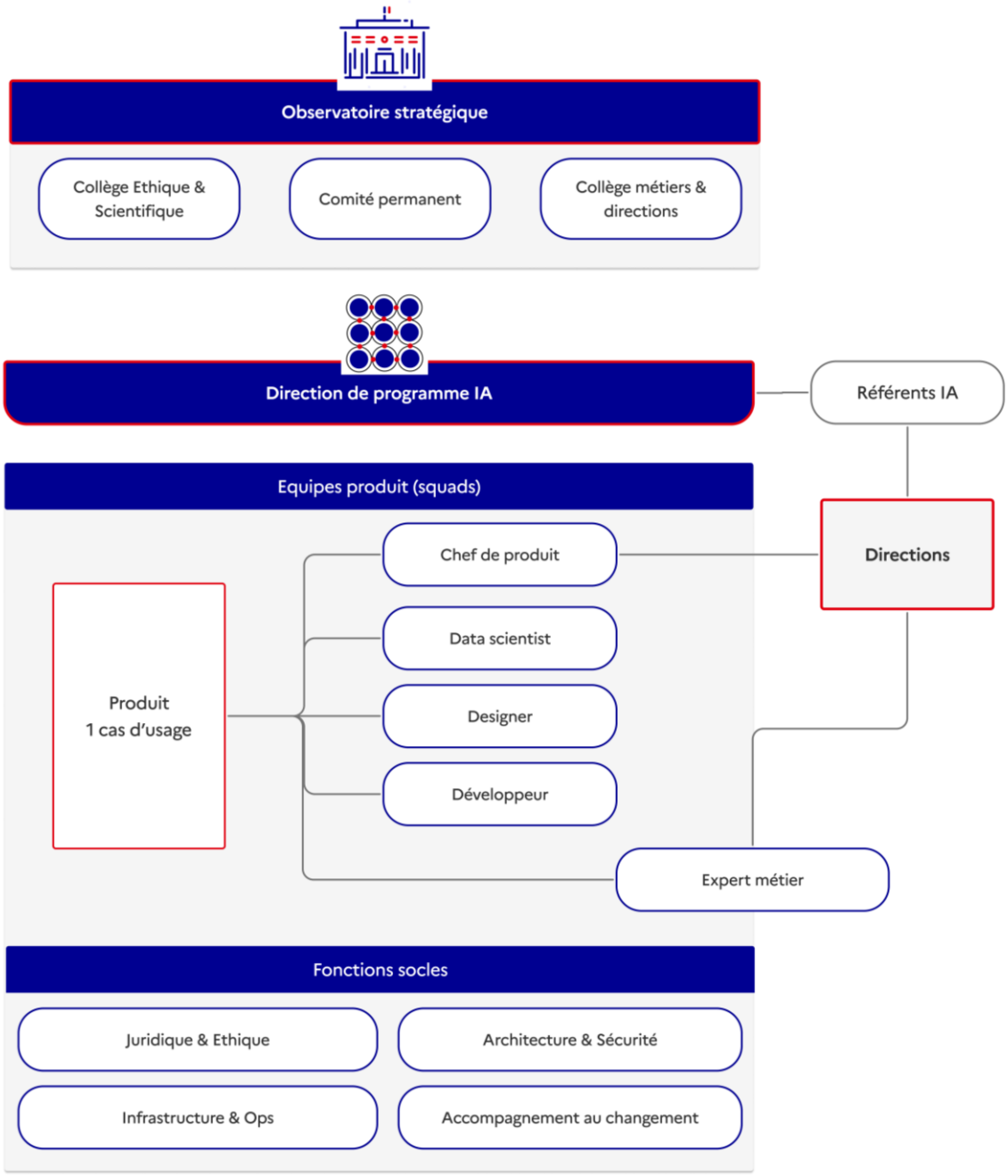
Attractivité : dans un univers à concurrence exacerbée pour la captation et la conservation des compétences, alors que les capacités d'offre salariale du ministère peuvent apparaître inférieures à celles d'un marché en constante évolution, une structure intégrée, visible, crédible à raison de sa masse et des réalisations dont elle peut se prévaloir, constitue un facteur certain d'attractivité.

Réactivité et agilité : Une structure étoffée permet de fonctionner en mode agile, d'adapter l'organisation et les ressources mobilisées pour chaque produit, favorisant l'expérimentation rapide, l'itération et la prise en compte au fil de l'eau des retours du terrain. Cette structure dédiée, souple, est la condition d'une indispensable vélocité dans un univers où la rapidité des sauts technologiques obligent à une ré-interrogation systématique et fréquente des choix opérés.

Suivi et évaluation : une structure dédiée, en responsabilité sur l'ensemble du champ de l'IA, du cadrage des besoins métiers à l'accompagnement au changement, en passant par le développement et le déploiement des outils, offre des garanties fortes en matière de respect des jalons, de maîtrise des risques associés aux projets et de production des données utiles à l'évaluation.

Benchmark des meilleures pratiques : Les exemples du ministère de l'Intérieur (DTNUM) et du ministère des Armées (AMIAD) montrent que la réussite des stratégies IA repose sur des équipes structurées et dimensionnées, capables de piloter, développer, sécuriser et accompagner les innovations sur le terrain.

Le Schéma de la gouvernance proposée



Afin d'assurer l'attractivité des postes pour des compétences en forte demande sur le marché privé, la **grille de rémunération établie par la DINUM** pourra être prise comme référence de seuil minimal en cohérence avec les compétences et le niveau d'expérience. Au-delà de la rémunération, il conviendra de mettre en place l'environnement et le matériel nécessaire pour permettre à ces magistrats et agents d'avoir un impact fort et rapide sur les métiers. La mise en place d'un **plateau projet central** permettra à ces différents acteurs de collaborer de manière pluridisciplinaire et d'assurer l'efficacité du développement

Les **ressources budgétaires** dégagées dans le cadre des investissements et de fonctionnement nécessaire à l'IA s'intègrent dans la **programmation budgétaire du comité stratégique de la transformation numérique ministériel** (CSTN), instance présidée par le garde des Sceaux.

A l'aune des priorisations budgétaires, un **plan programme triennal** est proposé au ministère pour illustrer les besoins dans le cadre d'une **approche en coût complet**. La **masse critique des effectifs attendus sur l'ensemble de ces activités est une des clés pour réussir cette transformation**.

C. Des mesures d'accompagnement des magistrats et agents sont nécessaires à l'appropriation de la solution IA proposée

Le sujet de la **formation à l'intelligence artificielle** s'impose comme un enjeu essentiel et une priorité nationale, car il dépasse largement le seul cadre professionnel. Il s'agit d'engager l'ensemble de la société française, du grand public aux experts, dans une appropriation collective de l'IA, à travers un vaste plan de sensibilisation et de formation inédit par son ampleur[43].

Reprenant les travaux de l'UNESCO, qui a élaboré un projet de lignes directrices[44] pour l'utilisation des systèmes d'IA dans les cours et tribunaux, nous constatons que **44 % des opérateurs judiciaires**, y compris les juges, les procureurs et les avocats, **utilisent des outils d'IA** tels que ChatGPT dans leur travail, mais seulement 9 % ont reçu une formation ou des directives institutionnelles appropriées.

1. Une stratégie d'accompagnement participative et inclusive articulée autour de trois axes : sensibilisation et formation, accompagnement à l'utilisation d'outils IA et animation d'un réseau de relais locaux

i. Sensibilisation et formation

La stratégie d'accompagnement doit répondre aux enjeux liés à l'utilisation de l'IA au sein du ministère : limiter les risques d'une utilisation non conforme et permettre à chaque agent de bénéficier pleinement des apports de l'IA dans l'exécution de ses missions. Elle devra également répondre aux interrogations des utilisateurs sur le stockage de leurs données ainsi que sur les enjeux de l'utilisation de l'IA dans leur quotidien. Le dispositif d'accompagnement repose ainsi sur trois axes complémentaires : la **sensibilisation et la formation de tous les magistrats et agents**, l'intégration native d'un **pas à pas dans l'assistant IA**, l'animation de **relais locaux et la communication.**

Afin de garantir cette appropriation, plusieurs actions de sensibilisation et de formation sont proposées par la mission :

- **MOOC** : Une formation en ligne vise à faire acquérir aux magistrats et agents les fondamentaux de l'IA, à développer leur aptitude à formuler des requêtes efficaces (l'art du prompt) et à leur fournir les outils nécessaires pour détecter et signaler les erreurs, tout en mettant l'accent sur les enjeux éthiques d'un usage responsable ;

- **Adoption d'une charte d'utilisation** des outils d'intelligence artificielle générative **et acceptation de conditions générales d'utilisation** : Le respect d'un cadre déontologique sera assuré par la validation d'une charte, accompagnée d'un principe d'adhésion aux conditions générales d'utilisation avant l'utilisation de la plateforme ;

- Une **approche pas à pas sera intégrée nativement** à la plateforme IA pour permettre aux utilisateurs de se familiariser de manière autonome et découvrir les fonctionnalités lors de l'utilisation.

[43] Commission nationale IA, Rapport 2024 - « IA Notre ambition pour la France »

- **Café Justice de l'IA** : conformément aux recommandations du Conseil national du numérique et à la mise en place de cette pratique au sein de la gendarmerie nationale et du ministère de la transition écologique, des rendez-vous sous forme de webinaire pourraient être mis en place auprès des magistrats et agents du ministère de la Justice pour échanger autour de l'IA.

Ces premières étapes de sensibilisation des magistrats et agents devront s'inscrire dans un cadre de formation plus global avec la création du campus du numérique permettant d'offrir une formation initiale et une formation continue plus approfondie et pérenne aux magistrats et agents.

5.A.2.1. Identification des relais locaux et stratégie de communication

Les relais traditionnels des différents réseaux, à l'instar des **Ambassadeurs à la Transformation Numérique pour les Services Judiciaires**, seront mobilisés afin de veiller à la bonne utilisation de l'outil, répondre aux questions des utilisateurs et assurer un lien avec la direction de programme. Ces relais devront bénéficier de formations complémentaires et s'organiser autour d'une communauté en ligne.

De plus, **une stratégie de communication dynamique devra être déployée**, soutenue par des lettres d'information, des webinaires, et permettra de maintenir un flux d'information régulier sur l'évolution du projet et les bonnes pratiques d'utilisation. Dans le cadre de ces actions, la prise en compte des publics réfractaires ou réticents à l'IA fera l'objet d'une attention particulière et d'actions adaptées afin de proposer une entrée progressive et différenciée dans le changement en identifiant les blocages, en montrant les utilités concrètes pour donner du sens au changement et ainsi éviter la saturation et l'abandon. L'ensemble des ressources mises à disposition, communications, supports de formation, fiches et la communauté devront être rassemblées sur l'Intranet Justice.

2. Accompagner la mise en service progressive de l'assistant IA

i. Une phase pilote impliquant 100 premiers utilisateurs testeurs (alpha-testeurs) à l'été 2025

Le déploiement initial du premier outil IA s'appuiera sur une phase pilote, programmée dès l'été, impliquant 100 alpha-testeurs volontaires issus de l'ensemble des directions du ministère et du terrain. Cette expérimentation, encadrée par un cahier de tests précis et enrichie par des requêtes spontanées, sera l'occasion de créer une première communauté d'utilisateurs IA réunie autour d'un club utilisateurs et d'un espace de discussion et aura pour objectif de vérifier la qualité des réponses et l'expérience utilisateur.
Au cours de cette phase, le **support auprès des utilisateurs** sera assuré par les équipes techniques et produit afin de réaliser les boucles d'itérations nécessaires à l'amélioration. Après cette phase, des correctifs pourront être appliqués pour améliorer le fonctionnement de l'assistant IA à partir des tests utilisateurs.

ii. Une extension auprès d'un panel élargi de 10 000 utilisateurs testeurs (bêta-testeurs) à partir de septembre 2025

A l'issue de la phase pilote, une extension pourra être envisagée dès septembre auprès d'un panel élargi de 10 000 bêta-testeurs afin de collecter des retours tant sur le produit que sur la robustesse du système dans le cadre d'une utilisation élargie. Au cours de cette phase, il conviendra de structurer le « support utilisateurs ». La mission recommande d'organiser la montée en compétence progressive du centre de soutien national (CSN) en étroite collaboration avec la direction de programme avant d'envisager une reprise complète du support lors de la généralisation.

iii. A l'issue de ces tests, une généralisation progressive pourra être envisagée dès décembre 2025, auprès des 90 000 magistrats et agents cibles du ministère de la Justice

Le dispositif d'accompagnement sera piloté par les indicateurs de déploiement, d'utilisation et d'impact, notamment le taux de personnes formées, le taux de déploiement, le nombre d'utilisateurs et le taux de

satisfaction ainsi que par des retours d'expérience. L'impact de l'IA sur les métiers du ministère pourra être évalué pour les métiers du terrain, notamment par le recours aux travaux de l'INRIA (LaborIA) sur la base du retour d'expérience du ministère de l'économie et des finances qui conduit actuellement cette étude.

D. La mise en place d'un « Campus du numérique » proposant une offre de formation initiale et continue aux enjeux du numérique, et plus spécifiquement à ceux de l'IA, est également préconisée

1. Les objectifs du campus

La création du **Campus du Numérique**[45], dispositif combinant un lieu physique et un espace numérique de formation vise à répondre aux **défis de la transition numérique** afin d'accélérer le développement des compétences et des usages responsables de l'IA dans les métiers de la Justice, de la fonction publique, de l'administration pénitentiaire et de la protection judiciaire de la jeunesse.

L'enjeu est double :

- **Utiliser l'IA pour moderniser la formation des écoles et renforcer leur collaboration** : intégration de l'IA dans les outils pédagogiques, ce qui permettra notamment de mutualiser les ressources pédagogiques et d'innover pédagogiquement grâce à des outils numériques immersifs,

- **Former les magistrats et agents (futurs et actuels) à l'IA** : former tous les publics des quatre écoles partenaires (ENM, ENG, ENAP, ENPJJ) et développer une « culture numérique partagée » garantissant l'acquisition des compétences numériques essentielles des apprenants et permettant de réduire les inégalités d'accès à la formation.

La **dimension hybride** du Campus du numérique (à la fois physique et virtuelle) apportera une accessibilité élargie, la flexibilité des parcours, la continuité pédagogique, un écosystème collaboratif, la réduction des coûts et l'optimisation logistique par la mutualisation des ressources pédagogiques numériques.

2. Description de l'offre de formation à l'IA

L'offre de formation du Campus du Numérique devra permettre de mettre en œuvre :

- La sensibilisation continue aux **évolutions technologiques et éthiques de l'IA**
- Le développement de **partenariats avec des experts et institutions spécialisées** pour enrichir les contenus pédagogiques : **une chaire « IA et Justice » pourrait ainsi être créée** afin d'explorer les applications de l'IA pour répondre aux enjeux de la Justice, sur le modèle de la chaire « IA et sécurité » du ministère de l'intérieur qui propose des actions de recherche, de formation et de développement technologique ainsi que l'organisation de séminaires et webinaires ouverts pour sensibiliser aux enjeux éthiques et techniques de l'IA appliquée à la sécurité (ou à la Justice dans le cas des présents travaux)s.
- L'organisation d'évènements, de séminaires et de colloques, notamment dans le cadre de la restitution de travaux de recherche, favorisant ainsi les échanges entre professionnels du terrain, experts, chercheurs et acteurs institutionnels aux fins d'assurer la diffusion de la culture du numérique et de l'IA au sein du ministère de la Justice.
- La mise en place de **formations continues pour les professionnels déjà en poste**, afin de les maintenir à jour sur les usages de l'IA dans leur domaine.

[45] Campus qui serait en lien étroit si ce n'est organique avec le Campus du Numérique Public — Campus du numérique public, qui « rassemble et valorise l'offre de formation interministérielle au numérique »

3. Enjeux de mise en œuvre du campus du numérique pour une mise en service dès 2026

Les premières formations IA pourraient avoir lieu dès 2026, après la phase de conception et de développement des modules.

Le projet pourra s'inspirer des **initiatives de la DINUM,** en mettant à disposition un ac**cès sécurisé à une plateforme d'apprentissage**. Les principaux défis à relever seront relatifs à son ergonomie et la sécurité de la plateforme ainsi que ses coûts de développement, de maintenance et d'hébergement. Il sera essentiel de mobiliser également les **ressources humaines suffisantes et qualifiées** tant pour la gestion et l'animation du portail en ligne que pour l'accueil et l'accompagnement sur le site physique du campus. Les publics formés ne se limitant pas aux magistrats et agents de l'État[46] la mise en place d'un système d'authentification et de parcours spécialisés par profil s'impose. Enfin, si certains contenus existent déjà, il sera nécessaire d'en concevoir de nouveaux, spécifiquement adaptés aux différents métiers et aux évolutions rapides des compétences numériques requises.

Afin de répondre pleinement aux **besoins de formation numérique** des quatre écoles de la justice, la création d'un **campus physique à Paris** – idéalement sur le site ENM Arborial – devra reposer sur plusieurs sous-jacents essentiels. Il sera nécessaire de prévoir une gouvernance partagée, réunissant des représentants de chaque école afin de piloter conjointement la mission, d'harmoniser les contenus pédagogiques et de garantir l'adéquation des formations aux spécificités de chaque filière. L'infrastructure devra être adaptée aux usages numériques intensifs : salles équipées de matériel informatique performant, espaces collaboratifs modulables, connexions haut débit sécurisées, et dispositifs d'accessibilité universelle. Un **dispositif de gestion et de protection des données sensibles** devra être mis en place, en conformité avec les exigences de cybersécurité et de confidentialité propres au secteur de la justice. Enfin, il conviendra de **mobiliser des ressources humaines qualifiées** – formateurs spécialisés, experts techniques, personnel d'accompagnement – et de **développer des partenariats** avec des acteurs publics et privés du numérique pour enrichir l'offre de formation et favoriser l'innovation pédagogique. Ce campus, **articulé avec le portail en ligne**, constituera ainsi un véritable **pôle d'excellence pour l'acculturation et la montée en compétences numériques** de l'ensemble des professionnels de la justice.

Proposition : Créer un « campus du numérique » dédié à la Justice », afin de sensibiliser les magistrats et agents aux enjeux de l'intelligence artificielle, de les accompagner dans l'appropriation des outils numériques et de leur proposer des formations adaptées à l'évolution des pratiques professionnelles et aux exigences éthiques.

[46] L'ENM forme à titre d'exemple des conseillers prud'homaux, des experts judiciaires, des avocats, journalistes de la presse judiciaire.

I- Liste des auditions et échanges

II- Liste des annexes

1. **Principes directeurs éthiques pour la gouvernance et la conception des SIA**
2. **Note juridique relative à l'encadrement de l'IA et arbre décisionnel juridique**
3. **Méthodologie de priorisation des cas d'usage**
4. **Labellisation et certification des systèmes d'IA dans le secteur de la Justice**
5. **Stratégie pour la création d'un campus du numérique**

I - Liste des auditions et échanges

1. Ministère de la Justice

Inspection générale de la Justice
- Stéphane NOEL, Chef de l'inspection, IGJ

Secrétariat général
- Audrey FARRUGIA, cheffe de service expertise et modernisation
- Claire STRUGALA, chargée de mission auprès de la cheffe de service
- Sylvie POSTEL, déléguée à la protection des données
- Philippe MONNOT, chef du service de l'immobilier
- Nicolas de SAUSSURE, chef du service des ressources humaines
- Frédéric WEIL, chef du bureau de l'activité digitale et stratégies de contenus à la direction de la communication

Direction des services judiciaires
- Pascal PRACHE, Directeur
- Roland de LESQUEN, directeur-adjoint
- Sylvie BERBACH, sous-directrice des ressources humaines des greffes
- Sandrine BRANCHE, sous-directrice des ressources humaines de la magistrature
- Guillaume MICHELIN, sous-directeur de l'organisation judiciaire et de l'innovation
- Félicie CALLIPEL, directrice de programme Portalis
- Ludovic BEY, adjoint au sous-directeur de l'organisation judiciaire et de l'innovation
- Gautier LEFORT, adjoint à la sous-directrice des finances, de l'immobilier et de la performance
- Delphine SOURMAIL, adjointe à la sous-directrice des ressources humaines des greffes
- Anaïs AGUDO, cheffe du bureau de la gestion de la mobilité et de la carrière
- Stéphanie FAURE, cheffe du bureau de la gestion prévisionnelle des ressources humaines des greffes
- Valérie GAILLOT-MERCIER, cheffe du bureau des juges élus ou désignés
- Virginie MAROSO, cheffe du bureau de la gestion de la performance
- Christophe POUGEOLLE, chargé de mission auprès de la sous-directrice des finances, de l'immobilier et de la performance

Direction des affaires civiles et du sceau
- Valérie DELNAUD, Directrice
- Emmanuelle MASSON, Directrice-adjointe
- Valentin RAGUIN, adjoint à la sous-directrice du droit civil

Direction des affaires criminelles et des grâces
- Laureline PEYREFITTE, Directrice

Direction de l'administration pénitentiaire
- Emmanuel RAZOUS, Directeur-adjoint
- Joachim BENDAVID, sous-directeur de l'expertise
- Sandrine ROSSI, adjointe au sous-directeur de l'insertion et de la probation
- Marc ETIENVRE, adjoint au sous-directeur des ressources humaines et des relations sociales
- Patrick GOMEZ, chef de la mission équipements
- Guillaume LORPHELIN, Chef de section SI, SNRP
- Gilles PIETRI, responsable du programme ATIGIP 360
- Isabelle WALTZ, responsable de l'Atelier Pédagogique du Numérique, ENAP

Direction de la protection judiciaire de la jeunesse
- Caroline NISAND, Directrice
- Marie LEON, Directrice-adjointe

2. Conseil supérieur de la magistrature

(Échanges informels)

- Rémy HEITZ, Procureur général près la Cour de cassation
- Patrick TITIUN, Ancien chef de cabinet à la CEDH, membre des deux formations
- Julien SIMON DELCROS, Président du Tribunal judiciaire d'Orléans
- Patrick WACHSMANN, Professeur émérite à l'Université de Strasbourg, membre des deux formations
- Alexis BOUROZ, Premier avocat général à la Cour d'appel de Paris, membre de la formation siège
- Sarah SALIMI, Secrétaire générale adjointe du CSM

3. Cour de cassation

- Christophe SOULARD, Premier président de la Cour de cassation
- Rémy HEITZ, Procureur général près la Cour de cassation
- Sandrine ZIENTARA, présidente de chambre, directrice du service de documentation, des études et du rapport (SDER), Cour de cassation
- Édouard ROTTIER, adjoint à la directrice du SDER, chef du pôle diffusion de la jurisprudence et open data, directeur du projet open data
- Matthieu ALLAIN, chef du bureau du droit du numérique et de la protection des données du SDER
- Sonya DJEMNI-WAGNER, avocate générale, chargée de mission auprès du procureur général de la Cour de cassation

4. Écoles de formation de la Justice

École nationale d'administration pénitentiaire

- Isabelle WALTZ COURNAC, responsable de l'atelier pédagogique du numérique, Direction de la formation

École nationale de la protection judiciaire de la jeunesse

- Frédérique BOTELLA, Directrice générale de l'ENPJJ, service d'appui à la pédagogie

École nationale des greffes

- Olivier LEMBERET, directeur adjoint en charge des activités pédagogiques
- Marina BARONE, experte pôle innovation et formation numérique

5. Juridictions

Juridictions civiles

- Caroline PACHTER-WALD, présidente de chambre sociale, cour d'appel d'Amiens
- Pierre ROUSSEL, directeur de greffe, tribunal judiciaire de Lille

Magistrats ayant participé à des tests de solution legaltech :

- Julien ADROIT, Juge d'instruction, Tribunal judiciaire de Nanterre
- Xavier BLANC, Président de chambre, Cour d'appel de Paris
- François BONNECARRERE, Juge d'instruction, Tribunal judiciaire de Marseille
- Aude CRISTAU, Présidente, Cour d'assise d'Orléans
- Marie-Catherine GAFFINEL, Conseillère, Cour d'appel de Paris
- Jean Christophe GAYET, Premier vice-président adjoint, Tribunal judiciaire de Paris

- Valérie GERARD, Première Présidente de chambre, Cour d'appel d'Aix
- Nicolas HENNEBELLE, Procureur de la République adjoint, Tribunal judiciaire de Paris
- Florence HERMITE, Conseillère, Cour d'appel de Paris
- Cyril JEANNINGROS, Juge, Tribunal judiciaire de Paris
- Muriel JOSSELIN-GALL, Vice-présidente, Tribunal judiciaire de Paris
- Gwenaëlle LEDOIGT, Présidente de chambre, Cour d'appel de Paris
- Aurélien LETOCART, Magistrat, AGRASC
- Gaspard LOSSON, Juge d'instruction, Tribunal judiciaire de Nancy
- Bastien MADELON, Vice-procureur de la République, Tribunal judiciaire de Marseille (JIRS)
- Julie MASMONTEIL, Juge, Tribunal judiciaire de Paris
- Caroline PACHTER-WALD, Présidente de chambre, Cour d'appel d'Amiens
- Marie PAPART, Vice-présidente, Tribunal judiciaire de Paris
- Stéphanie POTTIER, Vice-procureur de la République, Pôle national des crimes sériels ou non élucidés
- Diana SANTOS-CHAVES, Juge, Tribunal judiciaire de Paris
- Anne-Cécile SOULARD, Vice-présidente, Tribunal judiciaire de Paris

6. Ministères

Ministère de la Transition Ecologique

- Charline Meyer, chargée de mission, Ecolab

Ministère de l'Intérieur

- Emmanuel MAKSYMIW, adjoint à la Délégation Ministérielle à l'Intelligence Artificielle ;
- Frédéric AUBANEL, général, directeur de l'ANFSI ;
- Régis LAPORTE contrôleur général, directeur adjoint de l'ANFSI ;
- Cédric COLLARD, général, chef de direction des applications d'appui au commandement ;
- Patrick PERROT, général, coordonnateur de l'IA pour la Gendarmerie Nationale et conseiller IA au commandement de la gendarmerie dans le cyberespace ;
- Ysens DE FRANCE, chargée de mission IA au sein de la Gendarmerie Nationale.

Ministère de l'Economie et des Finances

- Raphaël AURUS, directeur du Bercy Hub et administrateur ministériel des données, Bercy Hub ;
- Vlad VALICA, responsable du Pôle incubateur d'innovation ministériel, Bercy Hub ;
- Anne-Sophie DUFERNEZ, cheffe du bureau transformation et transversalité, Direction générale du Trésor ;
- Pierre LANDAIS, adjoint à la cheffe de bureau, Direction générale du Trésor
- François JONKISZ, chef du département des systèmes d'information, Direction générale du Trésor ;
- Thomas BINDER, responsable de l'équipe IA, Direction générale des finances publiques, délégation à la transformation numérique.

Ministère des armées et des anciens combattants

- Alexandre BAILLOT, chef de la Mission d'Aide au Pilotage Centre d'expertise données & IA, secrétariat général pour l'administration du ministère des armées et des anciens combattants ;
- Guillaume VIMONT, chef du Centre d'expertise données & IA, secrétariat général pour l'administration du ministère des armées et des anciens combattants.

