



Guide des usages de l'IA dans les services support et les activités administratives

Sommaire

I. Introduction et objectifs du guide	3
II. Principes d'usage de l'intelligence artificielle dans les services support et les activités administratives	4
1. Responsabilité humaine dans les processus administratifs	4
2. Transparence et explicabilité des usages	4
3. Maîtrise des outils et vigilance critique	4
III. Protection des données, confidentialité et cadre juridique applicable	5
IV. Règles d'usage institutionnel	5
V. Gouvernance et validation des outils	5
VI. Gestion des risques et incidents	5
VII. Articulation avec les volets Formation et Recherche	5
VIII. Accompagnement, formation et partage des pratiques	6

Guide des usages de l'IA dans les services support et les activités administratives

I. Introduction et objectifs du guide

L'intelligence artificielle transforme profondément les pratiques administratives, organisationnelles et les fonctions support des établissements d'enseignement supérieur et de recherche.

Les systèmes d'intelligence artificielle, et en particulier les outils d'intelligence artificielle générative, ouvrent de nouvelles possibilités :

- d'assistance à la rédaction ;
- d'analyse documentaire ;
- de traitement et de synthèse de l'information ;
- d'aide au pilotage ;
- d'automatisation partielle de certaines tâches administratives.

Leur développement s'inscrit dans une évolution plus large des environnements numériques de travail, des systèmes d'information et des modalités d'organisation des activités universitaires.

L'intégration de ces technologies peut contribuer à améliorer la qualité du service public universitaire, la fiabilité des traitements, l'efficacité organisationnelle ainsi que l'accompagnement des missions de formation et de recherche.

Elle soulève toutefois des enjeux majeurs en matière :

- de responsabilité administrative ;
- de protection des données ;
- de confidentialité ;
- de sécurité des systèmes d'information ;
- de conformité réglementaire ;
- de souveraineté numérique ;
- de maîtrise des risques juridiques, organisationnels et informationnels.

Les systèmes d'intelligence artificielle ne sauraient se substituer à la responsabilité humaine dans les processus administratifs, financiers, juridiques ou organisationnels de l'établissement.

Leur usage implique au contraire une vigilance renforcée, une maîtrise des données et des infrastructures mobilisées, ainsi qu'une capacité permanente de vérification, d'analyse critique et de contrôle humain des traitements réalisés.

Dans ce contexte, le présent guide a pour objet d'accompagner les usages professionnels et institutionnels de l'intelligence artificielle au sein des services support et des activités administratives de l'Université Paris 8.

Il vise notamment à :

- encadrer les usages institutionnels de l'intelligence artificielle ;
- préciser les responsabilités associées à ces usages ;
- garantir un niveau de sécurité et de conformité adapté aux missions de l'établissement ;
- assurer la protection des données et la maîtrise des risques ;
- favoriser des pratiques responsables, proportionnées et compatibles avec les exigences du service public universitaire.

Le présent guide s'applique aux usages institutionnels et professionnels de l'intelligence artificielle au sein des services support et des activités administratives de l'Université Paris 8, notamment au sein :

- de la Direction des Systèmes d'Information et du Numérique ;
- des services juridiques ;
- des ressources humaines ;
- des services financiers ;
- des services de scolarité ;
- des services de recherche et de valorisation ;
- de l'ensemble des directions et services administratifs de l'établissement.

Les usages strictement personnels, sans lien avec les missions de l'Université, ne relèvent pas du périmètre du présent document.

Le présent guide s'inscrit dans le prolongement de la Charte des usages de l'intelligence artificielle de l'Université Paris 8 et en décline les principes dans le champ des activités administratives et organisationnelles. Il s'applique sans préjudice des obligations résultant notamment :

- du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD) ;
- du Code des relations entre le public et l'administration ;
- du Code du patrimoine ;
- du Code de la propriété intellectuelle ;
- des politiques de sécurité des systèmes d'information applicables à l'établissement ;
- des règles internes de l'Université Paris 8.

II. Principes d'usage de l'intelligence artificielle dans les services support et les activités