Ministère de l'Europe et des Affaires Étrangères

- Jean-Yves MAHÉ, administrateur ministériel des données délégué, Direction du numérique, bureau de la transformation ;
- Hugo BLAMONT, lead data scientist, Direction du numérique, bureau de la transformation ;
- Pascal NGUYEN, data scientist, Direction du numérique, bureau de la transformation.

7. Organisations syndicales et société civile

Participation aux CSA des services judiciaires, protection judiciaire de la jeunesse, et de l'administration pénitentiaire.

8. Professionnels du droit

Conseil National des Barreaux (CNB)]

- Hélène LAUDIC-BARON, vice-présidente
- Géraldine CAVAILLÉ, directrice adjointe et directrice juridique
- Anne-Charlotte VARIN, directrice des affaires publiques

9. Legaltechs, éditeurs juridiques et entreprises privées

Jimini.ai

- Raphael ARROCHE, co-fondateur et CEO
- Stéphane BÉREUX, co-fondateur et CTO

LexisNexis

- Christophe BONNET, Strategic Account Manager
- Chrystel FAURE, Directrice de la Stratégie Marchés Secteur Public et Académique
- Charles DANEAU, Customer Success Manager

Ordalie

- Léa FLEURY, Co-fondatrice et CEO

Lexbase

- Fabrizio PAPA TECHERA, Directeur Produit & Innovation

Lefebvre Group

- Sumi SAINT-AUGUSTE, Head of Prospective
- Michael BENESTY, Head of Research & Development
- Sarah LEVY, Chef de produit

Doctrine

- Paul GUILLEUX, Responsable Secteur Public
- Paul WARNIER, Conseiller Affaires Publiques et Juridiques

10. Organisme de certification

AFNOR

- Virginie DESBORDES, responsable du pôle confiance numérique d'AFNOR
- Thomas LOMMATZCH, directeur de la business unit Medical d'AFNOR Certification

11. Institutions et partenaires européens et internationaux

UNESCO

- Prateek SIBAL, Programme Specialist Digital Policies and Digital Transformation Section Communication and Information Sector UNESCO, Paris
- Dr. Kamel EL HILALI, Consultant, AI & the Rule of Law Digital Policies and Digital Transformation Section Communication and Information Sector UNESCO, Paris

Commission européenne

L'unité **A2 de la DG CONNECT de la Commission européenne :**

- Thierry BOULANGÉ, adjoint au chef d'unité
- Yodanka IVANOVA, cheffe de secteur, AI office, chargée de la mise en œuvre du RIA
- Laura JUGEL, policy officer

Les unités **A1 et D1 de la DG CONNECT de la Commission européenne :**

- Ivana ZEPPA, GenAI Pilots - Justice Sector -DG CONNECT A.1
- Matthieu DELESCLUSE, chef d'unité D1 par intérim en charge de la coordination des politiques et du EU Digital Europe Program

ANNEXES

ANNEXE n°1

Cadre juridique de l'intelligence artificielle

INTRODUCTION

Cette note a pour objectif de fournir le cadre juridique de l'IA, au niveau national et européen[1].

Il conviendra d'analyser les dispositions :

- De la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés »
- Du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)
- De la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, dite Directive « Police-Justice »
- Du règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (RIA), entrée en vigueur le 1er août 2024 (application progressive entre février 2025 et août 2027)[2]
- Du Code de procédure pénale et du Code de procédure civile
- De la loi n° 2016-1321 pour une République numérique
- De la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle
- De la doctrine « Cloud au centre »

[1] De manière générale, les dispositions relatives à la protection des données personnelles s'inscrivent dans un cadre juridique national (loi informatique et libertés), et supranational (règlement RGPD, directive police justice, convention 108+, convention européenne des droits de l'homme)

[2] Publication de lignes directrices par la Commission européenne attendue en fin d'année 2025.

Table des matières

1. Outil d'intelligence artificielle

Les systèmes d'intelligence artificielle (SIA) sont définis par le RIA comme « *un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels* » (art. 3.1).

L'entraînement des SIA nécessite l'utilisation régulière d'importants volumes de données provenant de diverses sources mais dont certaines constituent nécessairement des données à caractère personnel.
Sont ainsi concernés :

- Les systèmes fondés sur l'apprentissage automatique (machine learning) ;
- Les systèmes dont l'usage opérationnel est défini dès la phase de développement et les systèmes à usage général qui pourront être utilisés pour nourrir différentes applications (« general purpose AI »).
- Les systèmes dont l'apprentissage est réalisé « une fois pour toutes » ou de façon continue, par exemple en utilisant des données d'utilisation pour son amélioration.

Lorsque des données à caractère personnel sont utilisées, se pose la question de la **conformité avec la réglementation de protection des données à caractère personnel.** Sur un plan national, le traitement des données à caractère personnel de l'intelligence artificielle est soumis à la loi Informatique et libertés (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), qui a été modifiée afin de mettre en conformité le droit national avec le cadre juridique européen. Ces textes permettent la mise en œuvre concrète du Règlement général sur la protection des données (RGPD) et de la Directive « police-justice », applicable aux fichiers de la sphère pénale.

A l'inverse, si l'outil ne traite pas de données à caractère personnel, il n'existe aucun cadre à respecter d'un point de vue IL. Il pourrait notamment s'agir des cas d'usage de l'IA centrés sur de la recherche juridique intelligente, faisant appel à des modèles entraînés par des données publiques non personnelles.

Pour tout système d'IA, il convient de **distinguer deux phases** : **la phase d'entraînement de l'outil et la phase d'utilisation.** Les régimes peuvent être différents, notamment en fonction des données traitées.

2. Les types de données traitées par le SIA

Il convient de distinguer si les données traitées par le SIA sont des :

- **Données à caractère personnel** : toute information se rapportant à une personne physique **identifiée ou identifiable.** Est réputée être une « personne physique identifiable » celle qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (RGPD, art. 4.1).

- **Données sensibles** : données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les traitements des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits (RGPD, art. 9 et LIL, art. 6).

- **Données d'une sensibilité particulière** : des données, à caractère personnel ou non, d'une sensibilité particulière et dont la violation est susceptible d'engendrer notamment une atteinte à l'ordre public, à la sécurité publique. Ces données d'une sensibilité particulière recouvrent les données qui relèvent de secrets protégés par la loi, notamment aux procédures engagées devant les juridictions ou les données nécessaires à l'accomplissement des missions essentielles de l'État. Les **données judiciaires** en font donc partie.

- **Informations confidentielles** : toute information qui ne se rapporte pas à une personne physique mais qui devrait bénéficier de précautions afin d'en assurer la confidentialité.

3. Communication des données judiciaires

Parmi les différents cas d'usage de l'IA, tous ceux qui utilisent comme données d'entraînement ou comme données d'usage des pièces ou éléments tirés de dossiers de procédures pénales doivent respecter les règles relatives à la communicabilité de ces pièces ou relatives au « droit d'en connaître ».

S'agissant de l'utilisation du SIA après entraînement, en matière pénale comme en matière civile, les cadres posés par le CPP et le CPC ne semblent pas poser de difficultés particulières. En matière pénale, les règles du droit d'en connaître s'appliquent à l'utilisateur qui transmettra une procédure pénale à un outil d'IA.

Néanmoins, **la question de l'entraînement du moteur d'IA,** s'il apparaît nécessaire selon le cas d'usage de le faire sur la base de dossiers de procédures judiciaires, supposera la transmission d'un grand nombre de procédures à des tiers[3].

L'open data des décisions de justice peut constituer une première base de données. Elle est néanmoins insuffisante pour alimenter efficacement un système d'intelligence artificielle car elle ne vise que les « *décisions rendues publiquement et accessibles à toute personne sans autorisation préalable* » et ne renvoie pas, en tout état de cause, à l'intégralité des pièces composant une procédure mais seulement aux décisions de justice (COJ, articles R. 111-10 à R. 111-13).

Pour le pénal, cela renvoie à l'article R. 166 du CPP qui prévoit que peut être délivrée à des tiers, sans autorisation préalable, la copie :

- Des **arrêts de la Cour de cassation ;**
- Des **décisions des juridictions de jugement du premier ou du second degré, lorsqu'elles sont définitives et ont été rendues publiquement à la suite d'un débat public**.

Si ces dispositions ont l'avantage de permettre la communication de pièces judiciaires sans autorisation préalable du procureur de la République, elles portent toutefois sur un **nombre très restreint de décisions** et ne concernent pas les pièces de fonds de procédures,

Au-delà des dispositions relatives à l'open data, en matière pénale, l'article R. 170 est plus large en ce qu'il prévoit que le procureur de la République ou le procureur général, peut, autoriser la communication au tiers demandeur qui justifie d'un motif légitime :

- Des décisions non définitives ;
- Des décisions rendues par les juridictions d'instruction ou de l'application des peines ;
- Des décisions rendues par les juridictions pour mineurs ou après des débats tenus à huis clos ;

[3] En matière pénale, les règles applicables au secret de l'enquête et de l'instruction (CPP, art. 11[3]) constituent une exigence supplémentaire à respecter

- **Des autres actes ou pièces d'une procédure pénale** (sont concernés les PV, expertises, rapports, décisions, ordonnances pénales, etc.).

Néanmoins, il pose plusieurs conditions préalables à sa mise en œuvre[4] :

- Une **demande préalable du tiers** : la communication ne paraît pas pouvoir être réalisée à l'initiative du procureur de la République sur ce fondement ;
- **L'autorisation du procureur de la République** s'il s'agit d'une décision ou d'une pièce émanant d'une juridiction pénale du premier degré et détenue par le greffe du tribunal judiciaire, ou du procureur général s'il s'agit d'une décision émanant ou d'une pièce de la cour d'appel ou détenue par le greffe de la cour ;
- La justification par le demandeur d'un **motif légitime**, lequel relève de l'appréciation du magistrat.

Ainsi, si le fondement privilégié pour mettre à disposition du logiciel le maximum de pièces sur l'article R. 170, un important travail d'occultation est nécessaire, des noms d'un certain nombre d'acteurs ayant concouru à la procédure et de tout élément qui n'a pas à être divulgué et il convient d'obtenir l'accord des procureurs de la République concernés.

A noter que dans le cadre d'un groupe de travail Copies aux tiers, une réflexion est en cours pour intégrer au champ de l'article R. 170 les demandes de copies intègres – toujours sous réserve des occultations obligatoires de l'article R. 169.

Il convient de rappeler qu'avec le déploiement de la PPN, les pièces de procédure seront nativement numériques et pourront utilement être utilisées dans le cadre des différents cas d'usages judiciaires de l'IA en matière pénale. D'un point de vue informatique et libertés, l'accès à ces données est régi par les articles R. 249-9 et suiv. du CPP. Les magistrats, auditeurs de justice, agents du greffe, juristes assistants, assistants de justice, délégués du procureur et avocats peuvent accéder aux informations contenues dans le traitement, pour le seul accomplissement des missions qui leur sont confiées. Une liste plus large mentionne les personnes susceptibles d'être destinataires du dossier de procédure numérique (personnes concourant à la procédure, les avocats, les parties et les administrations autorisées).

En matière civile, il n'existe **pas de dispositions générales similaires à celles prévues à l'article R170 du CPP** : seuls peuvent être communiquées aux tiers la copie des décisions rendues publiquement (article 11-3 de la loi n°75-596 du 10 juillet 1975), ce qui interdit donc la communication à des tiers de copies de décisions rendues en chambre du conseil. De même il n'existe **pas de disposition générale permettant la remise d'une copie d'une pièce de procédure autre qu'une décision**.

Enfin, en l'état de la réglementation sauf dans les cas où le recours à la communication électronique est obligatoire[5], les pièces de procédure (actes et pièces) ne sont pas numérisées. Lorsque la communication électronique est obligatoire, cette dématérialisation ne concerne que les actes de procédure (et non les pièces produites par les parties). De même le cadre règlementaire permet l'établissement d'un jugement

[4] L'article R. 170 prévoit également que « L'autorisation peut n'être accordée que sous réserve de l'occultation des éléments ou des motifs de la décision qui n'ont pas à être divulgués », ce qui s'ajoute aux occultations systématiques prévues à l'article R. 169 s'agissant de l'identité des personnes ayant concouru à la procédure ou participé aux opérations de jugement

[5] Procédure écrite ordinaire et procédure à jour fixe devant le tribunal judiciaire (art. 850 CPC) et procédure contentieuse relevant de la procédure avec représentation obligatoire (art. 930-1 CPC) concrètement, les conclusions des avocats sont envoyées à la juridiction via RPVA en format .pdf. Pour le reste, la communication électronique est facultative.

sur « support électronique », toutefois la mise en œuvre de cette faculté suppose un minutier électronique civil en cours de déploiement.

4. Encadrement du traitement de données personnelles

4.1 Réglementation générale

Sur un plan national, le traitement des données à caractère personnel par des systèmes d'intelligence artificielle est soumis à la **loi Informatique et libertés** (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Cette loi et son décret d'application[6] ont été modifiés afin de **mettre en conformité le droit national avec le cadre juridique européen en matière de protection des données**. Ces textes permettent la mise en œuvre concrète du Règlement général sur la protection des données (RGPD) et de la Directive « Police-Justice », applicable aux fichiers de la sphère pénale.

La LIL affirme les **grands principes applicables aux traitements des données à caractère personnel** (art. 4), reprenant ceux énoncés au sein du RGPD (art. 5) et transposant ceux applicables aux traitements entrant dans le champ de la directive Police-Justice. Tous, sont d'interprétation souple, et appliqués suivant une appréciation au cas par cas :

Principe de loyauté : les données doivent être traitées de manière licite, loyale et, pour les traitements relevant du RGPD, transparente au regard de la personne concernée.

Le traitement n'est licite que s'il se fonde sur l'une des **six bases légales** :

- Le consentement de la personne concernée ;
- L'exécution d'un contrat ;
- Le respect d'une obligation légale ;
- La sauvegarde des intérêts vitaux ;
- L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- La poursuite d'un intérêt légitime.

Principe de proportionnalité ou minimisation des données : les données doivent être adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant de la directive Police-justice, non excessives.

Principe d'exactitude : les données doivent être exactes, et si nécessaire, tenues à jour.

Principe de limitation de la durée de conservation : les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Principe de sécurité : les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel.

Principe de finalité : les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Les finalités doivent être définies avant le traitement des données.

[6] Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les règles régissant l'extension de finalités des traitements dits de « Police-Justice » sont plus complexes et les données collectées pour ces finalités ne peuvent être traitées pour d'autres finalités, à moins que ce ne soit pour la tenue d'archives ou à des fins scientifiques, statistiques ou historiques (s'appliquent alors les régimes du RGPD en ces matières).

4.2 Traitements interdits

L'article 6 de la loi informatique et libertés (reprenant l'article 9 du RGPD) pose le principe **d'interdiction de traitements de données sensibles**[7], assorti de certaines **exceptions** : dont l'exception de consentement ou si les données sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des **juridictions agissent dans le cadre de leur fonction juridictionnelle**[8].

D'autres dérogations à l'interdiction de traitement des données sensibles sont prévues par la loi, notamment au sein de l'article 44 de la LIL pour les traitements portant notamment sur la **réutilisation des informations figurant dans les décisions de justice**[9].

Il convient d'ajouter les dérogations visant les **traitements dits « Police-justice »** (voir *infra*). Le traitement est possible uniquement **en cas de nécessité absolue**, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et **s'il est autorisé par une disposition législative ou réglementaire**, s'il vise à protéger les intérêts vitaux d'une personne physique, ou s'il porte sur des données manifestement rendues publiques par la personne concernée.

4.3 Décision de justice prise sur un traitement automatisé de données à caractère personnel

L'article 47 de la LIL, reprenant l'article 22, I du RGPD, prévoit :

- Qu'aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne ;

- Qu'aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, sauf exceptions comme des décisions administratives individuelles prises sur le fondement d'un traitement algorithmique, à condition que les données ne soient pas sensibles.

Les personnes destinataires de décisions individuelles fondées sur un traitement algorithmique bénéficient d'une information renforcée et, pour partie, spontanée.

[7] A noter que des données qui permettent indirectement de prendre connaissance de données sensibles doivent elles-mêmes être considérées comme des données sensibles et, par corrélation, se voir appliquer le régime très strict établi les concernant (CJUE, 1er août 2022, aff. C-184/20).

[8] Autres exceptions pour le champ du RGPD : Intérêt vital, données manifestement rendues publiques par la personne concernée, intérêt public important, associations religieuses, politiques, syndicales pour les données de leurs membres. La Directive, elle, ne prévoit pas de dérogation spécifique en cas de consentement ou d'intérêt public, mais renvoie au droit national ou au droit de l'Union.

[9] Autres dérogations : les traitements effectués par un membre d'une profession de santé ou par une autre personne à laquelle s'impose une obligation de secret professionnel, les traitements à finalités statistiques mis en œuvre par l'INSEE, les traitements de données de santé d'intérêt public, les traitements de données biométriques, traitements à finalité de recherche publique.

De manière analogue, en matière de service en ligne de conciliation, de médiation ou d'arbitrage, la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle vient encadrer l'utilisation de système d'intelligence artificielle. Elle prévoit que les services de conciliation, médiation ou arbitrage en ligne ne peuvent avoir pour seul fondement un traitement algorithmique ou automatisé de données à caractère personnel. Lorsque ce service est proposé à l'aide d'un tel traitement, les parties doivent en être informées par une mention explicite et doivent expressément y consentir (art. 4-1 à 4-3). Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par le responsable de traitement à toute partie qui en fait la demande. Le responsable de traitement s'assure de la maîtrise du traitement et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la partie qui en fait la demande la manière dont le traitement a été mis en œuvre à son égard.

S'agissant **des décisions administratives individuelles** (ex. si une SIA est utilisée pour une gestion RH individuelle au sein du MJ – gestion des congés / transparences)**, la loi n°2016-1321 pour une République numérique,** a, elle, précisé que les décisions individuelles prises sur le fondement d'un traitement algorithmique doivent « ***comporte(r) une mention explicite en informant l'intéressé***. *Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande* ».Cette disposition consacre donc un **droit d'information pour les personnes qui font l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique**[10].

4.4 Droits des personnes concernées

Les personnes concernées par des traitements de données personnelles disposent de droits leur permettant de garder la maîtrise des informations les concernant tout au long du cycle de vie du SIA.

Le **recueil du consentement** : Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée. Le consentement est "préalable" à la collecte des données. Il est notamment requis en cas :

- De collecte de données sensibles ;
- De réutilisation des données à d'autres fins ;
- D'utilisation de cookies pour certaines finalités ;
- D'utilisation des données à des fins de prospection commerciale par voie électronique.

[10] Trois points d'information :

- doivent être publiées en ligne, de manière spontanée, les « règles » qui définissent les « principaux » traitements algorithmiques des administrations d'au moins 50 agents, lorsqu'ils fondent des décisions individuelles (CRPA, art. L. 312-1-3) – ce qui sera évidemment le cas du MJ ;
- toute décision individuelle prise sur le fondement d'un traitement algorithmique doit le mentionner et rappeler les droits dont bénéficie son destinataire (art. L. 311-3-1).
- si l'intéressé en fait la demande, l'administration doit lui communiquer les règles définissant le traitement, et les principales caractéristiques de sa mise en œuvre. Les informations à communiquer, sous une forme intelligible, sont énumérées à l'article R. 311-3-1-2 du CRPA : il s'agit du degré et du mode de contribution du traitement algorithmique à la prise de décision, de la nature des données traitées et leurs sources, des paramètres du traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé, ainsi que les opérations effectuées par le traitement.

Le droit à l'information (LIL, art. 48 et RGPD, art. 12 à 14) : la collecte de données personnelles doit s'accompagner d'une information claire et précise des personnes sur :

- L'identité du responsable du fichier ;
- La finalité du fichier ;
- Le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse ;
- Les destinataires des données ;
- Leurs droits (droit d'accès, de rectification, et d'opposition) ;
- Les éventuels transferts de données vers des pays hors UE ;
- L'information est préalable à la collecte des données.

Le droit d'accès (LIL, art. 49 et RGPD, art. 15) : toute personne peut accéder à l'ensemble des informations la concernant, connaître l'origine des informations le concernant, accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant ou encore en obtenir la copie.

Le droit à la maîtrise de ses données :

- **Droit d'opposition** (LIL, art. 56 et RGPD, art. 21) : les personnes doivent pouvoir s'opposer à la réutilisation par le responsable du fichier de leurs coordonnées à des fins de sollicitation. Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale.

- **Droit de rectification** (LIL, art. 50 et RGPD, art. 16) : droit d'obtenir du responsable de traitement la rectification des données à caractère personnel la concernant qui sont inexactes.

- **Droit à l'effacement** (LIL, art. 51 et RGPD, art. 17) : droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, si, notamment, les données ne sont plus nécessaires au regard des finalités ou ont fait l'objet d'un traitement illicite.

- **Droit à la limitation des données** (LIL, art. 53 et RGPD, art. 18) : droit d'obtenir du responsable du traitement la limitation du traitement si l'exactitude des données est contestée par la personne concernée afin que le responsable du traitement puisse vérifier, si le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ou encore si le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice.

- **Droit à la portabilité des données** (LIL, art. 55 et RGPD, art. 20) : Toute personne a le droit de recevoir les données qui la concerne et qu'elle a fournies à un responsable de traitement, de les réutiliser, et de les transmettre à un autre responsable de traitement.

L'article 16 de la loi pour une République numérique est venue prescrire aux administrations le fait de veiller à « *préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information* », et d'encourager l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation, de tout ou partie, de ces systèmes d'information.

Elle est en outre venue modifier la LIL en prévoyant la création de nouveaux droits destinés à assurer une meilleure protection de l'utilisateur et de ses données :

- Un **« droit à l'oubli » spécifique aux mineurs** permettant d'obtenir l'effacement, dans les meilleurs délais, des données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information, lorsque la personne concernée était mineure[11].
- Un **droit à la « mort numérique »**, qui prévoit que toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès[12].

5. Détermination des finalités du SIA et régime applicable

Un SIA reposant sur l'exploitation de données personnelles **doit être développé avec une « finalité »**, c'est-à-dire un objectif bien défini. Il doit être **déterminé**, soit établi dès la définition du projet, **explicite**, autrement dit connu et compréhensible, et **légitime**, c'est-à-dire compatible avec les missions de l'organisme.

Le RGPD, auquel des renvois sont effectués par la LIL, a vocation à s'appliquer à l'ensemble des traitements de données à caractère personnel dans les Etats membres, à la fois dans le secteur public et le secteur privé, à l'exception toutefois des traitements mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit de l'Union européenne, telles que les activités de sûreté de l'Etat ou de défense nationale, et ceux mis en œuvre aux fins de la directive « Police-Justice ». La ligne de partage entre les traitements relevant du RGPD et ceux relevant de la directive « Police-Justice » n'est pas toujours facile à tracer.

5.1 Finalités civiles

Le RGPD s'applique à l'ensemble des traitements de données à caractère personnel dans les Etats membres (même sans établissement de l'entreprise sur le territoire dès lors que des résidents dans l'UE sont visés par le traitement des données).

5.1.1 Formalités préalables

La mise en œuvre d'un traitement de données à caractère personnel doit faire l'objet d'un acte règlementaire (a minima un arrêté ministériel)

Toutefois, dès lors que le traitement est susceptible de porter **sur des données sensibles**, ils doivent être **autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL**. Cet avis est publié avec le décret autorisant le traitement.

Certains traitements peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise.

A noter qu'un acte réglementaire unique est possible pour les traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant les mêmes destinataires ou catégories de destinataires (LIL, art. 31).

[11] Également prévu à l'article 17 du RGPD.
[12] Le décret d'application de cette disposition n'a pas été pris.

Pour les demandes d'avis à adresser à la CNIL, sont demandés :

- L'identité et l'adresse du responsable du traitement ou celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;
- La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 31 et 32, la description générale de ses fonctions ;
- Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;
- Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;
- La durée de conservation des informations traitées ;
- Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 31 et 32, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
- Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
- La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu aux articles 49,105 et 119, ainsi que les mesures relatives à l'exercice de ce droit ;
- Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;
- Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne, sous quelque forme que ce soit.

Exception : traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique : Un décret en Conseil d'Etat, pris après avis de la CNIL, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

Elle se prononce dans un délai de huit semaines à compter de la réception de la demande (renouvellement de six semaines possible).

5.1.2 Obligations incombant au responsable du traitement

La loi prévoit ensuite les obligations incombant au responsable du traitement[13] :

- **Mise en œuvre de mesures techniques et organisationnelles** (LIL, art 57 et RGPD, art. 24) appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD et à la LIL.

- Le responsable de traitement doit **tenir un registre des activités de traitement**, sous forme écrite (conditions à l'article 30 du RGPD) et mettre en œuvre des **mesures de journalisation**.

- **La notification des violations de données à caractère personnel à la CNIL** : prendre des mesures appropriées pour y remédier et communiquer à la personne concernée la violation de ses données à caractère personnel dans certains cas. Des dérogations à cette obligation de communication sont prévues par la loi.

[13] La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre (RGPD, art. 4)

- **Faire appel à des sous-traitants[14] qui présentent des garanties suffisantes et qui ne pourront agir que sur instruction du responsable de traitement** (LIL, art. 60 et RGPD, art. 28). En outre, le traitement réalisé par un sous-traitant doit être régi par un contrat ou tout acte juridique (définissant l'objet de la durée, nature et finalité, type de données, catégories de personnes concernées)[15]. Les sous-traitants sont tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité.

5.1.3 Obligations particulières prévues pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques

D'autres obligations particulières sont prévues pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques[16] (LIL, art. 62 et 63 et RGPD, art. 35 et 36).

Une analyse d'impact des opérations de traitement envisagées sur la protection des données doit être réalisée par le responsable du traitement, préalablement à la mise en œuvre. Elle doit faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées.

Cette analyse est particulièrement requise d'une part, pour l'évaluation systématique et approfondie d'aspects personnels, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la **base de laquelle sont prises des décisions produisant des effets juridiques** à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire, d'autre part, pour le traitement à grande échelle de catégories particulières de données sensibles ou de données à caractère personnel relatives à des condamnations pénales et à des infractions. En pratique, en matière civile une AIPD sera très probablement requise dès lors que les données collectées le seront à une large échelle, qu'elles peuvent contenir des données sensibles et qu'elle peut aboutir à un croisement de données.

[14] La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

[15] Le lien entre le ministère de la Justice et le sous-traitant, et notamment le détail des obligations qui incombe à chacune des parties, devra faire l'objet d'une convention de sous-traitance. Le responsable de traitement doit s'assurer que son sous-traitant respecte la réglementation. Pour ce faire, le contrat doit impérativement comporter une clause selon laquelle le sous-traitant tient à disposition du donneur d'ordre toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre la réalisation d'audit par le responsable de traitement (ou un autre auditeur qu'il a mandaté).

[16] Compte tenu de la nature, de la portée, du contexte et des finalités du traitement, une AIPD doit être faite doit obligatoirement être menée si deux au moins des neuf critères listés par la CNIL sont remplis. En pratique, en matière civile une AIPD sera très probablement requise dès lors que les données collectées le seront à une large échelle, qu'elles peuvent contenir des données sensibles et qu'elle peut aboutir à un croisement de données.

La CNIL a adopté une délibération portant adoption de la liste de types d'opérations de traitement pour lesquelles une analyse d'impact n'est pas requise[17].

L'analyse contient au moins : une **description** systématique des opérations de traitement envisagées et des finalités du traitement, une **évaluation de la nécessité** et de la **proportionnalité** des opérations de traitement au regard des finalités, une évaluation des **risques pour les droits et libertés** des personnes concernées ; et les mesures envisagées pour **faire face aux risques** (garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD).
Lorsque le traitement est nécessaire au respect d'une obligation légale ou nécessaire à l'exécution d'une **mission d'intérêt public ou relevant de l'exercice de l'autorise publique** (art. 6, I, c) et e)) et a une base juridique dans le droit de l'Union ou de l'État membre, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une **analyse d'impact générale** réalisée dans le cadre de l'adoption de la base juridique en question, pas d'étude d'impact, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

Le responsable de traitement est également tenu de **consulter la CNIL préalablement** à la mise en œuvre du traitement lorsqu'il ressort de l'analyse d'impact que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque (LIL, art. 63 et RGPD, art 36).

5.2 Finalités pénales

Pour mémoire, le RGPD a vocation à s'appliquer à l'ensemble des traitements de données à caractère personnel dans les Etats membres, à la fois dans le secteur public et le secteur privé, **à l'exception toutefois des traitements mis en œuvre aux fins de la directive « Police-Justice ».**

5.2.1 Champ d'application

La directive « Police-Justice » s'applique pour tous les traitements de données à caractère personnel mis en œuvre :

- A des **fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales**, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

- **Par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique**.

A noter que les données collectées ne peuvent être traitées pour d'autres finalités que celles énoncées, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires ou par le droit de l'Union européenne. Lorsque des données sont traitées à d'autres fins, le RGPD s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application.

[17] Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise

Il faudra notamment distinguer :

- La question des jeux de données judiciaires servant à l'entraînement du modèle. La problématique sera alors le *machine learning* consistant à fournir des données à un algorithme sans connaître le résultat final, ce qui peut entrer en contradiction avec l'un des principes du droit à la protection des données personnel selon lequel le responsable de traitement traite les données personnelles dans un but précis (principe de finalité) ;

- La question de l'usage de l'outil d'IA après entraînement qui impliquera que celui-ci soit alimenté de données issues de procédures judiciaires, relevant nécessairement pour partie de l'article 6 de la LIL.

A titre d'exemple, les outils d'IA de synthèse de dossiers devront soit faire l'objet d'un entraînement spécifique sur la base de procédures judiciaires, ce qui implique un encadrement, soit se baser sur des données d'entraînement génériques. L'utilisation de cet outil pour synthétiser un dossier précis devra respecter le cadre du titre III.

5.2.2 Traitements portant sur des données sensibles

S'agissant des traitements portant sur des données sensibles, par principe, interdits, la loi prévoit la possibilité d'en déroger uniquement **en cas de nécessité absolue**, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit **s'il est autorisé par une disposition législative ou réglementaire**, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée (LIL, art. 88).

5.2.3 Obligations spécifiques de la directive

Les principes relatifs aux traitements des données, c'est-à-dire le traitement loyal et licite, le principe de finalité, d'adéquation et proportionnalité, d'exactitude ou encore de sécurité, tels que prévus à l'article 4 de la directive 2016/680 sont identiques aux principes posés par le RGPD (*cf. supra*).

Certaines obligations prévues par la directive sont identiques à celles prévues par le RGPD (analyse d'impact relative à la protection des données à caractère personnel, mesures techniques et organisationnelles appropriées, registre des activités, sous-traitance présentant des garanties suffisantes, encadrement des décisions automatisées – article 95 LIL, etc.). **Aussi, les traitements relevant de la directive doivent être autorisés par arrêté ou décret en Conseil d'Etat (si des données sensibles sont collectées) pris après avis publié de la CNIL**.

D'autres sont spécifiques à la directive « Police-Justice », des obligations particulières ayant été instaurés. Le responsable de traitement doit **établir**, le cas échéant et dans la mesure du possible, **une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées**[18].
Il doit également **distinguer entre les données à caractère personnel** (données fondées sur des faits/données fondées sur des appréciations personnelles) et **vérifier la qualité des données** (garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition).

En raison de la spécificité du champ d'application de la directive « Police-Justice », certains **droits des personnes concernées** dans le RGPD ne se retrouvent pas dans la directive. Comme le permet le RGPD, la Directive prévoit que les droits des personnes concernées puissent faire l'objet de restrictions.

[18] Comme par exemple les personnes reconnues coupables d'une infraction pénale, les personnes victimes d'une infraction pénale, les tiers à une infraction pénale etc.

Néanmoins, elle prévoit un régime de protection supplémentaire en instituant un régime d'exercice indirect des droits lorsque ceux-ci ont été limités[19].

A titre d'exemple, la directive prévoit une exception de procédure pénale pour le droit d'accès, de rectification, d'effacement ou droit à l'information : lorsque les données figurent dans une décision judiciaire, dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale.

5.2.4 Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions

S'agissant des traitements de condamnations pénales et d'infractions, ne relevant pas de la directive Police-Justice, le régime général de la LIL et le RGPD s'appliquent.

Les articles 10 du RGPD et 46 de la LIL indiquent notamment que les **traitements de données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes** ne peuvent être effectués que par cinq catégories de personnes à des fins non pénales : les juridictions et certains autorités publiques ou privées, les auxiliaires de justice, les personnes autorisées à tenir des fichiers privés d'infractions, les sociétés d'auteur et les réutilisateurs des informations publiques figurant dans des décisions de justice.

5.3 Utilisation des données à d'autres fins

Pour toute autre finalité, il convient de faire application de la LIL et du RGPD (*cf. supra*).
Notamment, l'article 88 du RGPD apporte des précisions sur le traitement de données dans le cadre des relations de travail et permet aux Etats membres de prévoir des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, **de la gestion, ou encore de la planification et de l'organisation du travail.**

Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.

Il pourrait notamment s'agir du cas d'usage d'aide à l'audiencement ou aux plannings de service qui contiendrait des données personnelles, mais, ne serait pas mise en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, donc il relèvera du Titre II.

[19] Le régime d'exercice indirect des droits préexistait à l'adoption de la Directive police-justice en droit national, il couvre également les traitements de données dans le champ du RGPD et de la sécurité nationale. Il permet de s'adresser à la CNIL pour qu'elle exerce les droits qui ont été restreints auprès du responsable de traitement, et qu'elle ne communique pas systématiquement le détail des vérifications et l'issue de ses démarches si le traitement des données en question justifie de maintenir la confidentialité sur ces aspects.

5.4 Traitements ayant plusieurs finalités

La CNIL[20] et le Conseil d'Etat[21] dans un avis ont, à l'occasion de l'analyse du projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du 6 janvier 1978, consacré **la possibilité qu'un traitement soit « mixte »**, c'est-à-dire relève de plusieurs cadres juridiques.
Plusieurs conséquences découlent d'une mixité des régimes « Informatique et Libertés », à savoir :

- **Une nécessaire identification des bases juridiques adéquates pour chaque finalité du traitement mixte** ;
- **Le traitement doit faire l'objet d'un texte réglementaire pris après avis de la CNIL (art. 90 de la LIL) ;**
- **Un important impact sur les droits des personnes (selon la note du BIL[22] et le Conseil d'Etat[23]) :**
    - Lorsque les données collectées en application d'une finalité sont **facilement identifiables** et peuvent être distinguées des autres données relevant des autres finalités à Application distributive et précise des droits « Informatique et Libertés », selon le régime juridique applicable à chaque finalité ;
    - Lorsque les données collectées en application d'une finalité sont **difficilement identifiables** et ne peuvent pas être distinguées des autres données relevant des autres finalités à L'acte ayant autorisé le traitement de données à finalités mixtes doit s'appuyer sur l'article 23 du règlement (permettant une diminution de la portée des droits sous conditions, celle-ci devant être précise) afin de déterminer un régime des droits cohérent pour l'ensemble des données traitées pour les diverses finalités. Le cas échéant, la CNIL invite le ministère à garder des modalités d'exercice des droits aussi simples et unifiées que possible.

5.5 Aucune finalité

Le principe de finalité signifie que, pour être licite, un traitement de données à caractère personnel doit être assorti d'une finalité. La collecte de données à caractère personnel, pour être mise en œuvre, doit être justifiée par la poursuite d'un but déterminé.

La difficulté se pose notamment lorsqu'il n'est pas possible d'identifier clairement la finalité du traitement lors de la phase de développement.

6. Degré de proximité de l'outil d'IA avec la décision judiciaire

Le règlement européen sur l'intelligence artificielle (RIA) est entré en vigueur le 1er août 2024. Il vise à favoriser un développement et un déploiement responsables de l'intelligence artificielle dans l'UE.

Le ministère de la Justice peut être concerné par le RIA, soit en tant que fournisseur[24] situé dans l'UE

[20] Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978

[21] Avis du Conseil d'Etat sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[22] Note_analyse_BIL_traitements_mixtes.pdf

[23] Avis du Conseil d'Etat - Protection des données personnelles 13.12.2017.pdf

[24] Fournisseur : personne physique ou morale ou tout organisme qui développe ou fait développer un dispositif d'IA à usage général et le met sur le marché ou en service, à titre onéreux ou gratuit.

mettant en service des systèmes d'IA lorsqu'il met à la disposition de ses agents un outil d'IA développé en interne, soit en tant que déployeur[25] situé au sein de l'UE, lorsqu'il met à la disposition de ses agents un outil d'IA développé au sein du secteur privé.

Le RIA s'applique aux « systèmes d'IA[26] », notion large qui permet ainsi d'appliquer le RIA à de nombreuses applications d'IA.

Le règlement classe les IA selon leurs niveaux de risques et détermine quatre niveaux de risque :

- Risque inacceptable : SIA présentant des risques inacceptables, interdits.
- Risque élevé : il s'agit des SIA énumérés à l'annexe III du RIA et soumis à des exigences renforcées (dont les **systèmes concourant à « l'administration de la justice »**).
- Risque limité : il s'agit des SIA définis par la Commission Européenne et soumis à des obligations de transparence spécifiques (ex : chatbots, IA créant du contenu généré automatiquement).
- Risque minime ou nul : IA librement utilisable (ex : assistants vocaux de base, etc.).

A noter que sont interdits les systèmes d'IA utilisés pour évaluer ou prédire le risque qu'une personne physique commette une infraction pénale, uniquement sur la base du profilage de cette personne ou de l'évaluation de ses traits de personnalité ou caractéristiques.

6.1 Système d'IA à haut risque

Selon l'article 6 du RIA, un SIA à haut risque est (notamment) un système qui figure dans la liste prévue à l'annexe III du règlement. En particulier, cette annexe identifie comme « à haut risque » **les systèmes concourant à « l'administration de la Justice »**, lorsqu'ils aident l'autorité judiciaire à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits (art 6§2 et annexe III, point 8a).
Mais de tels systèmes peuvent ne pas être classés dans la catégorie « haut risque » s'ils ne présentent pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, et s'ils se contentent de :

- Améliorer le résultat d'une activité humaine préalablement réalisée ;
- Exécuter une tâche procédurale étroite ;
- Détecter des constantes en matière de prise de décision ;
- Exécuter une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'usage visés à l'annexe III.

Il peut s'agir de SIA de recherche dans des documents et de synthèse de dossier ou d'outils IA permettant la pré-orientation des cas au sein des tribunaux et la recherche assistée.

A noter que le considérant 61 donne des indices d'interprétation de l'article 6 : certains SIA destinés à être utilisés pour l'administration de la justice devraient être classés comme étant à haut risque du fait de leur incidence potentiellement significative sur la démocratie, l'état de droit, les libertés individuelles, et le droit à un recours effectif et à accéder à un tribunal impartial.

[25] Déployeur : personne physique ou morale ou tout organisme qui utilise sous sa propre autorité un système d'IA, dans le cadre d'une activité à caractère professionnel.
[26] SIA qu'il définit comme « un système automatisé conçu pour fonctionner à différents niveaux d'autonomie, qui peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des résultats, tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels ».

Les SIA destinés à être utilisés par des organismes de règlement extrajudiciaire des litiges à ces fins devraient également être considérés comme étant à haut risque lorsque les résultats de procédures de règlement extrajudiciaire produisent des effets juridiques pour les parties. En matière répressive notamment, sont à haut risque les SIA qui concernent les victimes d'infractions pénales, les détecteurs de mensonge, ou les SIA permettant d'évaluer la fiabilité des preuves ou de prévenir des risques de récidive.

Les systèmes d'IA à haut risque doivent respecter un ensemble de mesures strictes. Cependant, à l'heure actuelle, les livrables précis n'ont pas encore été détaillés. Ils devraient l'être dans les lignes directrices à venir :

- **Gestion des risques** (art. 9) : analyse de l'impact sur les droits fondamentaux et mise en place d'un système de gestion des risques tout au long du cycle de vie du SIA.
- **Gouvernance des données** (art. 10) : les données utilisées pour l'entraînement, la validation et le test de l'IA doivent être pertinentes, représentatives, et aussi exemptes d'erreurs que possible.
- **Documentation technique** (art. 11) : création d'une documentation complète pour prouver la conformité et fournir aux autorités les informations nécessaires à l'évaluation de cette conformité (notamment, conserver les journaux générés par le SIA pendant au moins 6 mois)
- **Enregistrement automatique** (art. 12) : les SIA à haut risque doivent être conçus pour enregistrer automatiquement les événements pertinents pour l'identification des risques au niveau national et les modifications substantielles.
- **Transparence et instructions d'utilisation** (art. 13) : les fournisseurs doivent fournir des instructions d'utilisation aux utilisateurs en aval pour leur permettre de comprendre le système, ses risques et de se conformer à la réglementation, et informer les représentants du personnel mais aussi les personnes faisant l'objet des décisions prises à l'aide du SIA.
- **Surveillance humaine** (art. 14) : les systèmes doivent être conçus pour permettre une surveillance humaine efficace et garantir que les décisions automatisées peuvent être contrôlées et corrigées si nécessaire.
- **Précision et cybersécurité** (art. 15) : les systèmes doivent être suffisamment robustes et sécurisés pour résister aux risques de cybersécurité et fonctionner avec un niveau de précision adéquat.
- **Gestion de la qualité** (art. 17) : mise en place d'un système de gestion de la qualité pour garantir la conformité.
- **Enregistrement et accessibilité des informations** (art. 71) : les SIA à haut risque doivent être enregistrés dans une base de données de l'UE, avec les informations détaillées aisément accessibles par le public et lisibles par machine, sauf exceptions spécifiées pour certaines informations restreintes aux autorités de surveillance, à moins que le fournisseur ne donne son consentement pour que ces informations soient accessibles.

En amont de la mise en service ou sur le marché du SIA, le fournisseur doit faire la démonstration du respect de ces exigences au travers d'une **procédure d'évaluation de la conformité** (art. 16 et 43) avant de déposer une **déclaration de conformité** (art. 47).

Cette mise en conformité doit être assurée par toute **mesure technique et organisationnelle** permettant d'utiliser le SIA conformément aux instructions d'utilisation (art. 26).

Lorsque l'utilisateur est une administration publique, il doit enregistrer son SIA dans la base de données européennes et produire une évaluation des impacts du SIA sur les droits fondamentaux (art. 27) préalablement à sa première utilisation.

6.2 Les SIA à usage général

Il existe des **SIA dits « à usage général ».** Ils reposent sur des modèles d'IA présentant une généralité significative, c'est-à-dire qui possèdent la **capacité de répondre à un large éventail de tâche distinctes**. Ils sont généralement entraînés à l'aide d'un grand nombre de données, souvent en utilisant des méthodes d'auto-supervision à grande échelle et peuvent être intégrés dans une variété de systèmes ou d'applications en aval. Ces SIA peuvent, pour certains, présenter un risque systémique qui les soumettra à des obligations supplémentaires. Tel sera le cas lorsque ces systèmes :

- Disposent de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence ;
- Sont désignés comme tels sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique parce qu'ils possèdent des capacités ou un impact équivalent à ceux énoncés aux précédents.

Sous réserve des compléments apportés par les lignes directrices de la Commission européenne, on pourrait considérer que la mise en place d'un « ChatGPT Justice » au sein du ministère à partir de modèles Open Source entrerait dans cette catégorie.

Sur les IA à usage général, les fournisseurs sont concernés par des obligations. Ils doivent :

- **Elaborer et tenir à jour une documentation technique** détaillant le processus d'entraînement et d'évaluation des modèles d'IA. Cette documentation doit être fournie sur demande au Bureau de l'IA et aux autorités nationales compétentes.
- **Fournir des informations et une documentation aux fournisseurs de systèmes d'IA** intégrant leurs modèles, permettant une bonne compréhension des capacités et limites des modèles et facilitant la conformité réglementaire.
- **Mettre en place une politique pour respecter les droits d'auteur et droits voisins**, notamment en identifiant et respectant les réservations de droits exprimées.
- **Mettre à disposition du public un résumé détaillé des données utilisées pour entraîner les modèles** conformément à un modèle fourni par le Bureau de l'IA.
- **Coopérer avec la Commission** et les autorités nationales dans l'exercice de leurs compétences.
- Respecter la législation de l'Union sur le droit d'auteur et les droits voisins.

Lorsque les SIA à usage général présentent un **risque systémique**, les fournisseurs doivent :

- **Effectuer des évaluations des modèles d'IA** en utilisant des protocoles et outils normalisés, y compris des essais contradictoires, pour identifier et atténuer les risques systémiques, y compris les risques systémiques potentiels au niveau de l'Union.
- **Mettre en place des politiques de gestion des risques**, y compris des processus de responsabilité et de gouvernance.
- **Suivre, documenter et communiquer** rapidement au Bureau de l'IA et aux autorités nationales compétentes les incidents graves et les mesures correctives prises.
- **Garantir un niveau approprié de protection en matière de cybersécurité** pour les modèles d'IA et leur infrastructure physique.

Comme mentionné précédemment, les obligations des fournisseurs ne s'appliquent pas aux modèles d'IA publiés sous licence libre et ouverte, sauf s'ils sont considérés comme présentant un risque systémique. Les déployeurs de ces systèmes d'IA à usage général ne sont, en l'état du règlement sur l'IA, pas concernés par des obligations particulières.

6.3 Les SIA à risque limité

Un SIA sera considéré comme n'étant pas à haut risque s'il est **supervisé par l'être humain**, sans risque de préjudice pour les droits fondamentaux et sans incidence significative sur la prise de décision. Sont donc classés comme système d'IA à risque minime ceux :

- Améliorant le résultat d'une activité humaine préalablement réalisée
- Permettant de réaliser tâche procédurale étroite
- Détectant des constantes en matière de prise de décision
- Exécutant une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'usage visés à l'annexe III

Le considérant 61 précise que les SIA n'étant pas à haut risque dans le domaine de la Justice sont ceux qui sont **utilisés pour des activités administratives purement accessoires et qui n'ont aucune incidence sur l'administration réelle de la justice dans des cas individuels**.

On peut par exemple classer dans cette catégorie les IA permettant :

- L'anonymisation ou la pseudonymisation de décisions, de documents ou de données
- La communication entre membres du personnel
- Le tri et la pré-rédaction des mails
- La retranscription de réunions ou d'audiences
- La traduction
- La répartition des affaires au sein des chambres d'un tribunal ou des détenus dans des cellules
- La détection des incohérences dans les dossiers
- De transformer des données non structurées en données structurées, classer des documents par catégories ou détecter des doublons
- De traiter des fichiers via diverses fonctions telles que l'indexation, la recherche, le traitement de texte et le traitement de la parole ou en reliant des données à d'autres sources de données

En ce qui concerne les SIA n'étant pas considérés comme « à haut risque », les fournisseurs sont concernés par diverses obligations de transparence.

Ainsi les fournisseurs doivent :

- **Concevoir les SIA de manière à informer les utilisateurs** qu'ils interagissent avec une IA, sauf si cela est évident pour une personne normalement informée
- **Marquer les contenus générés ou manipulés par l'IA** (audio, image, vidéo, texte) dans un format lisible par machine. Les solutions techniques doivent être efficaces, interopérables, solides et fiables.

Les informations fournies par les fournisseurs doivent l'être de manière claire et reconnaissable au plus tard au moment de la première interaction ou exposition, et doivent être conformes aux exigences d'accessibilité.

7. Hébergement des données

7.2 Hébergement des données d'utilisation ou d'entraînement

Selon la **doctrine « cloud au centre »,** les données judiciaires sont des données d'une particulière sensibilité, relevant du secret protégé par la loi et d'applications métiers relatives aux agents publics de l'État.

Ainsi, la doctrine Cloud au centre s'applique aux :

- Données relevant de secrets protégés par la loi
- Données nécessaires à l'accomplissement des missions essentielles de l'Etat
- Données judiciaires.

S'agissant des autres données, il n'existe pas de restriction concernant l'hébergement.

Ainsi, les services cloud utilisés pour l'hébergement et le traitement des données judiciaires relèvent de la **catégorie des infrastructures critiques** en raison des obligations de confidentialité et de protection des informations traitées. La qualification SecNumCloud[27] ou une certification équivalente au niveau européen est donc requise pour assurer la conformité aux exigences de cybersécurité et de souveraineté numérique.

L'utilisation d'un service cloud par les juridictions et le ministère de la Justice est encadrée par plusieurs principes :

- **Souveraineté et cybersécurité** : Conformément à la doctrine « cloud au centre », seules les offres qualifiées SecNumCloud ou disposant d'une certification équivalente peuvent être utilisées dès lors que des données de procédure sont traitées.
- **Protection du secret judiciaire** : Les données judiciaires doivent être hébergées sur des infrastructures garantissant leur inaccessibilité à toute autorité étrangère, ce qui est assuré par la qualification SecNumCloud.
- **Encadrement contractuel strict** : Les contrats liant l'administration judiciaire aux prestataires cloud doivent intégrer des exigences spécifiques en matière de cybersécurité, d'auditabilité et de réversibilité.
- **Réversibilité** : Les administrations doivent s'assurer que les solutions cloud choisies permettent une réversibilité soutenable, c'est-à-dire la possibilité de changer de fournisseur sans perte de données ou de fonctionnalités. Cela est essentiel pour garantir la continuité des procédures juridiques.

[27] SecNumCloud : Parmi ces offres de cloud commercial, certaines peuvent être qualifiées de SecNumCloud. Il s'agit d'une qualification délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) garantissant un niveau élevé de cybersécurité pour les services cloud. Un cloud commercial doit respecter cette qualification (ou une certification européenne équivalente) et être immunisé contre tout accès non autorisé par des autorités publiques d'un État tiers ([R9] de la doctrine). Élaboré par l'ANSSI, le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique. D'une part, les prestataires proposant une offre d'informatique en nuage (cloud) doivent présenter une bonne hygiène informatique, d'autre part, les données doivent être protégées en conformité avec le droit européen. Les exigences du référentiel garantissent la protection du service cloud vis-à-vis du droit extra-européen, grâce à la combinaison de trois types de mesures : techniques : étanchéité des systèmes d'information ; opérationnelles : seul le prestataire peut intervenir sur les ressources supportant le service et juridiques : application exclusive du droit européen.

- **Portabilité** : La portabilité multi-clouds doit être assurée pour éviter toute dépendance à un fournisseur unique. L'adéquation avec les règles de GAIA-X, notamment d'interopérabilité et de portabilité, devra également être recherchée dans la mesure du possible.

Cette doctrine a été confortée par les dispositions de l'article 31 de la loi n° 2024-449 visant à sécuriser et à réguler l'espace numérique (dite SREN), lesquelles imposent une obligation de protection des données stratégiques et sensibles sur le marché de l'informatique en nuage. Les autorités publiques qui ont recours à un prestataire privé pour une solution cloud ont une obligation légale de vérification de la sécurité de la solution cloud retenue pour l'hébergement des données sensibles, qui se traduit, en pratique, par le contrôle du fournisseur de services d'informatique en nuage quant au respect de cette nouvelle obligation. Cette obligation serait applicable à l'Etat dès lors que les données traitées dans le cadre d'un SIA dans le domaine justice seraient hébergées dans un cloud fourni par un prestataire privé dans la très grande majorité des informations qui seront traitées par une SIA seront qualifiées de sensibles au sens de cette disposition.

Le RGPD (article 48) interdit également de répondre aux requêtes d'autorités de pays tiers en leur transférant directement des données sans passer par mécanismes de transferts assurant un niveau suffisant de protection des données, en particulier des accords internationaux pour rendre exécutoires ces décisions. Il s'agit ici d'interdire les demandes d'accès directes auprès des opérateurs détenant des données en Europe dans le champ du RGPD. Cette disposition commande ainsi d'être vigilant dans le cadre du recours à des opérateurs (sous-traitants en particulier) qui seraient soumis à des législations étrangères qui pourraient leur imposer de répondre à ces demandes (cas des Etats-Unis par exemple, avec le cloud act, ou de la Chine).

En conclusion, l'application de ces dispositions au secteur judiciaire impose un cadre de sécurité et de souveraineté strict, garantissant la protection des données judiciaires contre toute ingérence non autorisée.

7.3 Transferts de données

S'agissant du transfert de données, le principe institué par le RGPD est que les données doivent continuer à bénéficier d'une protection substantiellement équivalente à celle offerte par ce texte. Il établit deux régimes :

- Ceux fondés sur une **décision d'adéquation** (RGPD, art. 45) : elle est prise sur la base d'un examen global de la législation en vigueur dans un Etat, sur un territoire ou applicable à un ou plusieurs secteurs déterminés au sein de cet Etat ;
- Ceux fondés sur des **garanties appropriées** (RGPD, art. 46) : décisions des autorités de contrôle et qui sont prises à la lumière des engagements des organismes concernés, ou accords internationaux présentant des garanties de protection des données suffisantes.

A ces deux régimes s'ajoutent des **dérogations pour des situations particulières** (RGPD, art. 49) : consentement explicite de la personne concernée, transfert nécessaire à l'exécution d'un contrat, pour des motifs importants d'intérêt public ou à la **constatation, à l'exercice ou à la défense de droits en justice.**

Pour les traitements dits de Police-Justice, ont été transposé à l'article 112 et suivants de la LIL, les articles 35, 36 et 37 de la directive, applicables aux échanges de données avec les **autorités homologues** des autorités compétentes en France pour la prévention ou la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanction pénale.

Le responsable de traitement de données à caractère personnel relevant de la directive, ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées (LIL, art. 112) :

- Le transfert des données est nécessaire à l'une des finalités ;
- Les données sont transférées à une autorité étrangère compétente, chargée des mêmes finalités ;
- Si les données à caractère personnel proviennent d'un autre Etat, l'Etat qui a transmis ces données a préalablement autorisé ce transfert conformément à son droit national (sauf si cette nouvelle transmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre Etat ou pour la sauvegarde des intérêts essentiels de la France) ;
- La commission européenne a adopté une décision d'adéquation ou un instrument juridiquement contraignant qui fournit des garanties appropriées en ce qui concerne la protection des données à caractère personnel ou, en l'absence d'une telle décision et d'un tel instrument, le responsable de traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées (garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet Etat hors Union européenne, ou dispositions juridiquement contraignantes exigées à l'occasion de l'échange de données).
-

Si le responsable de traitement, autre qu'une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles transfère des données à caractère personnel sur le seul fondement de l'existence de garanties appropriées au regard de la protection des données à caractère personnel, il doit en aviser la CNIL.

Par exception, le responsable de traitement de données à caractère personnel ne peut, en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire (LIL, art. 113) :

- À la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre ;
- À la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit (et en informant la CNIL) ;
- Si le responsale n'estime pas que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public :
- Pour prévenir une menace grave et immédiate pour la sécurité publique d'un Etat ;
- Dans des cas particuliers, à l'une des finalités des traitements relevant de la directive ;
- Dans un cas particulier, **à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins.**

Enfin, l'article 114 précise que l'autorité compétente peut dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un Etat n'appartenant pas à l'Union européenne lorsque les autres dispositions de la présente loi applicables aux traitements concernés sont respectées et si, avec information de la CNIL :

- Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données pour l'une des finalités ;
- L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public rendant nécessaire le transfert dans le cas considéré ;
- L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre État est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ;

- L'autorité compétente de l'autre État est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ;
- L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités pour lesquelles les données à caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire.

Outre les dispositions relatives aux transferts, la **coopération internationale** entre autorités de contrôle est envisagée tant par le RGPD que par la loi française.

Le RGPD évoque également plus largement la nécessité de mécanismes de coopération internationale dans le domaine de la protection des données à caractère personnel. Dans la loi française, ces mécanismes sont exprimés à travers les dispositions relatives à la coopération (art. 24 à 29) et à travers celles relatives aux suspensions des transferts (art. 39).

7.4 Communication du code source

En application de la loi n°2016-1321 pour une République numérique, en matière d'accès aux algorithmes, **les codes sources, fichiers, documentation achevée relative au système ou qui pourraient être utilisés par un SIA** sont inscrits sur la liste des **documents administratifs communicables** de l'article L. 300-2 du CRPA (il s'agit en effet de documents produits ou reçus, dans le cadre de leur mission de service public, par l'État, ou personnes de droit privé chargées d'une telle mission.).

Néanmoins, ne sont pas communicables les **documents administratifs dont la consultation ou la communication porterait atteinte** (CRPA, art. L311-5) **:**

- f) Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;

- g) A la recherche et à la prévention, par les services compétents, d'infractions de toute nature ;

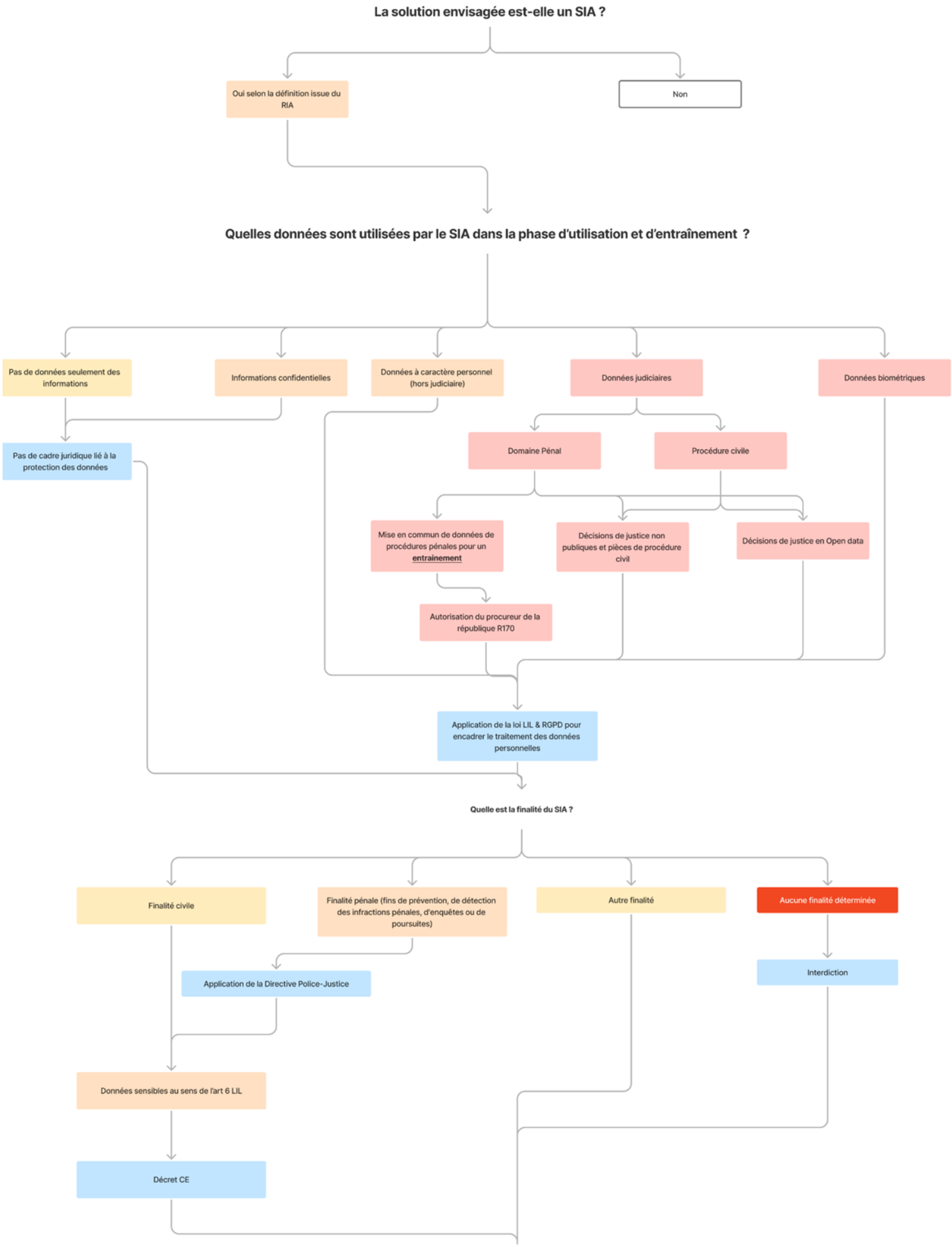
A priori la c**ommunication d'un code source n'est pas en lui-même de nature à porter atteinte à ces objectifs,** il s'en suit que ces exceptions ne pourraient pas être invoquées pour faire obstacle à la communication du code source.

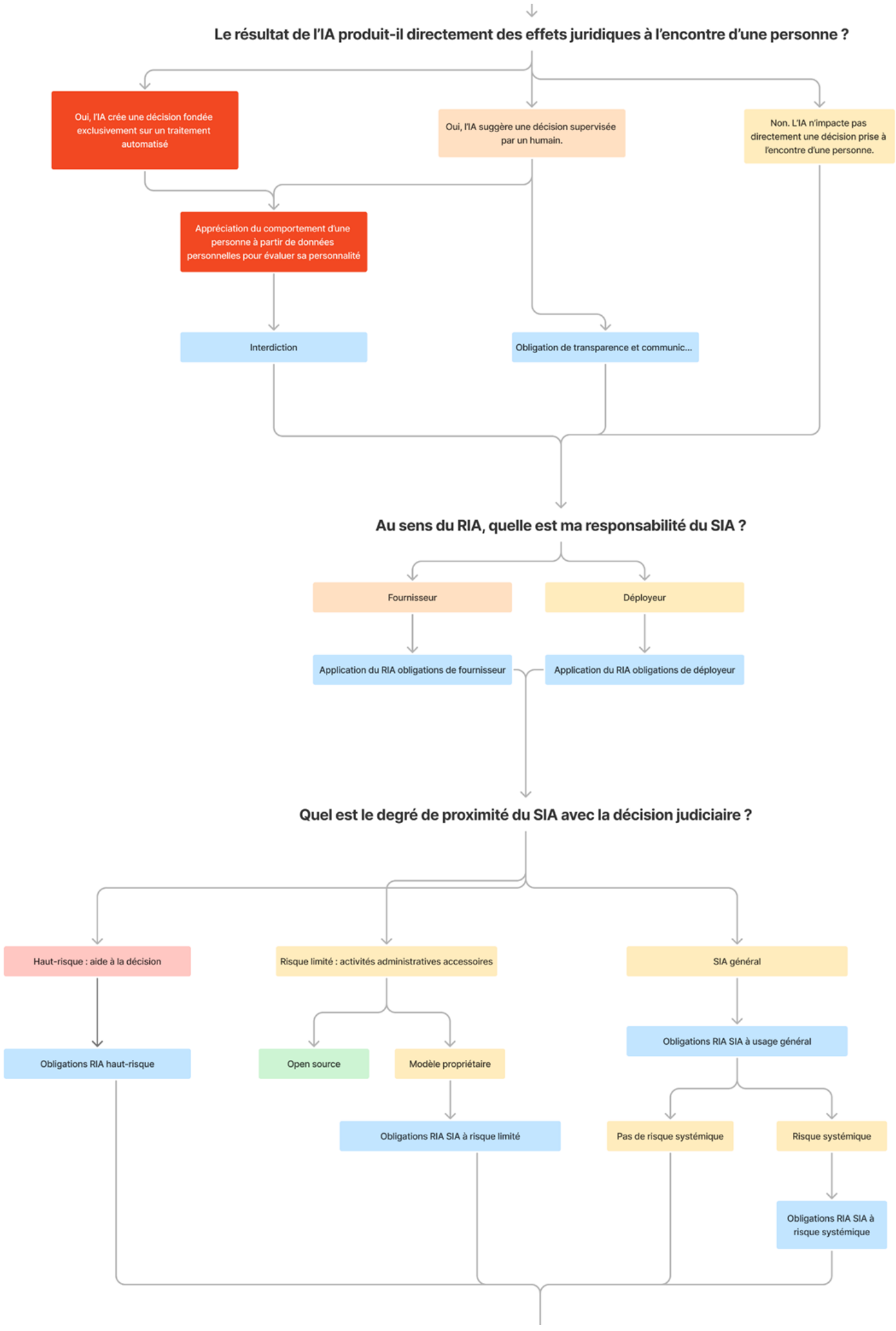
De même, en application de l'article L311-6 du CRPA, **la communication du document ne peut être faite qu'à l'intéressé si la communication porte atteinte à certains droits protégés**[28] : il en va ainsi par exemple (i) des documents contenant des données à caractère personnel utilisés pour l'entraînement de la SIA (par exemple jugements), (ii) des codes-sources s'il apparaît possible, par rétro-ingénierie, de retrouver ces données ou (iii) de l'algorithme qui aurait été développé par une entreprise privée pour les besoins de la SIA et qui pourrait relever du secret des affaires

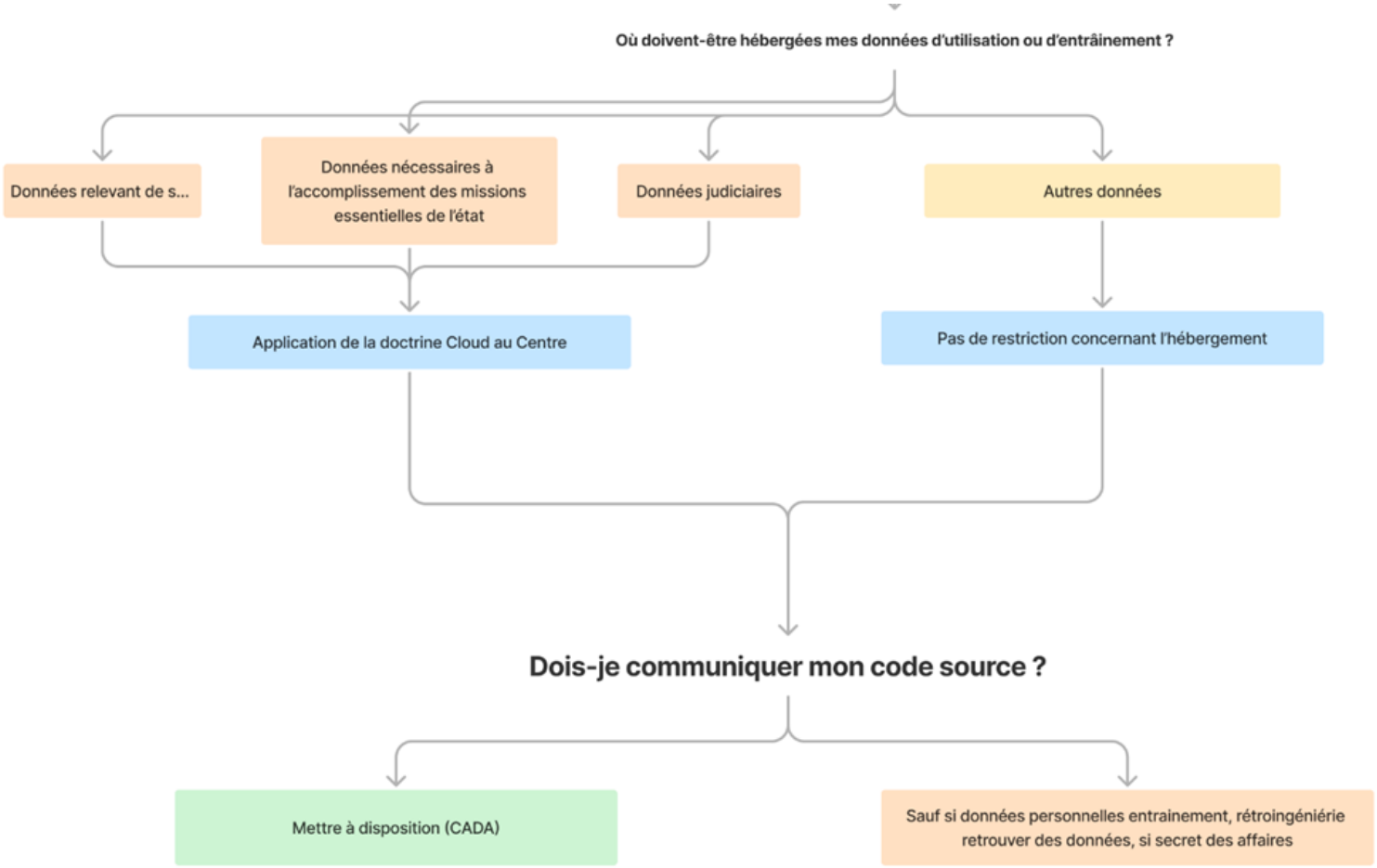
En tout état de cause la communication est **effectuée dans les conditions prévues par le CRPA** (art. L311-1 et s.) doit respecter les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (protection des données personnelles).

[28] Protection de la vie privée, secret médical, secret des affaires, ou si le document porte une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ou fait apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

Arbre décisionnel juridique




Le résultat de l'IA produit-il directement des effets juridiques à l'encontre d'une personne ?
Oui, l'IA crée une décision fondée exclusivement sur un traitement automatisé
Oui, l'IA suggère une décision supervisée par un humain.
Non. L'IA n'impacte pas directement une décision prise à l'encontre d'une personne.
Appréciation du comportement d'une personne à partir de données personnelles pour évaluer sa personnalité
Interdiction
Obligation de transparence et communic...
Au sens du RIA, quelle est ma responsabilité du SIA ?
Fournisseur
Déployeur
Application du RIA obligations de fournisseur
Application du RIA obligations de déployeur
Quel est le degré de proximité du SIA avec la décision judiciaire ?
Haut-risque : aide à la décision
Risque limité : activités administratives accessoires
SIA général
Obligations RIA haut-risque
Open source
Modèle propriétaire
Obligations RIA SIA à usage général
Obligations RIA SIA à risque limité
Pas de risque systémique
Risque systémique
Obligations RIA SIA à risque systémique


Où doivent-être hébergées mes données d'utilisation ou d'entrâinement ?
Données relevant de s...
Données nécessaires à l'accomplissement des missions essentielles de l'état
Données judiciaires
Autres données
Application de la doctrine Cloud au Centre
Pas de restriction concernant l'hébergement
Dois-je communiquer mon code source ?
Mettre à disposition (CADA)
Sauf si données personnelles entrainement, rétroingéniérie retrouver des données, si secret des affaires

ANNEXE N°2

Labellisation et certification des systèmes d'IA dans le secteur de la justice

SYNTHESE

La labellisation et la certification des systèmes d'IA en justice apparaissent comme des outils indispensables pour concilier l'innovation technologique avec les impératifs d'un État de droit. L'intégration d'IA dans la chaîne judiciaire nécessite un climat de confiance autour de ces systèmes.

Cela passe par des actions concrètes, graduées dans le temps, que le ministère de la justice peut entreprendre sans tarder. Dès aujourd'hui, la rédaction d'un référentiel provisoire expérimental à destination des concepteurs et la diffusion d'une charte aux utilisateurs permettraient d'installer les bases d'une future gouvernance. La mise en place d'un « bac à sable » réglementaire permettrait d'accompagner les expérimentations en cours.

À moyen terme, la structuration d'un organisme certificateur national et la définition de normes claires donneront aux acteurs (éditeurs, juridictions, justiciables) une visibilité sur les normes et une sécurité juridique.

À plus long terme, l'objectif est d'inscrire durablement ces procédures dans le fonctionnement quotidien de la justice, comme gage de qualité, de transparence et de respect des droits fondamentaux.

Des pistes concrètes existent déjà pour y parvenir : s'appuyer sur les référentiels éprouvés (comme ceux de la CEPEJ), exploiter le retour d'expérience d'initiatives internationales ou encore mutualiser les efforts au niveau européen pour éviter de dupliquer les évaluations.

En empruntant cette voie, la France pourrait être le premier État européen à mettre en place un label « IA digne de confiance en justice » (IADCJ), devenant un standard de fait. Cela fournirait aux décideurs publics un outil d'aide pour sélectionner les solutions technologiques les plus sûres, et aux citoyens une assurance que les systèmes d'IA (SIA) employés par la justice sont sous contrôle et améliorent le service public de la justice, sans laisser s'installer des narrations sur la dégradation des droits ou l'automatisation excessive de l'institution.

Il est également indispensable d'accompagner cette démarche d'un examen technique minutieux. Cela permettra de s'assurer que les solutions choisies respectent la souveraineté et protègent efficacement les données, notamment lorsqu'il s'agit d'informations sensibles du domaine judiciaire. Concrètement, il faut vérifier que les systèmes d'intelligence artificielle répondent aux exigences de sécurité et de confidentialité lorsque c'est nécessaire. Cette dimension technique, rendue impérative par la Loi, joue également un rôle clé pour instaurer un climat de confiance, aussi bien auprès des professionnels que du grand public.

INTRODUCTION

La présente note, établie dans le cadre de la mission attribuée à M. Haffide Boulakras sur l'accélération de la mise en œuvre de l'intelligence artificielle au sein des services du ministère de la justice (février-mai 2025), a pour objectif de présenter les enjeux et méthodes de dispositifs de labellisation et de certification de systèmes d'IA (SIA) dans le secteur de la justice.

Après avoir distingué la labellisation de la certification (1), il sera traité du cadre réglementaire et des acteurs compétents en matière de certification et de labellisation de SIA (2). Sur cette base, une méthode permettant de qualifier entre les différents SIA les besoins de certification ou de labellisation (3) sera proposée et quelques points d'attention identifiés (4). Cette note sera conclue par des propositions court, moyen et long terme de plan d'action pour un dispositif national de labellisation et de certification de systèmes d'IA dans le domaine de la justice (5).

1. Distinction de la labellisation et de la certification dans le contexte de systèmes d'intelligence artificielle

Dans le domaine des technologies, labellisation et certification désignent deux démarches de confiance distinctes et complémentaires.

Un **label** est une marque ou une attestation attribuée à un produit ou service pour signaler sa conformité à certains standards ou valeurs définis par un organisme (public ou privé) ou des consortiums (associations d'acteurs d'un secteur, pouvant mélanger public et privé). Il vise à valoriser le produit en informant les utilisateurs de ses caractéristiques de qualité spécifiques, et sa délivrance implique un contrôle effectué, le plus souvent, par l'organisme producteur du label. Dans le contexte de l'intelligence artificielle (IA), des labels sont déjà décernés par des organisations ou des associations[1] et traduisent le respect par les concepteurs d'un certain nombre de principes (transparence, équité, non-discrimination, etc.). Ces labels restent en général facultatifs et indicatifs, sur une base volontaire, avec l'ambition d'être un gage de confiance tant pour les utilisateurs que pour les décideurs.

Une **certification** est une procédure plus formelle par laquelle un organisme tiers du producteur de la norme, indépendant et accrédité, valide la conformité d'un produit, service ou système à des standards officiels. La certification implique un audit particulièrement rigoureux selon un référentiel précis, le plus souvent issu de standards élaborés par des organismes spécialisés (comme l'ISO, l'IEEE, le CEN-CENELEC ou l'AFNOR). Si les exigences sont satisfaites, une attestation de conformité est alors délivrée par l'organisme certificateur. Les certifications sont en général reconnues par l'État et offrent une garantie plus solide sur le plan juridique. Appliquée aux SIA, la certification vise à assurer que les systèmes respectent des critères techniques, juridiques et éthiques spécifiques (par exemple, absence de biais discriminants au-delà d'un certain seuil, robustesse en cybersécurité, respect de la vie privée, etc.).

En résumé

Dans le secteur de la justice, labelliser un système d'IA reviendrait à lui attribuer une marque pour sa conformité à des principes prédéfinis, de valeur variable selon le producteur de ces principes, tandis que le certifier impliquerait de le soumettre à un examen par un organisme officiel tiers, aboutissant à une autorisation ou une homologation attestant sa conformité aux normes légales en vigueur (le RIA à compter du 2 août 2026).

[1] V. 2.3, avec les initiatives LabelIA ou encore Positive AI

2. Cadre réglementaire et acteurs compétents en matière de certification et de labellisation de systèmes d'IA

2.1. Cadre réglementaire

Pour mémoire

Dans le domaine de la justice, les SIA qui devront être obligatoirement certifiés sur le fondement du RIA sont ceux qui seront employés pour aider à rechercher ou interpréter les faits et le droit, ou à appliquer la loi à un cas concret.

Pour l'ensemble des 27 États membres de l'Union européenne, le règlement sur l'intelligence artificielle (RIA ou AI Act), adopté en juin 2024, instaure une approche fondée sur l'appréciation du niveau de risque présenté par les SIA. Ce règlement classe les SIA en quatre catégories : inacceptables (interdits car portant atteinte aux droits fondamentaux, par ex. la notation sociale), à haut risque, à risque limité exigeant une obligation de transparence et l'ensemble des autres, présentant un risque minimal.

Les SIA « à haut risque » – c'est-à-dire ceux susceptibles d'avoir un impact significatif sur la vie des personnes, notamment dans des domaines sensibles comme la santé, l'éducation, l'emploi ou la justice – feront l'objet d'obligations strictes de conformité avant leur mise sur le marché et leur déploiement à partir du 2 août 2026[2]. Parmi ces obligations figurent une évaluation de conformité préalable (similaire à un contrôle technique, conduisant à un marquage « CE »), la constitution d'une documentation technique détaillée, la gestion des risques tout au long du cycle de vie, la transparence vis-à-vis des utilisateurs, ou encore une supervision humaine appropriée. Le règlement annexe une liste des usages d'IA classés comme « à haut risque » (annexe III) : à ce titre, les SIA destinés à être utilisés par les autorités judiciaires pour aider à rechercher ou interpréter les faits et le droit, ou à appliquer la loi à un cas concret (par exemple des outils d'aide à la décision judiciaire) paraissent explicitement dans la catégorie des IA à haut risque[3].

Ces obligations ont été édictées afin de créer un cadre de confiance pour des applications dans des domaines aussi sensibles que la justice. La certification de ces systèmes avant leur mise en service ambitionne de garantir, notamment, le respect des droits fondamentaux (non-discrimination, droit à un procès équitable, etc.). Notons que le RIA prévoit également des codes de conduite volontaires pour les SIA présentant moins de risques et un mécanisme de gouvernance à deux niveaux : un conseil européen de l'IA (*European AI Board*), assisté d'un bureau de l'IA (*AI Office*), chargé d'harmoniser les pratiques entre États membres et, dans chaque pays, une ou plusieurs autorités nationales compétentes désignées pour surveiller l'application du règlement.

Le RIA laisse aux États une large marge d'appréciation quant au choix de cette autorité nationale, sous réserve que certaines autorités sectorielles existantes conservent leur rôle de surveillance pour les SIA déjà régulés dans leur domaine (par ex. l'Agence du médicament pour les dispositifs médicaux d'IA).

A titre comparatif, dans le monde, d'autres types dispositifs de contrôle des algorithmes ont déjà vu le jour. Le Canada a mis en place dès 2019 un outil d'évaluation de l'incidence algorithmique (EIA) applicable à tout système automatisé de décision au sein de l'administration fédérale[4]. Cet outil consiste en un questionnaire normalisé d'environ 51 questions de risque et 34 questions destinées à limiter ces risques,

[2] Des délais supplémentaires pourraient être accordés aux autorités publiques opérateurs de SIA ayant déployé des systèmes avant le 2 août 2026, portant au 2 août 2030 la mise en conformité (art.111.2).

[3] L'interprétation de l'annexe III du point 8 du RIA parait, d'après une rencontre réalisée avec la Commission européenne (DG CONNECT), conduire vers de critères cumulatifs limitant le classement à haut risque de seuls systèmes présentant tous les critères. Il faudra attendre la publication lignes directrices relatives à l'application des art.6 et s. du RIA (systèmes à haut risque), disponibles fin 2025 – début 2026, pour confirmer cette analyse.

[4] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/evaluation-incidence-algorithmique.html

permettant de déterminer un *niveau d'impact* du projet algorithmique et d'identifier les mesures à prendre avant son déploiement. L'EIA canadien, rendu obligatoire par une directive gouvernementale sur les prises de décisions automatisées, assure une forme de mise en conformité interne des projets d'IA publics avant leur utilisation, et favorise une culture de l'audit algorithmique systématique. Les Pays-Bas, quant à eux, ont créé une instance de supervision des algorithmes, indépendante, chargée de surveiller l'usage des IA par les pouvoirs publics et de recevoir les plaintes des citoyens en la matière[5].

2.2. Les organismes producteurs de standards techniques pour les systèmes d'intelligence artificielle

En résumé

L'ISO, l'IEEE, le CEN-CENELEC et l'AFNOR[6] jouent un rôle déterminant dans la production de standards techniques pour la mise en œuvre de SIA, en fournissant les socles techniques et méthodologiques qui permettront aux autorités françaises de certifier les systèmes d'IA de manière fiable, interopérable et conforme au droit européen. Le rôle du CEN-CENELEC est particulièrement central pour avoir reçu mandat de la Commission européenne afin d'établir des standards dans le contexte du RIA.

La mise en place d'un dispositif de certification efficient pour les SIA, notamment dans des domaines sensibles comme la justice, suppose de s'appuyer sur des standards techniques reconnus, définissant des critères objectifs de qualité, de sécurité, de fiabilité et d'éthique. Ces standards sont élaborés et diffusés par des organismes de normalisation, à différents niveaux :

2.2.1. Au niveau international : l'ISO et l'IEEE

L'Organisation internationale de normalisation (ISO) est un réseau mondial de normalisation regroupant 170 pays. Elle élabore des normes techniques volontaires applicables à des produits, des services ou des processus. En matière d'IA, l'ISO travaille en partenariat avec la Commission électrotechnique internationale (IEC) au sein du comité mixte JTC 1/SC 42, qui est dédié exclusivement à l'intelligence artificielle. Ce comité a élaboré des normes portant sur la terminologie de l'IA (ISO/IEC 22989), les cadres de gouvernance (ISO/IEC 38507) et le management (ISO/IEC 42001). Ces normes serviront de base aux référentiels de certification dans de nombreux pays, y compris la France.

L'IEEE (Institute of Electrical and Electronics Engineers), principalement implanté aux États-Unis mais de portée mondiale, produit aussi des standards dans le domaine des technologies numériques. L'initiative IEEE SA (Standards Association) a lancé en 2016 le programme « *Ethically Aligned Design* » pour guider la conception de systèmes d'IA respectueux des valeurs humaines. Elle publie notamment des guides et des standards sur la transparence algorithmique (IEEE 7001) ou la gouvernance des données (IEEE 7002). Ces standards sont déjà utilisés dans certaines démarches de labellisation de l'IA (notamment aux États-Unis ou dans des consortiums industriels).

2.2.2. Au niveau européen : le CEN-CENELEC

Au niveau de l'Union européenne, les organismes de normalisation sont le CEN (Comité européen de normalisation) et le CENELEC (Comité européen de normalisation électrotechnique). Ces deux entités coopèrent avec l'ISO/IEC, mais adaptent leurs travaux au contexte réglementaire européen. À la demande de la Commission européenne, le CEN-CENELEC travaille depuis 2021 à l'élaboration de normes harmonisées qui viendront soutenir la mise en œuvre du RIA. Ces normes définiront concrètement les exigences de transparence, de gestion des risques, d'auditabilité, de sécurité ou d'intervention humaine

[5] L. Bertuzzi, « Les Pays-Bas prennent les devants en matière de supervision des algorithmes », Euractiv, 15 novembre 2022, accessible sur : https://www.euractiv.fr/section/tech/news/les-pays-bas-prennent-les-devants-en-matiere-de-supervision-des-algorithmes/

[6] D'autres organismes comme le LNE (laboratoire national d'essai) ou le bureau Veritas sont concurrents de l'AFNOR pour opérer des missions de certification. Le LNE et le bureau Veritas ne sont toutefois pas producteurs de normes, alors que l'AFNOR détient la marque « NF ».

prévues par le règlement. Pour les SIA à haut risque, ces normes deviendront des référentiels de certification officiels dans l'Union européenne. Un système certifié conforme à une norme harmonisée bénéficiera d'une présomption de conformité juridique au RIA. Ces travaux sont coordonnés avec les agences européennes comme l'ENISA (cybersécurité) et le FRA (droits fondamentaux).

2.2.3. Au niveau national : l'AFNOR

En France, c'est l'AFNOR (Association française de normalisation) qui représente le pays dans les instances ISO, IEC et CEN-CENELEC. Elle anime les groupes d'experts nationaux participant à l'élaboration des normes d'IA, en lien avec des acteurs publics (ministères, CNIL), des chercheurs, des industriels et des associations. L'AFNOR a publié en 2021 une norme XP Z77-101 (Guide de bonnes pratiques en matière de gouvernance des démarches éthiques au sein des organisations)[7]. Elle participe également aux travaux du comité SC 42 de l'ISO. L'AFNOR joue déjà un rôle opérationnel dans le dispositif de certification de l'IA, en fournissant des référentiels reconnus et en assurant la cohérence avec les standards internationaux.

L'AFNOR est également titulaire de la marque collective de certification « NF ».

2.3. Les organismes producteurs de labels ou d'évaluation pour les systèmes d'intelligence artificielle

La production de labels pour les systèmes d'intelligence artificielle est plus difficile à circonscrire au vu de la profusion d'acteurs et d'intérêts, ne permettant pas toujours d'évaluer la réelle portée des engagements.

La France a vu émerger des initiatives privées comme le label LabelIA[8] qui atteste le respect par des développeurs de SIA à son référentiel cadre, ou encore l'initiative Positive AI lancée par plusieurs grandes entreprises pour évaluer la maturité des organisations et délivrer un label après un audit indépendant[9].

Sans constituer à proprement parler un label et spécifiquement pour la justice, la CEPEJ a adopté en 2018 une charte éthique d'utilisation de l'IA dans les systèmes judiciaires[10]. Son opérationnalisation est assurée au travers d'un bureau consultatif sur l'intelligence artificielle (AIAB)[11] et d'une procédure de vérification de conformité avec la charte éthique, en cours d'expérimentation[12]. La pertinence de la méthodologie reste à évaluer.

De manière plus sectorielle, une charte entre legaltechs et professions réglementées a réuni en 2017 près de 150 signataires[13]. Les notaires ont également développé une charte pour un développement éthique du numérique notarial[14].

Sans produire de label, le groupe de travail IA du CNB a également réalisé un benchmark de différentes solutions d'IA générative à destination des avocats, sur la base de différents critères (cas d'usage, type de modèle de langage, sécurité et confidentialité, déploiement, autres spécificités).

[7] Norme accessible sur : https://norminfo.afnor.org/norme/xp-z77-101/guide-de-bonnes-pratiques-en-matiere-de-gouvernance-des-demarches-ethiques-au-sein-des-organisations/192346
[8] Porté par l'association LabelIA Labs : https://www.labelia.org
[9] Porté par des opérateurs privés (BCG X, L'Oréal, Malakoff Humanis and Orange) et un comité d'experts académiques : https://positive.ai/the-ai-label
[10] Charte accessible sur : https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment
[11] Rôle et composition du bureau : https://www.coe.int/fr/web/cepej/ai-advisory-board
[12] La Cour de cassation a testé cette grille d'évaluation sur ses systèmes d'IA en exploitation.
[13] Liste des signataires : https://www.charteethique.legal/signataires/
[14] Charte : https://compte.idnot.fr/doc/charte-ethique

3. Besoins de labellisation ou de certification en fonction des cas d'application de l'IA dans le domaine de la justice : proposition de méthode

Le développement de SIA dans le domaine de la justice a vocation à s'accélérer en 2025 pour améliorer l'efficacité du service public et doter les agents d'outils de leur temps. Ces SIA ne présentent toutefois tous pas le même niveau d'enjeu et il convient de les hiérarchiser afin de ne pas faire peser de manière indistincte la même charge de mise en conformité.

Ainsi, il devrait être distingué les applications à faible enjeu décisionnel (soutien aux tâches administratives ou documentaires), pour lesquelles la question de la labellisation ou de la certification paraissent moins prégnantes que pour les applications à plus fort enjeu, contribuant plus ou moins directement à la prise de décision de justice ou à l'évaluation de personnes.

En outre, ces applications à plus fort enjeu peuvent elles-mêmes être hiérarchisées à leur tour, entre les applications pour lesquelles une certification sera probablement obligatoire (SIA d'aide à la prise de décision, art.6 et annexe III RIA et d'autres applications pour lesquelles une démarche *ex ante* de certification volontaire ou de labellisation ne sera juridiquement pas imposée, mais paraîtra opportune afin d'améliorer la confiance des utilisateurs et des usagers.

Une grille d'analyse pourrait être élaborée à partir des cas d'usage retenus par le COMOP, afin de bien distinguer le périmètre des applications pouvant faire l'objet d'une labellisation volontaire (provenant du ministère, d'acteurs du marché ou de tiers) de celui des applications qui devront faire l'objet d'une certification obligatoire. L'évaluation pourrait être réalisée par un collège d'experts et validée par le futur observatoire / comité stratégique.

La pertinence de la certification, notée de 1 à 5, serait à évaluer en fonction de l'intensité de la contrainte réglementaire et de l'opportunité de créer un cadre de confiance renforcé. La pertinence de la labellisation décroit si une certification existe déjà ou si l'application ne présente aucun enjeu particulier.

La pertinence de la labellisation augmente en revanche pour des applications dont l'enjeu est intermédiaire, afin d'améliorer le cadre de confiance sans pour autant mettre en œuvre de plus lourdes procédures.

Exemples de cas d'usage	**Criticité sur la prise de décision judiciaire**	**Pertinence de certification**	**Pertinence de labellisation**
Retranscription automatique	Faible	■□□□□	■■■■□
Moteur de recherche avancé	Faible	■■□□□	■■■■□
Interprétariat et traduction	Faible	■■□□□	■■■■□
Résumé et synthèse de dossier	Médian	■■□□□	■■■□□
Occultation de données personnelles	Faible	■□□□□	■■■□□
Aide à la rédaction	Important	■■■■□	■□□□□
Jurimétrie	Important	■■■■■	□□□□□
IA générative généraliste	Médian	■■■□□	■■■□□

Modèle de grille d'analyse distinguant les systèmes à certifier de ceux à labelliser

4. Points d'attention

Il sera énoncé ici une série de risques déjà identifiés : la stratégie de limitation de ces risques sera traitée dans la partie 5, relative à une proposition de plan d'action.

4.1. Les enjeux en termes de responsabilité

La mise en place de politiques de certification ou de labellisation conduit à des transferts de responsabilité. En effet, le respect d'une mise en conformité imposé par la loi (trouvant principalement sa source, dans le cas de l'intelligence artificielle, au sein du RIA) ou l'approbation d'un label par le ministère de la justice, qu'il soit public, privé ou mixte, conduira à une probable exonération de l'opérateur ou de l'utilisateur fautif.

Les conséquences juridiques sur une potentielle mise en jeu de la responsabilité de l'Etat et le déficit d'image sont donc à anticiper et expertiser, spécialement pour les labels, dont les fondements et procédures sont, par nature, plus souples que des politiques de certification, adossées à des ensembles réglementaires et des standards plus robustes.

4.2. Confusions des rôles

S'agissant de la certification obligatoire de certains SIA, le RIA organise une séparation explicite des responsabilités, comme dans d'autres domaines industriels dans lesquels des législations sur les produits sont déjà intervenues[15]. Les autorités désignées comme « organes notifiés » par le RIA (qui sont les organismes indépendants et accrédités pour évaluer la conformité d'un SIA) sont ainsi totalement distinctes des producteurs de la norme. En France, le LNE, le bureau Veritas ou l'AFNOR sont déjà notifiés dans d'autres domaines (médical, sécurité).

La production d'un label par l'administration centrale du ministère de la justice, appliqué à elle-même, aux juridictions et à ses services déconcentrés, conduit en revanche à une certaine confusion de rôles : à la fois producteur de principes, commanditaire et concepteur de systèmes, possible vérificateur de la conformité à ces principes et utilisateur de ces mêmes systèmes, les justifications à l'extérieur de l'administration de l'absence de conflit d'intérêts pourraient être délicates à produire.

Une telle confusion entre régulateur et opérateur nuit donc à l'indépendance de l'évaluation, affaiblit la crédibilité du processus de certification et expose à des contentieux en cas de litige. Elle contrevient en outre à un principe fondamental de bonne administration : la séparation des fonctions de conception, d'utilisation et de contrôle.

4.3. Risque d'homologation prématurée de technologies non matures

Le rattachement de la labellisation ou d'une certification à l'administration centrale de la justice pourrait également entraîner une certaine pression institutionnelle pour valider rapidement des SIA développés en interne ou en partenariat public-privé, afin de répondre aux objectifs de modernisation rapide du service public. Dans un tel contexte, il existe un risque de labellisation anticipée de solutions insuffisamment auditées, mal entraînées ou biaisées. Cette validation prématurée pourrait compromettre l'image du ministère, qui est attendue tant par l'opinion publique que les professionnels pour ne pas reproduire les mêmes erreurs dans le domaine du numérique.

[15] Les dispositions du RIA s'inscrivent dans le *New Legislative Framework* de 2008, qui est un ensemble de textes visant notamment à établir un cadre commun de politiques de mise en conformité.

4.4. Risque de politisation des difficultés rencontrées

Enfin, une labellisation ou certification par le ministère de la justice, en tant qu'autorité politique, pourrait être perçue comme partiale ou dépendante d'orientations gouvernementales.

Une telle perception pourrait nourrir des controverses sur les intentions politiques derrière certains cas d'usage de SIA (par exemple, ciblage, automatisation des peines, contrôle social), et fragiliser tout développement ambitieux de cette technologie.

5. Proposition de plan d'action pour un dispositif national de labellisation et de certification de systèmes d'IA dans le domaine de la justice

Le développement de politiques de labellisation et de certification de SIA dans le domaine de la justice traduira concrètement la volonté politique de déployer des systèmes conformes à des exigences techniques (robustesse et fiabilité des systèmes, cybersécurité, etc.) et juridiques (protection des droits fondamentaux, de l'État de droit, etc.).

Il est proposé ici un plan d'action se décomposant en trois étapes temporelles : court (5.1), moyen (5.2) et long terme (5.3), avec des objectifs opérationnels pour chaque phase.

5.1. À court terme (dès 2025)

Il s'agira de s'accompagner le ou les cas d'usages prioritaires, au moyen d'actions immédiates et peu coûteuses :

• **Élaborer un référentiel *provisoire et expérimental* de bonnes pratiques[16] pour une « IA digne de confiance en justice » (IDCJ) à destination des concepteurs, tant publics que privés** : ce référentiel, élaboré sous forme de bonnes pratiques, permettrait aux concepteurs de distinguer si leur système relève d'un cas à « haut risque » ou non, et proposer pour les systèmes n'étant pas couverts par les obligations de certification du RIA, un ensemble de mesures volontaires ouvrant la voie à une possible labellisation IDCJ. Ces critères pourraient s'inspirer de la littérature existante (entre droit contraignant, dont les exigences du chapitre II du RIA pour les IA à haut risque, et droit souple, comme la Charte éthique européenne de la CEPEJ, le HUDERIA du Conseil de l'Europe ou encore les recommandations de l'OCDE et de l'UNESCO).

Pour garantir la légitimité du processus, ce référentiel devrait idéalement être validé par une autorité présentant certains critères d'indépendance ou reposer sur une gouvernance collégiale incluant des magistrats, des chercheurs, des représentants des usagers et des experts en régulation du numérique. Le comité stratégique et éthique / observatoire en cours de composition pourrait avoir vocation à réaliser cette validation, en s'adjoignant des représentants des usagers et experts en régulation du numérique si ces derniers ne sont pas représentés en son sein.

Ce référentiel servira de base à toute évaluation. Il pourra être publié, de manière provisoire et expérimentale, sous forme de guide de bonnes pratiques et être amélioré sur la base d'un travail avec l'ensemble des parties prenantes (professionnels, recherche, secteur privé, société civile).

• **Conditionner sans délai les nouveaux marchés publics à une obligation d'information de critères de qualité spécifiques à l'IA :** les appels d'offres pourrait d'ores-et-déjà contenir une clause demandant si le produit possède déjà un label d'IA responsable, a fait l'objet d'un audit préalable ou d'une certification tierce.

[16] Ce référentiel est une production originale du COMOP à destination des concepteurs, complémentaire au référentiel à destination des utilisateurs, déjà produit par le SEM (*cf.supra*).

• **Finaliser et diffuser le référentiel à destination de l'ensemble des utilisateurs du ministère de la justice** : finaliser et diffuser le projet de charte élaboré par le secrétariat général (SEM), en rendant obligatoire la réalisation de la formation déjà existante sur MENTOR (afin de mieux comprendre les enjeux et les limites des systèmes qu'ils seront amenés à utiliser).

• **Travailler sur la mise en place d'un « bac à sable » réglementaire dédié aux applications de l'IA dans la justice :** Initier une discussion conjointe principalement entre le ministère de la justice, la DINUM et la CNIL[17], afin d'autoriser la mise en place d'un espace d'expérimentation en conditions réelles de SIA dédiés à la justice. Ce cadre permettrait tant aux initiatives publiques que privées de tester des applications à une échelle pertinente hors des laboratoires de conception, avec l'accompagnement des régulateurs. En échange, les concepteurs s'engagent à respecter, *a minima*, le référentiel de bonnes pratiques. L'avantage d'un tel dispositif est double : il aide les porteurs de projet, tant publics que privés, à améliorer la conformité de leur IA tout en familiarisant l'administration aux innovations, dans un cadre contrôlé. À l'issue de la période de test, si l'outil est jugé satisfaisant, une attestation de conformité temporaire (ou label « prototype ») pourrait lui être délivrée, facilitant son déploiement ultérieur.

• **Identifier et hiérarchiser les cas d'usage nécessitant une labellisation ou une certification :** les efforts devront être ciblés et circonscrits aux seules applications présentant un enjeu pertinent.

5.2. À moyen terme (horizon 2025-2026)

Il s'agira alors de structurer formellement le dispositif de labellisation et d'amorcer la certification obligatoire des IA « à haut risque », en phase avec l'entrée en application du règlement européen.

Cela implique de :

• **Institutionnaliser une autorité de labellisation et réaliser les désignations d'autorités dans le cadre du RIA** : outre la désignation des autorités compétentes et des organismes notifiés dans le cadre du RIA, le ministère de la justice pourrait pérenniser le comité stratégique et éthique / observatoire en tant qu'organe de pilotage de ses politiques relatives au déploiement de SIA, dont la validation de référentiels et la mise en place de procédures de mise en conformité. L'appui à cette structure pourrait être assuré par un secrétariat *ad hoc* pour cette période cruciale d'accélération de l'implantation des SIA. Cet organe pourrait être point de contact national pour le volet justice du RIA et contribuer aux travaux du Conseil européen de l'IA.

• **Lancer un programme de certification pilote** : identifier 1 ou 2 SIA concrets déjà en service ou sur le point de l'être dans la justice française et soumettre ces « cas pilotes » à une procédure de certification. Par exemple, si un système généraliste est en test dans un tribunal, mandater un audit indépendant (réalisé par un organisme certificateur accrédité, par exemple le LNE, le Bureau Veritas ou l'AFNOR, sous supervision de la CNIL) pour évaluer sa conformité au référentiel. À l'issue de l'audit, délivrer (si la conformité est avérée) un certificat valable pour une durée déterminée (2 ou 3 ans), avec suivi annuel. Ce certificat attestera que l'IA est « apte au service » dans le respect des principes énoncés. Les résultats de l'évaluation pourraient être publiés pour assurer une totale transparence vis-à-vis du public. Cette phase pilote permettra d'ajuster les modalités pratiques (coûts, durée, tests techniques nécessaires) de la certification avant sa généralisation.

• **Développer les référentiels certifiables** : sur la base du référentiel provisoire et expérimental de bonne pratique et du résultat du programme de certification pilote, élaborer des normes françaises ou européennes applicables spécifiquement aux SIA dans le domaine de la justice. Cela peut passer par la participation aux comités de standardisation (AFNOR, CEN/CENELEC, ISO) qui travaillent sur des normes d'IA fiable, afin d'intégrer des exigences spécifiques aux applications juridiques. Le référentiel devra couvrir les aspects clés : qualité des données d'entraînement (exclusion de biais manifestes), niveau d'explicabilité requis (par exemple, obligation de fournir aux magistrats une notice expliquant le

[17] D'autres acteurs comme l'ANSSI et le Défenseur des droits pourraient également être joints.

fonctionnement de l'algorithme et les facteurs influençant ses recommandations), dispositifs de recours ou de plainte en cas d'erreur, etc. Une fois validés, ces critères pourront être adoptés officiellement par arrêté ou décret comme base de la certification.

• **Préparer le terrain réglementaire** : si nécessaire, il pourrait être proposé des adaptations législatives ou réglementaires pour arrimer le dispositif national au RIA. Par exemple, intégrer dans le code de l'organisation judiciaire ou le code de procédure civile des dispositions imposant que tout logiciel d'aide à la décision utilisé par un juge doit avoir obtenu une certification conforme au droit de l'UE. De même, prévoir dans la loi les pouvoirs de contrôle et de sanction en cas d'utilisation d'une IA non certifiée ou présentant un danger (cela pourrait s'inspirer du régime de police administrative existant pour la sécurité des produits).

5.2. À long terme (horizon 2027+)

Il conviendra alors de pérenniser et d'élargir le dispositif pour qu'il devienne une composante naturelle du fonctionnement du système judiciaire. Une fois le RIA pleinement en vigueur et les mécanismes nationaux rodés, le ministère de la justice pourrait :

• **Rendre obligatoire la certification pour toutes les IA de justice, même avec un risque modéré** : concrètement, aucun SIA susceptible d'influencer directement ou indirectement une décision judiciaire ou d'évaluer des justiciables ne devrait pouvoir être utilisé sans le visa délivré par l'autorité compétente, dans laquelle les cours supérieures (Cour de cassation et Conseil d'État) disposeraient d'un pouvoir de véto. Cela rejoindra d'ailleurs l'obligation de conformité du fournisseur prévue par le RIA, mais on pourrait l'étendre aux outils développés en interne par l'administration. Un calendrier d'application gradué pourra être fixé (par ex. d'abord les domaines pénaux et d'aide à la décision, puis d'autres).

• **Institutionnaliser le label public « IA Digne de Confiance en Justice » (IDCJ)** : en complément des certifications strictement techniques et juridiques obligatoires, pérenniser le label national « IDCJ » piloté par l'observatoire / comité, qui valorise les SIA allant au-delà des exigences minimales. Ce label, attribué après évaluation, pourrait prendre en compte des critères éthiques plus larges (par ex. contribution à l'open source, ergonomie pour les magistrats, approches anti-biais innovantes). Il inciterait les éditeurs à viser l'excellence et serait un signe distinctif lors des achats publics. Sur le modèle du label « SecNumCloud » en cybersécurité qui garantit un haut niveau de sécurité des services cloud utilisés par l'État, un label « IDCJ » garantirait un haut niveau de qualité algorithmique pour les outils adoptés par les tribunaux et l'ensemble des administrations du ministère.

• **Assurer une veille et une réévaluation continues** : le dispositif devra évoluer avec la technique. Il devra être prévu des réexamens périodiques des algorithmes certifiés, car un SIA peut voir ses performances varier dans le temps (données mises à jour, dérive du modèle). Par exemple, il pourrait être imposé une re-certification tous les 2 ans pour les SIA en service, ou immédiatement en cas de modification majeure de l'algorithme. Il devrait être également mis en place un système de retour d'expérience : en collectant les retours des utilisateurs (juges, greffiers) et éventuellement des justiciables, afin de détecter d'éventuels problèmes passés inaperçus lors de la certification initiale. Ce retour d'information pourrait alimenter les futures versions du référentiel.

• **Coordination internationale** : le dispositif français pourrait être étendu au niveau européen, et participer à l'émergence d'un éventuel label européen d'IA fiable dans la justice. Le but à long terme serait d'éviter la multiplicité des évaluations : une certification obtenue en France pourrait être mutuellement reconnue chez nos voisins (et vice versa) grâce à l'harmonisation européenne. La France, forte de son expérience, pourrait jouer un rôle moteur dans les instances européennes (tant au sein de l'Union qu'au Conseil de l'Europe) pour diffuser les meilleures pratiques. Enfin, encourager la coopération scientifique (par ex. avec le Canada ou les Pays-Bas) autour de banques de données d'essai ("AI audit sandbox") internationales, où différents pays soumettraient les mêmes algorithmes à évaluation afin de comparer et unifier les méthodes d'audit.

ANNEXE N°3

Principes directeurs pour la conception de systèmes d'IA dans le domaine judiciaire

SYNTHESE

Le développement de systèmes d'intelligence artificielle (SIA) dans le domaine judiciaire présente des enjeux spécifiques, tenant essentiellement à la spécificité des mesures à mettre en œuvre pour garantir le respect de l'État de droit. Ces systèmes, quand ils sont destinés aux magistrats et agents du Ministère de la Justice (fonctionnaires de greffe, personnels pénitentiaires, protection judiciaire de la jeunesse), manipulent des données sensibles et peuvent influencer des décisions ayant un fort impact sur les droits des citoyens. Quand ils sont à destination d'autres professionnels du droit ou au grand public, des garanties essentielles doivent également pouvoir leur être appliquées afin, notamment, de ne pas limiter l'accès au juge ou créer des discriminations illégitimes.

En faisant converger les obligations résultant du droit positif (règlement général sur la protection des données (RGPD), règlement européen sur l'IA (RIA), convention-cadre du Conseil de l'Europe, loi informatique et libertés notamment) et du droit « souple » (comme la charte éthique de la CEPEJ), les SIA dans le domaine de la justice doivent satisfaire une série d'exigences strictes, qui peuvent être regroupés en 8 principes : respecter les droits fondamentaux et les libertés publiques, garantir l'équité et la non-discrimination, assurer la sécurité et la souveraineté des données et des modèles, fournir transparence et traçabilité pour permettre l'explicabilité, maintenir un contrôle humain sur les décisions, adopter une approche de sobriété numérique, et enfin s'inscrire dans une logique de gouvernance partagée avec toutes les parties prenantes.

Le respect de ces exigences a pour objectif de garantir les droits des justiciables, la sécurité juridique et la confiance du public envers l'institution judiciaire et les administrations à son service.

Ces principes visent à guider les concepteurs de SIA (équipes internes ou prestataires externes) dans la réalisation de solutions conformes aux valeurs et obligations du ministère.

Ils traduisent des principes éthiques et juridiques dans un langage opérationnel, composé d'actions concrètes et vérifiables à chaque étape du cycle de vie d'un SIA. Ils opérationnalisent le cadre législatif existant – RGPD, RIA, loi Informatique et libertés – tout en fournissant des recommandations opérationnelles spécifiques au domaine de la justice.

PRINCIPES DIRECTEURS DE CONCEPTION

1. Veiller, dès la conception, au respect absolu des droits fondamentaux et des libertés individuelles

Les systèmes d'IA (SIA) doivent être conçus et utilisés dans le strict respect des droits fondamentaux, incluant la dignité humaine, la vie privée et le droit à un procès équitable. Aucune fonctionnalité d'un SIA ne doit porter atteinte aux droits et libertés garantis tant par les différents traités internationaux ratifiés par la France que les dispositions relevant du droit de l'Union ou du droit national.

2. Prévenir toute forme de biais algorithmique afin de garantir au mieux l'équité et la non-discrimination dans les résultats produits par les systèmes

Prévenir toute forme de biais ou de discrimination dans les SIA en veillant à la représentativité des données et à la cohérence de traitement des cas similaires, conformément au principe d'égalité devant la loi. En d'autres termes, l'algorithme doit traiter tous les usagers de manière équitable et ne pas reproduire ou aggraver des inégalités injustifiées.

3. Assurer la sécurité et la souveraineté des systèmes d'IA, ainsi que la protection des données tout au long du cycle de vie, de la conception au déploiement, jusqu'au décommissionnement

Assurer la sécurité informatique et physique des SIA en utilisant des infrastructures fiables et souveraines, en protégeant les données sensibles et en intégrant des mécanismes de fonctionnement sûr. L'IA doit être sécurisée « de bout en bout » : elle doit résider sur des plateformes de confiance, préserver la confidentialité et l'intégrité des données judiciaires, et fonctionner de manière sûre même en cas d'incident technique ou de tentative malveillante.

4. Garantir, tout au long du cycle de vie et par des mesures de supervision adaptées, la qualité, la fiabilité et la robustesse des données, des modèles et des systèmes d'IA dans leur ensemble afin d'en limiter les éventuelles dérives

Garantir la qualité des données, la fiabilité des modèles et la robustesse du système face à de divers aléas, en évaluant rigoureusement les performances et en assurant une surveillance continue. En d'autres termes, l'IA doit fournir des résultats aussi exacts et stables que possible, et continuer de fonctionner correctement même dans des conditions dégradées ou imprévues.

5. Pour les systèmes les plus sensibles, produire une documentation exhaustive et garantir la traçabilité des opérations afin de garantir, dans les limites techniques des méthodes employées, explicabilité et transparence

Rendre compréhensible le fonctionnement de l'IA, fournir des explications sur les résultats, documenter les algorithmes et données utilisés, et assurer la traçabilité des décisions. En pratique, cela signifie que les concepteurs doivent documenter le système de manière exhaustive, au moins pour les systèmes les plus sensibles, et prévoir des moyens d'explication et de suivi pour que ni les utilisateurs internes ni les usagers externes ne soient confrontés à une « boîte noire ».

6. Maintenir un contrôle humain à chaque étape critique du processus décisionnel assisté par l'IA

Maintenir l'humain au cœur du processus décisionnel, avec la possibilité de valider, modifier ou infirmer les résultats de l'IA. En toutes circonstances, le décideur final doit être un humain. Le SIA ne fait qu'assister ou éclairer la décision, mais ne se substitue jamais à la responsabilité humaine.

7. Adopter une approche de frugalité numérique et de développement durable dans la conception des systèmes d'IA

Adopter une approche sobre en optimisant les algorithmes et l'infrastructure pour limiter l'empreinte environnementale et les coûts, en privilégiant des solutions proportionnées aux besoins réels et évolutives. Il s'agit de développer des IA « à la juste mesure » du besoin à traiter : éviter la surenchère technologique inutile, minimiser la consommation d'énergie et de ressources, et concevoir des systèmes pérennes plutôt qu'éphémères.

8. Favoriser la collaboration et une gouvernance partagée dans le développement des projets d'IA

Favoriser les échanges entre services et institutions, promouvoir l'usage de solutions open source quand c'est possible, et établir une gouvernance claire des projets d'IA. Ce principe promeut une démarche collective et transparente autour de l'IA, afin d'éviter l'isolement des projets, de tirer parti de l'intelligence collective et de garantir la cohérence à l'échelle du ministère.

* * *

Chacun de ces principes fait l'objet d'une explication détaillée ci-après, incluant son rappel, des exemples d'application, les risques en cas de non-respect, les mesures préventives à mettre en œuvre, et d'éventuelles spécificités liées aux IA génératives.

EXPLICATION DÉTAILLÉE DE CHAQUE PRINCIPE

1. Principe 1 – Veiller, dès la conception, au respect absolu des droits fondamentaux et des libertés individuelles

Rappel du principe : Les systèmes d'IA doivent être conçus et utilisés dans le strict respect des droits fondamentaux, incluant la dignité humaine, la vie privée et le droit à un procès équitable. Aucune fonctionnalité d'un SIA ne doit porter atteinte aux droits et libertés garantis tant par les différents traités internationaux ratifiés par la France que les dispositions relevant du droit de l'Union ou du droit national.

Exemples concrets de situations concernées par le principe :

- **Atteinte à la dignité humaine** – Lors de la création de systèmes en capacité de contribuer à l'appréciation d'une situation individuelle créant ou limitant des droits, les utilisateurs pourraient progressivement limiter leur office à la simple reproduction de l'évaluation algorithmique. En ce sens, il pourrait être rappelé qu'aucune décision de justice ayant un effet significatif sur un individu ne doit être prise de manière entièrement automatisée, sans intervention humaine (art. 47 de la loi informatique et libertés modifiée). Un utilisateur doit toujours vérifier et valider la recommandation d'un SIA avant que soit produit un effet juridique.
- **Violation de la vie privée** – Des données sensibles ou des informations confidentielles pourraient être divulguées à des plateformes externes non validés par le ministère.
- **Barrière d'accès au juge** – Un SIA ne devrait pas limiter ou dissuader des usagers d'exercer leurs droits. Par exemple, un SIA situant les prétentions d'un justiciable dans des fourchettes d'indemnisation ou de compensation ne doit pas constituer le seul critère d'appréciation pour élaborer une stratégie judiciaire.

Risques en cas de non-respect :

- **Atteintes aux personnes** – Fuite ou utilisation abusive de données personnelles portant atteinte à la vie privée des justiciables ; traitements injustes portant atteinte à la dignité (par exemple, décisions automatisées perçues comme inhumaines) ou violation des droits des usagers (droit à un recours effectif, droit à un procès équitable).
- **Illégalité et contentieux** – Un SIA non conforme aux droits fondamentaux peut entraîner des décisions exposant l'administration à des contentieux et à des sanctions (administratives, pénales ou disciplinaires).
- **Perte de confiance** – Les professionnels et les usagers perdront confiance en l'IA (voire dans l'institution judiciaire elle-même) si celle-ci génère des injustices flagrantes ou compromet la confidentialité des informations sensibles. Un scandale lié à une IA violant les droits fondamentaux pourrait discréditer durablement l'usage des technologies numériques au sein de la justice.

Mesures préventives à mettre en œuvre :

- **Information aux utilisateurs** – Introduire des messages d'avertissement à destination des utilisateurs utilisant des recommandations algorithmiques, apparaissant à une fréquence régulière, pour qu'ils ne limitent pas leur office à la simple reproduction de l'évaluation produite par un système.
- **Conformité juridique dès la conception** – Intégrer des juristes et experts éthiques dès le début du projet pour valider juridiquement les cas d'usage. Vérifier la conformité aux textes applicables (RGPD, Loi Informatique et Libertés, RIA). Réaliser une étude d'impact sur la protection des données (AIPD) et, le cas échéant, une analyse d'impact éthique, afin d'identifier et traiter en amont les risques pour les droits et libertés.
- **Minimisation et protection des données** – Appliquer le principe de minimisation des données : ne collectez et n'utilisez que les données strictement nécessaires[9] à la finalité poursuivie. Mettre en place un chiffrement systématique des données personnelles sensibles et des mécanismes de contrôle d'accès rigoureux. Par exemple, isoler les données judiciaires dans des environnements sécurisés, compartimenter les accès selon les habilitations, et conserver une traçabilité des consultations.
- **Équipe pluridisciplinaire** – Constituer une équipe de conception pluridisciplinaire incluant des spécialistes du droit, de l'éthique, de la cybersécurité, etc. Cette équipe garantira que le développement technique intègre bien toutes les obligations de respect des droits.
- **Vérifications et audits** – Prévoir des audits réguliers (juridiques, éthiques et techniques) du système aux différentes phases (conception, test, exploitation) pour vous assurer qu'il demeure conforme aux droits fondamentaux. Si l'IA est basée sur des modèles externes (par exemple un modèle de langage pré-entraîné), examiner attentivement les conditions d'utilisation de ce modèle et ses éventuels biais connus afin de vous prémunir contre tout usage non conforme aux valeurs du service public.

Spécificités concernant les IA génératives : Les IA génératives (capables de produire du texte, des images, etc.) posent des défis particuliers en matière de droits fondamentaux. D'une part, elles peuvent générer des contenus faux ou trompeurs (« hallucinations ») pouvant porter atteinte à la dignité d'autrui ou diffuser involontairement des données personnelles sensibles extraites de leur corpus d'apprentissage. D'autre part, nombre de ces IA génératives sont proposées via des services en ligne par des entités privées : leur utilisation dans un contexte judiciaire doit donc respecter strictement la souveraineté et la confidentialité des données. En pratique, si une solution du ministère inclut une IA générative (par exemple un modèle de langage pour rédiger des documents juridiques), il doit être garanti que toutes les données judiciaires envoyées au modèle restent sous contrôle du ministère (hébergement souverain, absence de conservation non autorisée par le fournisseur). Mettre en place des filtres ou des garde-fous empêchant la génération de contenus discriminatoires, diffamatoires ou contraires aux droits de la défense. Enfin, rappeler aux utilisateurs finaux qu'ils doivent vérifier tout contenu généré avant de l'utiliser dans une procédure, afin d'éviter qu'une erreur de l'IA ne conduise à une atteinte aux droits d'une partie.

2. Principe 2 – Prévenir toute forme de biais algorithmique afin de garantir au mieux l'équité et la non-discrimination dans les résultats produits par les systèmes

Rappel du principe : Prévenir toute forme de biais ou de discrimination dans les SIA en veillant à la représentativité des données et à la cohérence de traitement des cas similaires, conformément au principe d'égalité devant la loi. En d'autres termes, l'algorithme doit traiter tous les usagers de manière équitable et ne pas reproduire ou aggraver des inégalités injustifiées.

Exemples concrets de situations concernées par le principe :

- **Données non représentatives** – Par exemple, pour une IA analytique d'aide à la décision, les jeux de données pourraient ne pas inclure des cas diversifiés (âges, genres, origines, contextes socio-économiques…). Des données non représentatives pourraient conduire une IA analytique à produire systématiquement les mêmes recommandations pour certains groupes de personnes, reproduisant ainsi des préjugés existants.
- **Traitement incohérent de cas similaires** – Pour des situations identiques, les SIA devraient pouvoir fournir des résultats similaires, sans disparités inexpliquées. Par exemple, deux dossiers comparables devraient aboutir à un même niveau d'évaluation, indépendamment de caractéristiques personnelles telles que l'origine ou le genre des individus concernés. Si le SIA propose des décisions divergentes pour des cas analogues, cela peut conduire à choisir une autre méthode algorithmique.
- **Manque d'attention aux biais lors de la conception** – Les processus de conception eux-mêmes pourraient créer ou renforcer des biais. Par exemple, certains scénarios minoritaires pourraient être exclus du processus d'entraînement (biais d'exclusion) : négliger les cas peu fréquents pourrait défavoriser ces minorités lorsque le système sera utilisé. Un autre exemple est le biais de confirmation chez les concepteurs : si l'on suppose dès le départ une corrélation (par ex. « telle infraction est plus fréquente chez tel groupe ») et qu'on oriente le modèle dans ce sens, on crée un biais. Pour éviter cela, baser le développement sur des données objectives et vérifier les hypothèses avec des experts externes (sociologues, statisticiens…).

Risques en cas de non-respect :

- **Décisions biaisées et inégalitaires** – Un SIA n'ayant pas été conçu avec une attention suffisante aux éventuels biais peut produire des décisions défavorisant systématiquement certains groupes de population. De telles discriminations exposent les concepteurs à des contentieux pour discrimination et à de graves atteintes à son image.
- **Reproduction d'inégalités sociales** – L'IA risquerait de perpétuer ou aggraver les inégalités existantes. Par exemple, si un algorithme d'affectation de ressources (comme l'aide juridictionnelle) est entraîné sur des données reflétant un sous-investissement historique dans certaines zones géographiques, il pourrait continuer à désavantager ces zones.
- **Perte de confiance et efficacité réduite** – Les professionnels et les usagers pourraient perdre confiance dans un SIA perçu comme « injuste ». Une telle perte de confiance conduit souvent à un rejet pur et simple de l'outil, même s'il présente par ailleurs des bénéfices.

Mesures préventives à mettre en œuvre :

- **Audit et détection des biais** – Vérifier si le modèle n'a pas uniquement appris à partir d'un profil dominant. Auditer régulièrement les algorithmes et les données utilisés afin d'identifier

d'éventuels biais avant et après la mise en service. Mener des tests spécifiques sur des sous-groupes (par exemple, comparer les taux de précision de l'IA pour différents groupes démographiques) pour repérer toute disparité. Si un biais est détecté, analyser l'origine (donnée d'entrée incomplète, variable *proxy* inappropriée, etc.) et ajuster le système en conséquence.

- **Diversification et nettoyage des données** – Pour les IA analytiques, diversifier les données d'entraînement et éliminer les biais connus (inclure des données de différentes sources et périodes, écarter les attributs clairement discriminatoires sauf s'ils sont légitimes au regard du cas d'usage, et corriger les erreurs ou déséquilibres flagrants comme la surreprésentation d'un type de cas).
- **Conception guidée par l'équité** – Intégrer des métriques d'évaluation de l'équité dès la phase de conception. Par exemple, définir des indicateurs de non-discrimination (comme l'écart de taux d'erreur entre groupes) et fixer des seuils à ne pas dépasser. Utiliser, quand cela est possible, des techniques de « debiasing » automatique (retrait de certaines variables, rééquilibrage d'échantillons, ajustement de paramètres) pour atténuer les biais tout en surveillant l'impact sur la performance globale.
- **Équipe multidisciplinaire** – Comme pour le principe précédent, faites appel à une équipe multidisciplinaire comprenant des chercheurs, des représentants du terrain et des juristes.
- **Transparence sur l'équité** – Documenter et publier, dans la mesure du possible, des informations sur les tests de biais effectués et les résultats obtenus. Une transparence sur l'évaluation de l'équité renforcera la confiance des utilisateurs et permettra un contrôle externe. Par exemple, un rapport interne pourrait indiquer : « l'algorithme a été testé pour détecter des disparités de traitement hommes/femmes dans les recommandations, aucune différence significative n'a été relevée au seuil de 5%. »

Spécificités concernant les IA génératives : Les modèles d'IA générative sont entraînés sur de très grands volumes de données (textes, images…) généralement issus d'Internet. Ils peuvent hériter des stéréotypes et préjugés présents dans ces données. Par conséquent, si vous intégrez une IA générative dans un processus judiciaire, divers tests devront être menés. Par exemple, un modèle de langage pourrait, sans le vouloir, utiliser un ton ou un vocabulaire différent selon le genre ou l'origine ethnique des personnes mentionnées dans un dossier, reflétant ainsi des biais des textes d'entraînement. Prévoir des filtres et des relectures humaines pour corriger des sorties biaisées. Envisager de fine-tuner (reconfigurer) le modèle génératif sur des données spécialisées et contrôlées du domaine juridique, afin d'atténuer les influences indésirables de données génériques. Enfin, informer clairement les utilisateurs que l'IA peut être influencée par des biais cachés et qu'ils doivent donc exercer un regard critique, en particulier sur les contenus générés touchant à des populations potentiellement vulnérables ou stigmatisées.

3. Principe 3 – Assurer la sécurité et la souveraineté des systèmes d'IA et la protection des données tout au long du cycle de vie, de la conception au déploiement, jusqu'au décommissionnement

Rappel du principe : Assurer la sécurité informatique et physique des SIA en utilisant des infrastructures fiables et souveraines, en protégeant les données sensibles et en intégrant des mécanismes de fonctionnement sûr. L'IA doit être sécurisée « de bout en bout » : elle doit résider sur des plateformes de confiance, préserver la confidentialité et l'intégrité des données judiciaires, et fonctionner de manière sûre même en cas d'incident technique ou de tentative malveillante.

Exemples concrets de situations concernées par le principe :

- **Hébergement de traitements et de données relevant d'une sensibilité particulière** – Les traitements, les modèles d'IA et les données pourraient être traités sur des infrastructures non approuvées par l'État.
- **Absence de plan de secours en cas de panne** – Absence de procédures manuelles de secours au cas où l'IA deviendrait indisponible ou défaillante. Documenter les modes dégradés et entraîner les personnels à les activer.
- **Sécurité physique** – Si le système repose sur un serveur local, le matériel pourrait être exposé à des personnels non habilitées.
- **Manipulations et attaques de systèmes** – Pour des SIA accessibles via une interface publique (chatbot pour orienter les justiciables), des entrées spécifiques pourraient conduire le système à produire des résultats inattendus ou problématiques.

Risques en cas de non-respect :

- **Fuite, perte ou compromission de données** – Si la sécurité n'est pas assurée, des données judiciaires sensibles (données personnelles de justiciables, dossiers confidentiels, informations sur des enquêtes en cours, etc.) pourraient fuiter, être volées ou altérées. Outre le préjudice pour les personnes concernées (vie privée violée, risque pour la sécurité des victimes ou témoins…), de tels incidents entacheraient gravement la crédibilité de l'institution et constitueraient des manquements au RGPD, passibles de sanctions.
- **Cyberattaques et sabotage** – Un SIA mal sécurisé est une porte d'entrée pour des cyberattaques. Une intrusion pourrait mener à un sabotage du service ou, pire, à des modifications subreptices des algorithmes ou des données entraînant des décisions erronées.
- **Atteinte à la continuité du service public** – En cas de panne non anticipée ou d'indisponibilité de l'IA sans plan de secours, le service rendu par la Justice pourrait être interrompu ou dégradé.
- **Non-conformité juridique** – Sur le plan juridique, un manquement à la sécurité peut entraîner des obligations de notification (notification de violation de données personnelles à la CNIL et aux personnes concernées sous 72h selon le RGPD) et d'éventuelles actions en responsabilité. Par ailleurs, l'utilisation d'un service cloud non conforme aux exigences étatiques de souveraineté pourrait être invalidée par les autorités (ex. invalidation de transferts de données hors UE).

Mesures préventives à mettre en œuvre :

- **Hébergement souverain et conforme pour le traitement de données relevant d'une sensibilité particulière** – Déployer les modèles d'IA et stocker les données sur des infrastructures approuvées par l'État. Par exemple, un système d'IA traitant des casiers judiciaires devrait être hébergé sur les serveurs sécurisés du ministère de la Justice ou sur un cloud certifié SecNumCloud répondant aux exigences nationales.
- **Chiffrement et contrôle d'accès** – Protéger les données manipulées par les SIA par des mesures de cryptographie et d'authentification fortes. Par exemple, les communications entre un SIA et une base de données de décisions de justice devraient être chiffrées de bout en bout (protocoles HTTPS, VPN interne…) pour empêcher toute interception. De même, restreindre l'accès aux données d'entraînement et aux réglages du modèle : seuls les personnels habilités (développeurs accrédités, administrateurs sécurité) doivent pouvoir y accéder, via des comptes sécurisés et une traçabilité des actions.
- **Approche « sécurité dès la conception »** (SecByDesign) – Intégrer les experts en cybersécurité dès le début du projet. Réaliser une analyse de risques dédiée à la sécurité du système d'IA (identifier les menaces potentielles, les vulnérabilités, estimer l'impact et la probabilité) puis appliquer les mesures de réduction de ces risques.
- **Infrastructures fiables et tests** – Utiliser des infrastructures éprouvées et conformes : privilégier des datacenters agréés, des systèmes d'exploitation tenus à jour, et isoler les environnements (développement, test, production) pour limiter les propagations en cas d'incident. Avant le déploiement, effectuer des tests d'intrusion et des audits de sécurité du code et de l'architecture. Corriger toutes les vulnérabilités critiques identifiées. Renouveler ces audits régulièrement, au moins une fois par an ou à chaque modification majeure.
- **Sauvegardes et plan de continuité** – Mettre en place un système de sauvegarde sécurisé et fiable de toutes les données critiques de l'IA (données d'entraînement, modèles entraînés, configurations). Stocker les sauvegardes chiffrées sur un site distinct. Élaborer un Plan de continuité d'activité (PCA) incluant des scénarios de panne de l'IA : ce PCA doit détailler les procédures de bascule en mode manuel ou alternatif. Tester périodiquement ces procédures de reprise afin de vous assurer qu'elles fonctionnent et que le personnel sait les déclencher. Documenter les modes dégradés et entraîner les personnels à les activer.
- **Contrôle d'accès et traçabilité** – Appliquer une gestion rigoureuse des identités et des accès : principe du moindre privilège pour les comptes ayant accès au système d'IA, authentification multi-facteur, journalisation (*logging*) de toutes les actions d'administration et des accès aux données. Mettre en place une traçabilité fine : chaque décision ou recommandation produite par l'IA devrait être loggée avec un identifiant de requête, l'utilisateur demandeur, la date/heure et idéalement l'empreinte de la version du modèle ayant produit l'output.
- **Surveillance continue** – Une fois le SIA en production, assurer une surveillance continue de son comportement. Cela inclut la mise en place d'alertes automatiques en cas d'anomalies (par exemple, un volume inhabituel de requêtes pouvant indiquer une attaque DDoS, ou un taux d'erreur qui bondit soudainement) et de vérifications régulières de l'intégrité du modèle et des données (pour détecter toute manipulation ou dégradation). Un SIA critique devrait idéalement être supervisé 24/7 par un centre opérationnel de sécurité (SOC) capable de réagir en cas d'alerte.
- **Mises à jour et patchs** – Maintenir à jour le SA et l'ensemble de ses dépendances logicielles. Appliquer rapidement les correctifs de sécurité dès leur disponibilité (après les avoir testés en environnement de pré-production). De même, prévoir un budget et un calendrier pour mettre à niveau régulièrement l'infrastructure matérielle afin de bénéficier des dernières protections technologiques.

- **Prévention des entrées malveillantes** - Prévoir des mécanismes pour détecter et bloquer les entrées malveillantes (injections de code, envois massifs de requêtes pour la faire planter, etc.). Une autre précaution est de sécuriser la chaîne d'approvisionnement des données : s'assurer que les données d'entraînement ou de mise à jour du modèle ne puissent être empoisonnées par un acteur tiers (par ex. vérification d'intégrité des fichiers de données, contrôle des sources).

Spécificités concernant les IA génératives : L'usage d'IA génératives (fournies souvent via des API en ligne) pose des défis de sécurité particuliers : risque de divulgation de données et dépendance à un fournisseur externe. Si votre système appelle un service d'IA générative tiers (ex. une API de résumé de texte), sachez que chaque requête transmet potentiellement des données au fournisseur. Assurez-vous contractuellement que ce dernier n'enregistre ni ne réutilise ces données (accord de traitement des données conforme au RGPD). Idéalement, privilégiez les modèles génératifs open-source déployés sur une infrastructure du ministère, pour garder la maîtrise des informations. Par ailleurs, les modèles génératifs peuvent être la cible de *« prompt injections »* ou manipulations de requêtes malveillantes visant à les faire sortir du cadre prévu (par ex., pousser l'IA conversationnelle à divulguer des informations confidentielles en contournant ses filtres). Pour anticiper ces attaques, limiter sur la longueur des entrées, filtrer de certains motifs ou instructions suspectes, et valider par des humains les sorties sensibles. Enfin, surveiller les mises à jour du modèle génératif lui-même : s'il est régulièrement entraîné ou modifié par son fournisseur, réévaluer la sécurité à chaque nouvelle version (les changements de comportement pourraient introduire de nouvelles failles exploitables).

4. Principe 4 – Garantir, tout au long du cycle de vie et par des mesures de supervision adaptées, la qualité, la fiabilité et la robustesse des données, des modèles et des systèmes d'IA dans leur ensemble afin d'en limiter les éventuelles dérives

Rappel du principe : Garantir la qualité des données, la fiabilité des modèles et la robustesse du système face à de divers aléas, en évaluant rigoureusement les performances et en assurant une surveillance continue. En d'autres termes, l'IA doit fournir des résultats aussi exacts et stables que possible, et continuer de fonctionner correctement même dans des conditions dégradées ou imprévues.

Exemples concrets de situations concernées par le principe :

- **Données obsolètes ou non qualitatives** – Les données d'entraînement pourraient provenir de sources obsolètes ou peu qualitatives.
- **Production de résultat aberrant** – Si une entrée essentielle est manquante (dossier incomplet) ou si une donnée d'entrée est très inhabituelle (valeur extrême, situation jamais vue), le système pourrait produire un résultat aberrant sans avertissement.
- **Surveillance limitée ou défaillante en production** – Le fonctionnement du SIA pourrait s'effectuer sur des indicateurs non pertinents.

Risques en cas de non-respect :

- **Erreurs et décisions erronées** – Des données de mauvaise qualité (incomplètes, fausses) produiront des modèles peu fiables, menant à des résultats erronés. Un SIA non testé rigoureusement risque de se tromper fréquemment. Si ces erreurs ne sont pas détectées, elles peuvent induire des mauvaises décisions de la part des utilisateurs finaux qui s'y fient.
- **Interruption du service par absence de robustesse** – Un QIA non robuste peut cesser de fonctionner face à des situations imprévues, provoquant des interruptions du service. Par exemple, un simple caractère non standard dans les données (un accent, un symbole inhabituel) pourrait faire arrêter l'exécution d'un algorithme mal préparé, paralysant l'outil jusqu'à correction. De plus, l'absence de robustesse face à la charge (pics de requêtes) peut rendre le système indisponible lorsqu'il est le plus sollicité, ce qui est particulièrement préjudiciable si l'IA gère des fonctionnalités essentielles.
- **Exploitation malveillante** – Un système peu robuste peut être plus facilement exploité par des acteurs malveillants. Par exemple, s'il est possible de provoquer des comportements anormaux de l'IA en lui fournissant certaines entrées (ce qu'on appelle des *attaques adversariales*, où de légères perturbations de l'entrée induisent une erreur de l'algorithme), alors des individus pourraient intentionnellement exploiter ces failles pour biaiser les résultats d'un SIA à leur avantage.
- **Détection tardive des problèmes** – Sans surveillance continue, vous pourriez découvrir tardivement que le SIA se comporte mal en production. Par exemple, si un bug introduit dans une mise à jour fait chuter la performance de l'IA, et qu'aucune alerte n'est en place, des décisions erronées pourraient s'accumuler pendant des semaines avant qu'on identifie le problème. Les conséquences pourraient alors être massives (grand nombre de dossiers à reprendre).
- **Coûts de maintenance accrus** – Un système non fiable et non suivi impliquera de nombreuses corrections urgentes post-déploiement, des interventions manuelles fréquentes pour rattraper ses erreurs, et *in fine* un coût de maintenance et d'exploitation beaucoup plus élevé que prévu.

Mesures préventives à mettre en œuvre :

- **Qualité des données** – Documenter la provenance et la qualité des données (sources, date de collecte, taux de remplissage des champs…) pour garder la maîtrise.
- **Validation croisée du modèle** – Utiliser des méthodes d'évaluation robuste : validation croisée, jeu de validation séparé, etc., afin de vous assurer que le modèle généralise bien et n'est pas surentraîné (*overfitting*) sur les données d'entraînement. Publier les résultats de performance avec transparence quand le cas d'usage s'y prête, en soulignant les limites.
- **Tests en bac à sable et en pré-production** – Avant le déploiement effectif, tester le SIA dans un environnement bac à sable reproduisant fidèlement le contexte réel (mêmes types de données d'entrée, mêmes intégrations avec d'autres logiciels) pour observer son comportement. Ensuite, faire une phase pilote ou de pré-production avec des utilisateurs réels sur un échantillon limité, afin de recueillir leurs retours et de détecter les derniers problèmes pratiques.
- **Plan de gestion des anomalies** – Définir à l'avance comment le système doit réagir en cas d'anomalie : par exemple, si l'IA renvoie un score de confiance très faible ou une réponse vide, que fait- on ? Préparer des règles métiers de secours (par ex. « si l'IA n'est pas sûre, escalader à un agent humain ») pour éviter les difficultés les plus graves. Incorporer dans le code des limites : seuils de déclenchement d'alerte quand une mesure sort de la normale, exceptions gérées proprement avec des messages explicites.
- **Maintenance et amélioration continue** – Considérer le déploiement initial d'un SIA comme le début d'un cycle d'amélioration continue. Planifier des réévaluations périodiques (par ex. tous les 6 mois) de la qualité et fiabilité du système avec l'équipe projet. Mettre en place un canal de retour utilisateur : les utilisateurs finaux utilisant l'IA doivent pouvoir facilement signaler un résultat incohérent ou une erreur. Chaque retour doit donner lieu à une analyse et, si nécessaire, à une mise à jour du système (nouvel entraînement avec des données corrigées, amélioration de l'interface, etc.). Documenter chaque incident et les corrections apportées.
- **Évaluation rigoureuse du modèle** – Tester le modèle d'IA sur un jeu de test représentatif et selon des métriques diversifiées. Procéder à des tests en conditions réelles simulées : faire fonctionner le SIA sur des scénarios concrets reconstitués de A à Z pour voir comment il s'intègre dans le processus métier (ce qui peut révéler des problèmes d'interface ou de compréhension par l'utilisateur, en plus des problèmes algorithmiques).
- **Robustesse aux données atypiques** – Concevoir l'algorithme et l'interface pour gérer des cas non standards. Par exemple, si une entrée essentielle est manquante (dossier incomplet) ou si une donnée d'entrée est très inhabituelle (valeur extrême, situation jamais vue), le système devrait soit fournir un résultat avec un indicateur d'incertitude, soit basculer vers une procédure alternative, mais en aucun cas produire un résultat aberrant sans avertissement.
- **Résistance aux pannes et erreurs** – S'assurer que le système d'IA, en cas d'erreur logicielle ou de panne partielle, échoue de manière sécurisée (« fail safe »). Par exemple, si un SIA ne répond plus, l'application globale qui l'utilise ne doit pas s'arrêter brutalement : elle pourrait afficher un message d'indisponibilité et orienter l'utilisateur vers une solution alternative. De même, intégrer des *timeouts* et des mécanismes de reprise pour éviter qu'une requête bloquée n'immobilise l'ensemble du système.

Spécificités concernant les IA génératives : Les IA génératives sont notoirement sujettes à la production de corrélations fallacieuses (« hallucinations »), c'est-à-dire qu'elles peuvent produire des informations parfaitement plausibles en apparence mais totalement fausses. Cela soulève de gros enjeux de fiabilité. Par exemple, on a vu des cas où un agent conversationnel juridique a inventé de toutes pièces des références de jurisprudence inexistantes ou attribué à un texte de loi un contenu erroné, induisant en erreur l'utilisateur non averti. En phase de conception, si vous intégrez un modèle génératif, il faut tester systématiquement l'exactitude des réponses qu'il fournit sur un panel de questions métiers. Un taux d'erreur factuelle élevé ne devrait pas être toléré**.** Prévoir une révision et une validation humaine de toutes les sorties génératives importantes avant d'être utilisées dans un contexte réel. De plus, le modèle génératif devrait être enrichi avec des sources fiables : il est possible d'implémenter des mécanismes où le SIA génère une réponse en s'appuyant sur une base documentaire contrôlée pour améliorer la fiabilité. Enfin, concernant la robustesse, une IA générative peut être détournée par des entrées imprévues. Le SIA doit pouvoir refuser les demandes inappropriées (par ex. ne pas fournir de conseil juridique si elle n'en est pas capable de façon fiable, ne pas générer de contenu illégal…), et les comportements-limites doivent être testés en phase de recette.

5. Principe 5 – Pour les systèmes les plus sensibles, produire une documentation exhaustive et garantir la traçabilité des opérations afin de garantir, dans les limites techniques des méthodes employées, explicabilité et transparence

Rappel du principe : Rendre compréhensible le fonctionnement de l'IA, fournir des explications sur les résultats, documenter les algorithmes et données utilisés, et assurer la traçabilité des décisions. En pratique, cela signifie que les concepteurs doivent documenter le système de manière exhaustive, au moins pour les systèmes les plus sensibles, et prévoir des moyens d'explication et de suivi pour que ni les utilisateurs internes ni les usagers externes ne soient confrontés à une « boîte noire ».

Exemples concrets de situations concernées par le principe :

- **Absence ou lacune des documentations techniques et fonctionnelles** – La production de systèmes d'information peuvent parfois souffrir d'une absence de documentation ou d'une rétro-documentation incomplète.
- **Résultats erronés** – Les résultats fournis par l'IA (recommandation par exemple) pourraient paraître crédibles, mais s'appuyer en réalité sur des facteurs erronés.
- **Interactions avec une IA** – En interagissant avec un chatbot juridique, un usager pourrait implicitement croire agir avec un humain.

Risques en cas de non-respect :

- **« Boîte noire » opaque** – Sans transparence ni explicabilité, le SIA devient une boîte noire incompréhensible, Les utilisateurs finaux risquent de l'utiliser de manière inappropriée faute de comprendre son fonctionnement ou son domaine de validité. Les justiciables et usagers pourraient contester des décisions en arguant qu'elles proviennent d'un traitement automatisé les privant d'accès à toute justification. Un manque d'explications pourrait ainsi mener à des recours juridiques accrus et à des annulations de décisions
- **Dépendance et perte de compétence** – Avec un outil opaque, les agents utilisateurs risquent de suivre les recommandations du SIA sans esprit critique, perdant progressivement leur savoir-faire. Cela peut entraîner des erreurs (le SIA pouvant se tromper) et une déqualification des personnels à long terme.
- **Absence de responsabilité claire** – La transparence est liée à la question de la responsabilité. Si personne ne comprend comment le SIA prend ses décisions, qui pourrait être identifié comme responsable en cas d'erreur grave ? L'imputabilité pourrait devenir floue. Sans traçabilité, il sera très difficile d'identifier les causes d'un dysfonctionnement ou d'une décision litigieuse, et donc de corriger ou d'améliorer le système.
- **Perte de confiance** – Un SIA non transparent finira par susciter la défiance des utilisateurs et du public. Dans le domaine de la justice, où la légitimité repose aussi sur la compréhension et l'acceptation des décisions, un outil perçu comme occulte ou arbitraire pourrait être rejeté.
- **Risque d'abus** – L'absence de traçabilité rend possible des usages non conformes et mal intentionnés. Une bonne traçabilité permet de repérer des anomalies ou des usages détournés.

Mesures préventives à mettre en œuvre :

- **Documentation technique et fonctionnelle à jour** – Rédiger un dossier documentaire complet du SIA. Celui-ci comprendra la description de l'algorithme ou du modèle utilisé, l'origine et la nature des données d'entraînement, les paramètres choisis, ainsi que les résultats des évaluations de performance. Par exemple, si vous utilisez un réseau de neurones, précisez-en l'architecture (nombre de couches, type), les données sur lesquelles il a été entraîné (période, source) et les niveaux de précision obtenus sur le jeu de test. En complément de cette documentation technique, produire une documentation pédagogique à destination des utilisateurs finaux expliquant de manière accessible comment fonctionne l'outil, quelles sont ses limites et comment interpréter ses résultats. Cette double documentation (technique et vulgarisée) doit être tenue à jour à chaque nouvelle version du système.
- **Explicabilité des résultats** – Prévoir, dans l'interface utilisateur, des explications sur les résultats fournis par l'IA. Par exemple, si le SIA produit une recommandation, le système devrait pouvoir afficher les facteurs principaux qui ont influencé cette proposition. Cela peut se faire via des techniques d'explicabilité ou tout simplement via une logique métier compréhensible si l'algorithme est plus simple (règles décidables, arbre de décision…).
- **Indication d'utilisation d'une IA** – Informer toujours clairement lorsqu'un contenu ou une décision a été produit (entièrement ou substantiellement) par un SIA. Par exemple, si un justiciable interagit avec un chatbot juridique, mentionner dans l'interface l'absence d'un agent humain. De même, si un rapport ou une décision a été élaboré avec l'aide d'un SIA, s'assurer que ceci soit tracé et signalé. Cette transparence vis-à-vis des usagers est essentielle pour des raisons de confiance et de droit à l'information. Dans certains cas, cela peut être une obligation juridique : par exemple, le RIA prévoit une information de l'utilisateur lorsqu'il interagit avec une IA.
- **Formation des utilisateurs** – Former les utilisateurs à comprendre l'IA. La meilleure explicabilité technique ne sert à rien si les utilisateurs finaux ne savant pas interpréter l'information fournie. Organiser des sessions de formation ou au minimum fournissez un guide utilisateur clair. Expliquer le but de l'outil, son mode de fonctionnement simplifié, comment lire les résultats et explications affichées, quels sont les cas où l'IA peut se tromper, comment réagir en cas de doute, etc. Un utilisateur bien formé est beaucoup plus à même de tirer profit d'un SIA tout en restant vigilant.
- **Indicateurs de confiance** – Fournissez, lorsque c'est pertinent, un indice de confiance ou de fiabilité avec les résultats. Par exemple « l'IA estime à 80% la probabilité d'occurrence de tel événement (fiabilité du modèle : 90%) ». Cela aide l'utilisateur à calibrer son degré de précaution. Si le SIA est incertain, l'humain saura qu'il doit d'autant plus approfondir par lui-même.
- **Registre et auditabilité** – Tenir un registre des SIA en développement ou en production et qualifier leur niveau de risque au regard du RIA. S'assurer que ce registre inclut les cas d'utilisation d'une IA générative ou d'un outil tiers, le tout associé à une analyse de conformité (une fiche par cas d'usage d'IA décrivant risques et mesures). Rendre ce registre disponible en cas de contrôle interne ou externe (CNIL, inspection). Par ailleurs, prévoir pour les systèmes les plus critiques des audits externes périodiques sur la transparence et l'éthique : inviter des experts indépendants à examiner le système, sa documentation, et formuler des recommandations.
- **Communication sur le projet** – En interne comme en externe, communiquer de manière appropriée sur le fonctionnement et l'usage du système d'IA. Par exemple, élaborer une fiche de présentation à destination du grand public expliquant en termes simples l'objectif du SIA,

les données qu'il utilise, et les garanties mises en place (contrôle humain, absence de décision automatique…). Une telle transparence proactive peut désamorcer les méfiances et montrer que le concepteur a agi avec précaution. En interne, partager aussi ces informations avec les représentants du personnel, les instances de gouvernance, afin de bâtir une culture commune autour de l'IA.

Spécificités concernant les IA génératives : Les IA génératives sont souvent vues comme des « boîtes noires » particulièrement opaques car leurs modèles (de type réseau de neurones profonds) sont peu interprétables. De plus, les fournisseurs de services d'IA générative (par ex. entreprises privées) sont parfois peu transparents sur la façon dont leur modèle a été entraîné ou sur les données utilisées. Pour un concepteur du secteur public, il est crucial de compenser ce manque de transparence. S'assurer de documenter précisément l'usage de l'IA générative : quel service ou modèle est utilisé, quelles données lui sont envoyées, quelles mesures de filtrage ou de post-traitement vous appliquez aux contenus générés. Concernant l'explicabilité, noter qu'il existe de nouvelles méthodes pour essayer d'expliquer les sorties d'un grand modèle de langage, mais celles-ci sont encore limitées. Il peut être plus efficace de fournir un cadre de confiance autour de l'IA générative : par exemple, accompagner chaque réponse générée d'un lien vers les sources utilisées (si votre IA va chercher de l'information dans une base juridique, citez les textes ou jurisprudences en appui de la réponse générée). Cela augmente la transparence de la réponse, même si le modèle en lui-même reste complexe. Enfin, prévoir un marquage des contenus générés afin qu'ils soient reconnaissables. Par exemple, insérer automatiquement une mention ou un filigrane dans un document créé par IA pour indiquer son origine. Ainsi, il n'y aura pas d'ambiguïté pour un lecteur quant à la nature du document, ce qui rejoint l'exigence de transparence vis-à-vis des usagers.

6. Principe 6 – Maintenir un contrôle humain à chaque étape critique du processus décisionnel assisté par l'IA

Rappel du principe : Maintenir l'humain au cœur du processus décisionnel, avec la possibilité de valider, modifier ou infirmer les résultats de l'IA. En toutes circonstances, le décideur final doit être un humain. Le SIA ne fait qu'assister ou éclairer la décision, mais ne se substitue jamais à la responsabilité humaine.

Exemples concrets de situations concernées par le principe :

- **Défaut de maîtrise des utilisateurs** – Un assistant virtuel renseigne les citoyens sur des démarches juridiques pourrait fournir des réponses incomplètes ou erronées, sans vérification d'un agent en *back-office* pour éditer ou compléter la réponse avant qu'elle ne soit envoyée ou présence d'une possibilité de feedback des utilisateurs.
- **Formation incomplète des utilisateurs** – Former La formation des utilisateurs pourrait se limiter à des aspects purement fonctionnels, sans développer un esprit critique permettant de prévenir des biais **:** biais d'automatisation (tendance à faire trop confiance à une décision automatisée), biais d'ancrage (une fois qu'une recommandation est donnée, on a du mal à en diverger), biais de confirmation, etc.
- **Approche solutionniste de l'IA** – L'engouement et les possibilités offertes par les SIA pourrait conduire au développement hâtif de solutions, négligeant de conserver un contrôle humain adéquat des processus décisionnels assistés par l'IA.

Risques en cas de non-respect :

- **Automatisation abusive de décisions** – Si le contrôle humain n'est pas effectif, il existe le risque d'une automatisation de fait, contraires aux dispositions du RGPD et de la loi informatique et libertés.
- **Erreurs non détectées** – Un SIA sans supervision peut commettre des erreurs graves qui passeraient inaperçues si aucun humain ne les traite. Le risque est démultiplié si les agents font excessivement confiance à l'outil.
- **Dérive de la finalité de l'outil** – Sans surveillance humaine régulière, un SIA peut progressivement être utilisé hors du cadre prévu, intentionnellement ou non. Par exemple, un outil conçu pour de l'aide à la préparation de décision pourrait, sans contrôle, commencé à être utilisé comme instrument principal de prise de décision.
- **Désengagement et perte de compétence** – Si les agents s'en remettent systématiquement à un SIA sans exercer de contrôle, leurs compétences peuvent s'amoindrir. À terme, un service pourrait perdre sa capacité à fonctionner sans SIA, créant une dépendance risquée. De plus, les agents pourraient se désengager moralement des décisions, en rejetant la faute sur le SIA en cas de problème.
- **Non-conformité juridique** – Des dispositions (en France et en Europe) prohibent dans plusieurs cas les décisions entièrement automatisées sans intervention humaine, notamment lorsqu'elles produisent des effets juridiques sur les individus (art.22 RGPD, art.47 loi informatique et libertés notamment).

Mesures préventives à mettre en œuvre :

- **Intervention humaine décisive** – Aucune décision ayant un impact juridique significatif ne doit être prise par un SIA seul, sans validation humaine. Les résultats doivent être présenté aux utilisateurs finaux comme une recommandation et non comme une conclusion impérative. Les utilisateurs finaux, seuls responsables de leurs fonctions, doivent pouvoir s'en écarter librement.
- **Supervision et audit réguliers** – Organiser le suivi du fonctionnement du SIA en continu et prévoir des points de contrôle humains réguliers. Une instance de gouvernance *ad hoc* devrait recevoir pour mission de passer en revue les performances des SIA, les éventuels incidents ou dérives constatées, et décider de la suspension du système si nécessaire. Des comités d'utilisateurs pourraient aussi être mandatés pour revoir régulièrement les résultats des SIA les plus sensibles.
- **Processus de décision hybride** – Dès la conception, modéliser les processus de travail en intégrant explicitement l'étape de validation humaine. Par exemple, dans le workflow d'une décision assistée par IA, insérer une étape « validation obligatoire par l'utilisateur » avec reformulation explicite de la décision, sans laquelle le processus ne peut se conclure (par exemple par un verrouillage technique). Cela garantit qu'aucune recommandation d'un SIA ne se transforme en décision sans que quelqu'un n'ait validé avec discernement la recommandation.
- **Interface centrée sur l'humain** – Concevoir les interfaces de façon à valoriser la décision humaine. Par exemple, évitez des formulations trop péremptoires ou impératives de la part d'un SIA et utiliser plutôt des tournures conditionnelles. Offrir toujours à l'utilisateur des options claires : accepter, modifier, ou refuser la proposition du SIA. Un champ de justification pourrait être prévu pour que l'humain indique les raisons en cas de divergence avec le SIA, à des fins d'audit et d'apprentissage continu.
- **Limitation des usages de l'IA** – Ne déployer un SIA que dans des cadres où le contrôle humain est matériellement possible. Éviter les scénarios où la décision à prendre est trop rapide ou volumineuse pour qu'un humain vérifie (sinon, c'est que l'IA n'est pas adaptée au contexte). Si le SIA propose de façon récurrente des résultats que l'humain ne fait que valider machinalement par manque de temps, alors il faut soit ralentir le flux, soit revoir l'outil pour qu'il assiste l'humain différemment.
- **Formation continue et sensibilisation** – Former régulièrement les utilisateurs aux bonnes pratiques de l'IA. Insister sur le fait qu'il s'agit d'un outil d'aide et non d'un automate décisionnel. Faire remonter des cas concrets d'erreurs évitées grâce à la vigilance humaine pour illustrer son importance. Mettre en place des rappels (par exemple des info-bulles dans l'interface rappelant de vérifier tel élément). Cette culture du contrôle humain doit être entretenue sur la durée, pas seulement lors du déploiement initial.
- **Mécanismes de retour** – Permettre aux utilisateurs de signaler facilement tout comportement atypique du SIA ou tout cas où ils estiment que l'outil n'est pas fiable. Avoir un point de contact (support) réactif pour traiter ces signalements. De tels dispositifs encourageront les agents à rester attentifs puisqu'ils savent que leur retour sera pris en compte.
- **Responsabilisation** – Rappeler clairement par note ou circulaire que l'utilisation d'un SIA n'exonère pas l'agent de sa responsabilité. Par exemple : « *L'agent restera responsable des décisions prises avec l'aide d'un système algorithmique, au même titre qu'une décision prise sans cet outil.* »

Spécificités concernant les IA génératives : Les IA génératives accentuent la nécessité de contrôle humain car elles peuvent produire du contenu très convaincant en langage naturel. Par exemple, un assistant conversationnel basé sur un modèle de langage pourrait rédiger un document entier avec une apparence de véracité, alors que des erreurs peuvent se dissimuler dans des propos *a priori* vraisemblables. Un texte généré ne doit pas être utilisé sans relecture humaine approfondie. Il est par ailleurs facile pour un utilisateur non formé d'oublier qu'il a affaire à une machine. Les efforts doivent être redoublés pour maintenir l'humain « dans la boucle », par exemple par des alertes dans l'interface (« *Brouillon généré par IA – à vérifier par vos soins* »), par des formations spécifiques sur les limites des IA génératives (« hallucinations, biais », manque de contexte juridique précis), et éventuellement en bridant certaines fonctionnalités de génération automatique tant qu'un utilisateur n'a pas attesté sa compréhension (par ex., obliger une phase d'apprentissage initiale où l'agent valide X exemples avant d'accéder à l'usage libre de l'outil). Enfin, les IA génératives étant souvent généralistes, elles peuvent proposer des solutions qui semblent plausibles mais ne respectent pas exactement la procédure ou le formalisme juridique requis – seul un humain juriste peut s'en apercevoir et rectifier.

7. Principe 7 – Adopter une approche de frugalité numérique et de développement durable dans la conception des systèmes d'IA

Rappel du principe : Adopter une approche sobre en optimisant les algorithmes et l'infrastructure pour limiter l'empreinte environnementale et les coûts, en privilégiant des solutions proportionnées aux besoins réels et évolutives. Il s'agit de développer des IA « à la juste mesure » du besoin à traiter : éviter la surenchère technologique inutile, minimiser la consommation d'énergie et de ressources, et concevoir des systèmes pérennes plutôt qu'éphémères.

Exemples concrets de situations concernées par le principe :

- **Généralisation de l'emploi de modèles complexes** – Pour trier automatiquement des documents juridiques simples par type, mobilisation d'un réseau neuronal complexe.
- **Usages superflus** – Ajout systématique de divers dispositifs (chatbot basé un modèle de langage par exemple) dans des applications ou des sites web.
- **Dépendance à des solutions non maîtrisées** – Emploi de technologies propriétaires et fermées, du fait de leur simplicité et leur commodité apparente.

Risques en cas de non-respect :

- **Modèle simple *versus* modèle complexe** – Avant d'opter pour un modèle très complexe ou un modèle de grande taille, se demander si une solution plus simple ne suffirait pas.
- **Optimisation du code et de l'infrastructure** – Paramétrer et configurer le système dans un souci d'efficacité énergétique. Par exemple, éviter les requêtes redondantes ou mal mises en cache qui sursollicitent les serveurs inutilement. Si l'IA doit effectuer des calculs intensifs, essayer de les planifier aux heures creuses énergétiques (nuits, heures d'excédent d'énergie renouvelable). Utiliser la virtualisation et la mutualisation pour éviter de multiplier les machines sous-exploitées. Si vous utilisez du cloud, choisissez des instances à la demande qui s'arrêtent quand elles ne sont pas utilisées, ou des architectures qui allouent juste les ressources nécessaires.
- **Consommation énergétique et impact carbone** – Un SIA non optimisé peut engendrer une consommation énergétique très importante et donc une empreinte carbone élevée. Par exemple, l'entraînement de grands modèles nécessite des fermes de serveurs énergivores. Même en phase d'inférence (utilisation courante), un modèle de langage très complexe mobilisé pour de nombreuses requêtes quotidiennes peut consommer autant qu'un grand nombre de PC allumés en permanence. À l'heure de l'urgence climatique et de l'exemplarité attendue des services publics, un tel gaspillage d'énergie sera fortement critiqué.
- **Coûts financiers excessifs** – Le manque de frugalité peut se traduire par des coûts budgétaires élevés : facture d'électricité gonflée, nécessité d'acheter du matériel informatique très puissant, coûts de licences logicielles onéreuses ou encore dépenses cloud exponentielles si l'usage n'est pas maîtrisé. Un projet d'IA qui voit trop grand sans maîtrise peut vite dépasser son budget et devenir intenable financièrement pour l'administration.
- **Système surdimensionné et sous-utilisé** – Sans approche sobre, on risque de développer des systèmes surdimensionnés par rapport aux besoins réels, qui resteront sous-utilisés. Par exemple, déployer 10 serveurs GPU pour une IA qui finalement ne traite que quelques requêtes par jour. Cela mobilise inutilement des ressources et augmente la complexité de maintenance.
- **Difficulté d'évolution et obsolescence rapide** – Un système non conçu dans la durée peut

devenir obsolète très vite (technologie propriétaire abandonnée par le fournisseur, incapacité à l'adapter à de nouveaux besoins). Si au contraire le système est pensé dès le départ pour être évolutif, on peut le faire vivre plus longtemps avec des ajustements limités.

- **Multiplication anarchique des projets** – L'absence de mutualisation et de gouvernance peut conduire à la duplication des efforts : plusieurs entités peuvent créer des outils similaires sans se concerter, diluant les compétences et multipliant les dépenses. En plus de l'inefficacité, cela peut poser des problèmes de cohérence (des résultats différents selon l'outil utilisé) et de maintenance (plein de petits projets difficiles à maintenir, faute d'économie d'échelle). Au niveau du ministère, favoriser la mutualisation des projets et ressources. Par exemple, si plusieurs directions envisagent chacune de développer un outil de traitement automatique de la langue pour opérer de la traduction, il est sans doute plus efficient de développer un socle commun que chacun pourra adapter à ses besoins, plutôt que 5 projets distincts redéveloppant la même chose. Cela économisera du temps de calcul (un seul entraînement de modèle au lieu de cinq), de l'énergie et du budget.
- **Conception durable** – Penser à la maintenabilité long terme de l'outil. Par exemple, optez pour des technologies ouvertes et standardisées qui seront encore supportées dans 5-10 ans, afin d'éviter de tout refaire à chaque évolution (ce qui serait du gâchis). Concevez une architecture modulaire, afin que l'on puisse ne remplacer ou améliorer que certains composants sans jeter l'ensemble. Une conception durable, c'est aussi documenter (pour que d'autres équipes puissent reprendre le flambeau) et anticiper les montées en charge futures pour éviter de reconstruire en urgence sous la pression.

Mesures préventives à mettre en œuvre :

- **Évaluation coût/bénéfice** – Dès le lancement d'un projet, réaliser une étude d'opportunité qui met en balance les bénéfices attendus du SIA avec ses coûts (financiers, techniques, environnementaux). Si le rapport coût/bénéfice est défavorable, ne pas hésiter à abandonner ou redimensionner le projet. Par exemple, si l'IA vise à gagner 2% d'efficacité sur une tâche mais qu'elle requiert un investissement massif en serveurs et en données, il peut être plus rationnel de renoncer ou de trouver une autre approche. Formaliser cette analyse pour chaque projet et faire valider par la gouvernance.
- **Optimisation technique** – Optimiser les algorithmes et l'infrastructure pour la sobriété énergétique. Par exemple, choisir des bibliothèques connues pour leur efficacité, utilisez des algorithmes d'entraînement plus frugaux, et suivre la consommation des ressources pendant les tests pour identifier les goulots d'étranglement. Un objectif de performance énergétique peut être fixé, par exemple « traiter X requêtes par seconde avec une machine de tel gabarit, et ne pas dépasser Y kWh par jour en production ». Tester les différentes configurations matérielles pour trouver le meilleur compromis énergie/performance.
- **Mutualisation et synergies** – Éviter la redondance en coordonnant les initiatives. Mettre en place un mécanisme au niveau ministériel pour que les porteurs de projets IA se signalent et partagent leurs travaux. Créer éventuellement des composants réutilisables (modules logiciels communs, bases de données de référence partagées, etc.). Par exemple, une bibliothèque de fonctions d'anonymisation de documents pourrait être développée une fois et utilisée dans plusieurs projets, plutôt que chacun développe la sienne.
- **Suivi de l'impact environnemental** – Intégrez un suivi de l'empreinte écologique du SIA. Par exemple, suivre la consommation CPU/GPU mensuelle et estimer les émissions de CO_2 correspondantes. Sensibiliser les équipes à ces chiffres et afficher dans les rapports : « Ce mois-ci, l'IA a traité X requêtes pour un coût énergétique estimé de Y kWh, soit Z kg de CO_2 ».

Employer des comparaisons simples à comprendre pour encourager à la modération dans l'usage : par exemple « *une seule requête sur un grand modèle de langue peut émettre autant de CO_2 que l'envoi de plusieurs dizaines de courriels* » .

- **Décommissionnement et fin de vie** – Si un SIA s'avère peu concluant ou trop coûteux à maintenir, il faut savoir stopper le projet. Il vaut mieux décommissionner proprement un outil que de le maintenir artificiellement au prix fort. Planifier dès le départ la possibilité de cette fin de vie : comment les données seront archivées ou détruites, comment les utilisateurs seront redirigés vers une autre solution. Par ailleurs, tenir à jour un inventaire des SIA en place et évaluer régulièrement leur utilité. Ceux qui font doublon ou qui n'apportent plus de gain suffisant devraient être fusionnés ou stoppés. Cette gestion de portefeuille évite l'inflation incontrôlée de systèmes coûteux.

Spécificités concernant les IA génératives : Les IA génératives, en particulier les modèles de traitement du langage ou d'images de très grande taille, sont connues pour être très consommatrices en ressources. Leurs phases d'entraînement initial ont une empreinte carbone énorme, et même leur utilisation courante requiert beaucoup de calcul. Ainsi, utiliser un large modèle de langage pour des tâches triviales a un impact non négligeable. Pour les concepteurs, cela implique de bien cibler l'emploi des IA génératives. Par exemple, si l'objectif est de générer des résumés de documents internes, peut-être qu'un modèle de langage de taille moyenne entraîné spécifiquement sur vos documents sera tout aussi efficace qu'un modèle générique géant, pour une consommation bien moindre. Il peut être pertinent de limiter la longueur ou la fréquence des requêtes envoyées à une IA générative (côté interface, brider la génération de très longs textes si ce n'est pas indispensable). Par ailleurs, surveiller l'évolution des technologies : de nouveaux modèles plus efficients émergent régulièrement. Un modèle open-source plus petit et optimisé pourrait remplacer avantageusement un modèle propriétaire gigantesque. Enfin, intégrer la frugalité, c'est aussi sensibiliser les utilisateurs : dans l'interface d'un outil basé sur l'IA générative, on peut par exemple afficher un rappel à une utilisation raisonnée (« *Veuillez n'interroger l'assistant que lorsque nécessaire, et pensez à clôturer la conversation une fois votre réponse obtenue.* »).

8. Principe 8 – Favoriser la collaboration et une gouvernance partagée dans le développement des projets d'IA

Rappel du principe : Favoriser les échanges entre services et institutions, promouvoir l'usage de solutions open source quand c'est possible, et établir une gouvernance claire des projets d'IA. Ce principe promeut une démarche collective et transparente autour de l'IA, afin d'éviter l'isolement des projets, de tirer parti de l'intelligence collective et de garantir la cohérence à l'échelle du ministère.

Exemples concrets de situations concernées par le principe :

- **Développement en silo** – A l'intérieur d'une organisation, laisser se développer des solutions répondant à des besoins identiques au sein de différentes structures.
- **Communiquer de manière trop optimiste sur les apports d'un nouveau système** – La mise en production d'un nouveau système pourrait faire l'objet d'une communication trop optimiste sur ses performances et ses apports.
- **Reposer sur une externalisation trop affirmée** – La très haute technicité des projets IA et les évolutions technologiques rapides pourraient conduire à se reposer sur des entreprises externes, se présentant comme mieux à même de suivre les derniers développements.

Risques en cas de non-respect :

- **Projets en silos et inefficaces** – Sans ouverture ni collaboration, les ressources sont dispersées et le travail doublé. Chaque service pourrait développer son IA de son côté, gaspillant temps et argent, et aboutissant à des solutions redondantes voire incompatibles entre elles.
- **Manque de cohérence et d'interopérabilité** – L'absence de gouvernance commune peut conduire à des systèmes non interopérables (difficiles à faire communiquer entre eux) et à des approches divergentes sur des sujets similaires.
- **Opacité et méfiance** – Un manque d'ouverture externe peut alimenter la méfiance du public ou des professionnels quant aux outils d'IA. Si aucune information n'est donnée, des inquiétudes peuvent émerger. Inversement, communiquer sur l'existence d'une charte utilisateur et de principes directeurs, sur des expérimentations en cours, montre que le ministère agit avec méthode.
- **Dépendance à un fournisseur unique** – Ne pas promouvoir l'open source et la collaboration peut entraîner une dépendance forte vis-à-vis de fournisseurs privés. Si un composant central de votre SIA est propriétaire, vous dépendrez des conditions commerciales et techniques imposées (licences, évolutions non maîtrisées). En cas de défaillance ou de changement de stratégie du fournisseur, vous pourriez vous retrouver bloqué. L'ouverture logicielle réduit ce risque en permettant la reprise du code par la communauté ou par d'autres prestataires.
- **Moins d'innovation** – Isolément, chaque équipe avance lentement et peut manquer d'idées. La collaboration stimule l'**i**nnovation : croiser les regards de juristes, de data scientists, d'utilisateurs terrain, etc., permet de trouver des solutions plus créatives et mieux adaptées. Sans cet esprit d'ouverture, on risque de tourner en rond avec des solutions mal adaptées, tandis que d'autres organisations auront peut-être déjà résolu le problème différemment.
- **Non-alignement avec les standards** – Enfin, ne pas s'ouvrir aux travaux externes (normes, standards, recherches) peut conduire à développer des systèmes non conformes aux standards émergents d'une IA digne de confiance.

Mesures préventives à mettre en œuvre :

- **Politique open source** – Adopter au niveau ministériel une politique encourageant l'open source. Cela peut passer par la création d'une base où publier certains codes, par une clause dans les marchés publics incitant les prestataires à livrer le code source des développements, ou par l'utilisation prioritaire de logiciels libres éprouvés (éviter de réinventer ce qui existe déjà en open source). Former les équipes développement aux bonnes pratiques open source (documentation, licence à choisir, etc.).
- **Structures de pilotage et d'échange** – Établir une structure de haut niveau, sous la forme d'un observatoire, chargée de piloter la stratégie d'intégration, d'assurer un suivi éthique des usages, leur impact sur les métiers, ou encore de garantir une veille scientifique régulière pour actualiser la compréhension de l'IA dans la Justice. Constituer, de plus, une équipe en charge de la conduite opérationnelle de la stratégie IA, sous la forme d'une direction de programme, intégrant les expertises techniques, métier, juridiques et éthiques appliquées à l'IA et dimensionnée en fonction des cas d'usage retenus. Un réseau social interne ou un espace collaboratif dédié aux sujets IA pourrait également être créé, où chacun peut poser des questions, partager un article, demander un retour d'expérience sur un outil.
- **Projets pilotes partagés** – Lancer des projets pilotes multi-acteurs. Par exemple, pour tester une IA d'analyse de texte, associer dès le départ plusieurs juridictions pilotes plutôt qu'une seule, afin de diversifier les points de vue et de créer une dynamique collective. En cas de succès, cela facilitera l'extension du projet à l'échelle nationale car plusieurs acteurs clés y auront déjà contribué.
- **Communication et transparence** – Communiquer de manière mesurée mais réelle sur vos travaux. Publier par exemple un rapport annuel sur l'IA au ministère de la justice, qui ferait état des projets en cours, des résultats obtenus, des difficultés rencontrées et des perspectives. Incluez-y comment la collaboration et l'éthique (via cette charte) sont mises en œuvre. Ce rapport pourrait être public ou au moins partagé avec les parties prenantes (CNIL, Parlement si demandé, etc.). La transparence crée un cercle vertueux de confiance et de soutien.
- **Veille et participation externe** – Encourager les concepteurs et chefs de produit IA du ministère à participer à des travaux externes : groupes de normalisation, conférences, ateliers interministériels, etc. De même, la communauté scientifique organise des conférences sur l'IA et l'éthique : des représentants peuvent être mobilisés pour présenter les projets, pour montrer les progrès du ministère et apprendre des autres initiatives.
- **Gouvernance et pilotage central** – La gouvernance créée (observatoire et direction de programme) devra être dotée d'indicateurs (par ex. % de projets ayant publié leur documentation, % de code mutualisé, etc.) pour mesurer les progrès.

ANNEXE N°4

Stratégie de création d'un Campus du Numérique Justice

1. Contexte et enjeux

Les travaux menés par la mission ont mis en lumière l'ampleur des enjeux liés à la transformation numérique dans les métiers de la Justice. Ils soulignent que le sujet du numérique, déjà structurant, nécessite désormais un accompagnement à la hauteur des défis, d'autant plus que l'arrivée de l'IA en démultiplie la portée et la complexité. Dans ce contexte, la création d'un campus dédié au numérique apparaît comme une réponse stratégique pour mutualiser les ressources, moderniser les pratiques pédagogiques et renforcer les compétences numériques des différents publics relevant de l'ENM, de l'ENG, de l'ENAP et de l'ENPJJ.

L'intégration progressive de solutions fondées sur l'intelligence artificielle constitue par ailleurs un levier essentiel pour actualiser les dispositifs de formation, optimiser l'efficacité des parcours pédagogiques et accompagner l'évolution des compétences requises dans les métiers de la Justice.

Ce projet s'inscrit dans la dynamique initiée au niveau national par le Campus du numérique public, sous l'impulsion de la DINUM, et poursuit l'objectif de créer un espace fédérateur et innovant, propice à la montée en compétences et à l'excellence numérique au sein du ministère.
Il répond à la fois aux besoins de formation initiale et continue, tout en favorisant l'émergence de pratiques pédagogiques innovantes, notamment par l'utilisation d'outils numériques immersifs et interactifs.

Par ailleurs, le campus entend renforcer la coopération entre les écoles et les acteurs du secteur, en s'appuyant sur des méthodes éprouvées pour accélérer la transformation numérique et promouvoir une culture numérique partagée.

Fidèle aux recommandations du rapport rendu par la commission nationale sur l'IA en 2024 « ***IA : Notre ambition pour la France*** », le campus devra se doter d'une mission d'accompagnement forte, en développant des actions de communication ciblées, notamment auprès des publics éloignés ou non-candidats aux formations, et en soutenant activement l'accompagnement au changement.

Ainsi, le campus du numérique Justice entend non seulement former et professionnaliser, mais aussi accompagner durablement la transformation numérique de la Justice, en s'inspirant des meilleures pratiques portées par la DINUM.

2. Objectifs stratégiques

La définition d'objectifs stratégiques clairs constitue une étape essentielle pour structurer le déploiement du Campus du Numérique Justice et garantir la cohérence des actions engagées. Ces objectifs s'articulent autour de trois dimensions complémentaires : le développement des compétences numériques, l'intégration progressive de l'intelligence artificielle dans les pratiques pédagogiques, et la mise en place d'outils et de dispositifs opérationnels adaptés. Cette approche vise à répondre aux besoins actuels et futurs des apprenants, à favoriser l'accessibilité et la mutualisation des ressources, ainsi qu'à instaurer une gouvernance partagée et pérenne.

2.1. Objectifs généraux

- Développer les compétences numériques essentielles des apprenants et des professionnels.
- Proposer des formations accessibles partout et à tout moment.
- Mutualiser les ressources pédagogiques pour optimiser les coûts et la qualité des formations.
- Promouvoir une culture numérique partagée au sein des quatre écoles.

2.2. Objectifs spécifiques liés à l'IA

- **Préparer les apprenants à collaborer avec des technologies basées sur l'IA** dans leurs futures missions.
- **Sensibiliser aux usages et aux limites de l'IA** dans la prise de décision professionnelle.
- **Utiliser l'IA comme outil pédagogique** pour personnaliser les parcours d'apprentissage.
- **Former aux enjeux éthiques et juridiques** de l'intelligence artificielle dans le cadre des métiers de la Justice.

2.3. Objectifs opérationnels

- Identifier une **plateforme numérique centralisée** et ergonomique (envisager la mise en place d'un espace numérique de formation : ENF)
- Concevoir des **contenus pédagogiques innovants** et adaptés aux réalités des métiers.
- Accompagner les **formateurs** dans la transformation de leurs pratiques.
- Mettre en place une **gouvernance partagée** garantissant la pérennité du projet.
- Identifier un **site géographique unique** pour le Campus : le site de l'ENM à Arborial pouvant répondre à cette exigence dans le cadre d'une colocation.

3. Analyse des besoins et du contexte

Avant de déployer toute initiative de formation commune, il est essentiel de bien comprendre la diversité des publics concernés ainsi que leurs besoins spécifiques. Cette analyse vise à dresser un panorama général des profils, des compétences attendues et des contraintes propres à chaque catégorie d'utilisateurs. Elle permet également d'identifier les attentes communes en matière d'accès aux ressources, de flexibilité des formations, de collaboration et de sécurité des données. Il faudra approfondir cette démarche afin que les solutions proposées soient adaptées, efficaces et réellement porteuses de valeur pour l'ensemble des acteurs du campus.

3.1. Typologie des publics

Publics	Compétences numériques attendues	Contraintes
Auditeurs de Justice(ENM)	Acculturation, maîtrise des outils métier	Charges de formation dense
Magistrats	Acculturation, maîtrise des outils métier et expertise dans l'accompagnement à la transformation numérique	Variété des niveaux de compétence Formation sur la base du volontariat
Autres publics non magistrats	Acculturation et expertise dans l'accompagnement à la transformation numérique	Variété des niveaux de compétence
Fonctionnaires de greffe (ENG)	Acculturation, maîtrise des outils métier et expertise dans l'accompagnement à la transformation numérique	Variété des niveaux de compétence
Agents pénitentiaires (ENAP)	Gestion numérique des dossiers des détenus, sécurité informatique	Travail en environnement sécurisé
Éducateurs de la PJJ (ENPJJ)	Outils numériques d'accompagnement éducatif	Terrain souvent éloigné des centres de formation

3.2. État des lieux et attentes

- Besoin d'un accès **simplifié** aux ressources pédagogiques.
- Attente d'une **offre de formation flexible** (asynchrone et synchrone).
- Nécessité d'**outils collaboratifs** pour favoriser les échanges inter-écoles.
- Importance d'une **sécurisation des données** et du respect des normes RGPD.

4. Axes stratégiques et actions clés

Notre stratégie s'articule autour de quatre axes complémentaires et structurants. Le premier axe vise à doter le campus d'une plateforme numérique centralisée, garantissant un accès simple, sécurisé et personnalisé à l'ensemble des ressources et outils pédagogiques. Le deuxième axe porte sur la conception de contenus innovants, interactifs et immersifs, intégrant les dernières avancées en matière d'intelligence artificielle pour enrichir l'expérience d'apprentissage. Le troisième axe place la formation des formateurs et l'accompagnement au changement au cœur du dispositif, afin de permettre à chaque acteur de s'approprier pleinement les nouveaux outils et pratiques. Enfin, le quatrième axe s'attache à structurer une gouvernance efficace, à développer des partenariats stratégiques et à assurer une communication transparente, indispensables pour garantir la qualité, l'éthique et la pérennité de l'ensemble du projet. Ces quatre axes, étroitement liés, constituent le socle d'une démarche ambitieuse et collaborative au service de la réussite du campus numérique.

Axe 1 : Développement d'une plateforme numérique centralisée

Actions clés :

- Sélection d'un **Learning Management System (LMS)** évolutif et interopérable.
- Création d'un **espace utilisateur personnalisé** avec des parcours adaptés à chaque public.
- Intégration d'outils : visioconférence, forums, messagerie, partage de documents.
- Accès aux contenus via ordinateur, tablette et mobile pour garantir la flexibilité.
- Développement de **modules multilingues** si nécessaire (notamment pour les échanges internationaux ou européens).

Livrables attendus :

- Plateforme fonctionnelle et sécurisée.
- Interface intuitive testée par des groupes pilotes.
- Application mobile complémentaire pour un accès en mobilité.

Axe 2 : Conception de contenus pédagogiques innovants

2.1. Actions clés :

- Développement de **modules e-learning interactifs** (vidéos, quiz, serious games).
- Mise en place de **simulations immersives en réalité virtuelle** (reconstitution d'audiences, gestion de crises en milieu pénitentiaire, intervention éducative en situation sensible).
- Création de **ressources sur la cybersécurité, l'éthique numérique et la dématérialisation**.
- Réalisation de **MOOC inter-écoles** sur des thématiques transversales (déontologie, IA Gen, Savoir Prompter, gestion du stress en environnement numérique, etc.).

Exemples de modules :

- **Pour l'ENM :** Simulations de plaidoiries, gestion d'un dossier numérique.
- **Pour l'ENG :** Formation aux logiciels métiers de gestion d'audience.
- **Pour l'ENAP :** Gestion sécurisée des données des détenus.
- **Pour l'ENPJJ :** Utilisation d'outils numériques pour les entretiens avec les mineurs.

2.2. Typologies de modules immersifs - exemples

Type de module	Description	Public cible
Simulations d'audience en réalité virtuelle (RV)	Reconstitution immersive d'un procès avec prise de rôle (juge, greffier, avocat).	ENM, ENG
Gestion de crises en milieu pénitentiaire	Scénarios interactifs pour gérer des situations d'urgence (émeutes, évacuations).	ENAP
Entretiens éducatifs simulés	Simulation d'échanges avec des mineurs en difficulté pour évaluer les bonnes pratiques.	ENPJJ
Modules de cybersécurité	Jeux de rôle numériques pour identifier les menaces et sécuriser les données.	Tous publics
Serious games sur la déontologie	Scénarios où les apprenants doivent faire des choix éthiques dans leur pratique professionnelle.	Tous publics

2.3. Méthodologie de conception

Étape 1 : Analyse des besoins pédagogiques

- Entretiens avec des formateurs et des professionnels pour identifier les situations clés à simuler.
- Recueil des attentes des apprenants via des enquêtes.

Étape 2 : Scénarisation des modules

- Rédaction de **scénarios interactifs** avec plusieurs branches narratives selon les décisions prises.
- Collaboration avec des experts métiers pour garantir le réalisme.

Étape 3 : Développement technologique

- Utilisation de **logiciels de RV/RA** (Unity, Unreal Engine) pour les environnements 3D.
- Intégration de **voix off interactives** et d'effets sonores pour renforcer l'immersion.
- Accessibilité via casques de RV, mais aussi en mode simplifié sur ordinateur/tablette.

Étape 4 : Phase de test et d'ajustement

- Groupes pilotes avec des élèves et des formateurs.
- Recueil des feedbacks pour améliorer la fluidité et la pertinence des scénarios.

Étape 5 : Déploiement et accompagnement

- Mise en ligne sur la plateforme du Campus.
- Formation des formateurs à l'utilisation des modules immersifs.
- Sessions d'accompagnement pour les utilisateurs novices en RV.

2.4. Exemples concrets de modules immersifs

1. Module "Audience pénale en RV" (ENM, ENG)

- L'apprenant endosse le rôle d'un magistrat, d'un greffier ou d'un avocat.
- Il interagit avec des personnages virtuels (prévenus, témoins, procureurs).
- Objectifs : apprendre à gérer le déroulement d'une audience, prendre des décisions en temps réel.

2. Module "Gestion de crise en prison" (ENAP)

- Simulation d'une émeute dans un établissement pénitentiaire.
- L'apprenant doit coordonner les équipes, sécuriser les détenus et préserver l'ordre.
- Retour d'évaluation sur la prise de décision sous pression.

3. Module "Entretien éducatif avec un mineur" (ENPJJ)

- Mise en situation d'un éducateur face à un jeune en difficulté.
- Différents choix d'approches sont proposés, avec des conséquences sur l'évolution de l'entretien.
- Objectif : développer l'écoute active et l'adaptation aux besoins du jeune.

2.5. Développement de modules immersifs avec l'IA

2.5.1. Nouveaux modules dédiés à l'IA

Module	Description	Public cible	Compétences développées
Initiation à l'IA et ses enjeux dans la Justice	Cours interactif expliquant le fonctionnement de l'IA, ses applications et ses limites.	Tous les publics	Compréhension des bases de l'IA et de son impact sur la Justice. Apprentissage de l'intégration de l'IA dans la pratique professionnelle quotidienne
Cycle approfondi du numérique et de l'IA	Cours interactif niveau avancé	Tous les publics	Niveau avancé et accompagnement de la conduite du changement
Simulations de décisions assistées par IA	Mise en situation où l'apprenant évalue les recommandations d'un système d'IA dans des cas juridiques ou pénitentiaires.	ENM, ENG, ENAP	Prise de décision critique face à des suggestions générées par IA.
IA et cybersécurité	Modules sur l'utilisation de l'IA pour prévenir les cybermenaces et protéger les données sensibles.	Tous les publics	Maîtrise des enjeux de cybersécurité et utilisation d'outils IA.
Déontologie et éthique de l'IA	Scénarios immersifs où l'apprenant doit identifier des biais algorithmiques et résoudre des dilemmes éthiques.	Tous les publics	Sensibilisation aux biais et respect des principes éthiques.

2.5.2. Utilisation de l'IA dans les outils pédagogiques

- **Chatbots d'assistance** : accompagnement des apprenants 24/7 avec des réponses personnalisées.
- **Analyse prédictive** : recommandations de contenus adaptés au rythme d'apprentissage de chacun.
- **Correction automatisée** : évaluation instantanée des exercices avec des feedbacks détaillés.

Axe 3 : Formation des formateurs et accompagnement au changement

L'Axe 3 vise ainsi à placer la formation des formateurs et l'accompagnement au changement au cœur de la stratégie de développement du campus. Il s'agit de doter les équipes pédagogiques des compétences nécessaires pour exploiter pleinement le potentiel du numérique et de l'intelligence artificielle, tout en favorisant une dynamique collaborative et un partage des bonnes pratiques. Cet axe entend également instaurer un environnement d'entraide, afin de garantir une évolution durable des pratiques éducatives.

Actions clés :

- Organisation d'ateliers pour **monter en compétence les formateurs** sur les outils numériques et sur les outils d'IA.
- Mise en place d'un **réseau de référents-ambassadeurs numériques** dans chaque école.
- Élaboration de guides pratiques et tutoriels vidéo.
- Création d'un **centre d'assistance technique et pédagogique** disponible en continu.
- Organisation de **séminaires ou d'évènements** afin de contribuer à la diffusion des connaissances et au rayonnement du campus

Indicateurs de succès :

- Pourcentage de formateurs formés.
- Satisfaction des apprenants concernant les outils numériques.
- Taux d'utilisation des ressources mises à disposition.

Axe 4 : Gouvernance, partenariats et communication

Actions clés :

- Création d'un **comité de pilotage inter-écoles** pour assurer le suivi et la coordination.
- Création d'un comité d'experts pour adapter les formations aux évolutions technologiques (en lien avec le Lab IA Innovation)
- Création d'un comité éthique et pédagogique de l'IA : chargé notamment de la rédaction de la Charte éthique partagée entre les 4 écoles
- Identification de **partenaires stratégiques** :
- Acteurs publics : DINUM, CNIL, Ministère de la Justice
- Acteurs privés : entreprises EdTech, start-ups innovantes.
- Partenariats avec des universités pour la recherche sur la pédagogie numérique et les avancées en IA et cybersécurité
- Élaboration d'un **plan de communication** pour informer et mobiliser l'ensemble des parties prenantes.

Pour assurer le développement efficace, éthique et innovant des modules liés à l'IA, le **Campus du Numérique** doit s'appuyer sur des **partenariats stratégiques** avec des acteurs publics, privés, académiques et institutionnels. Ces collaborations permettront de mutualiser les compétences, d'accéder aux dernières technologies et de garantir la qualité des formations proposées.

1. Partenaires institutionnels et gouvernementaux

1.1. Ministères et agences nationales

- **Ministère de la Justice** : pour assurer la cohérence avec les politiques publiques et les besoins du terrain.
- **DINUM (Direction Interministérielle du Numérique)** : accompagnement sur l'architecture numérique et la cybersécurité.
- **CNIL (Commission Nationale de l'Informatique et des Libertés)** : conseils sur la protection des données et la conformité RGPD.
- **INRIA (Institut National de Recherche en Informatique et en Automatique)** : expertise technique et accès à des chercheurs en IA.
- **IERDJ** (Institut des études et de la recherche sur le droit et la Justice)
- **REFJ** (Réseau Européen de Formation Judiciaire).

1.2. Institutions européennes

- **Commission européenne – Programme Digital Europe** : financement de projets liés à l'IA dans la formation.
- **Conseil de l'Europe – Commission de l'éthique de l'IA** : accompagnement sur les enjeux éthiques et déontologiques.

2. Exemples de partenaires académiques

Établissement	Type de partenariat	Bénéfices attendus
Collège de France – Chaire IA	Collaboration sur des contenus pédagogiques liés à l'éthique de l'IA.	Modules de qualité basés sur la recherche académique de pointe.
Université PSL (Paris Sciences & Lettres)	Développement conjoint de serious games immersifs avec l'IA.	Accès à des chercheurs et étudiants pour co-construire les modules.
Sorbonne Université – Laboratoire d'informatique de Paris 6	Partage de compétences sur les algorithmes et la cybersécurité.	Intégration de technologies fiables et sécurisées.
École Polytechnique & Institut Polytechnique de Paris	Création de simulateurs IA pour les formations des magistrats et éducateurs.	Outils immersifs réalistes et scientifiquement validés

3. Partenaires technologiques et industriels

3.1. Entreprises technologiques françaises

- Entreprise A : expertise en cybersécurité et intelligence artificielle sécurisée pour les institutions publiques
- Entreprise B : solutions immersives en 3D pour la formation professionnelle
- Entreprise C : intégration de plateformes cloud sécurisées pour héberger les modules d'IA
- Entreprise D : accompagnement sur la modélisation des scénarios immersifs et leur développement.

3.2. Startups et PME spécialisées en EdTech

- Startup/PME E : personnalisation des parcours d'apprentissage par l'IA
- Startup/PME F : développement de serious games et de modules immersifs pour la formation
- Startup/PME G : IA adaptative pour le suivi et la recommandation de contenus pédagogiques.

4. Partenaires associatifs et ONG

- Association H Veille sur les questions de libertés numériques
- Association I Participation à des événements et groupes de travail
- Association J Ateliers sur la confiance dans les systèmes IA

5. Gouvernance des partenariats

Pour assurer la **bonne coordination** et la **pérennité des partenariats**, il est recommandé de mettre en place principalement entre les 4 écoles Justice :

- **Un comité stratégique des partenaires**, réunissant les acteurs clés pour définir les grandes orientations.
- **Des groupes de travail opérationnels**, pour piloter le développement des modules IA.
- **Des conventions de partenariat** précisant les rôles, responsabilités et droits de propriété intellectuelle.
- **Un dispositif d'évaluation et de suivi**, avec des indicateurs de performance partagés.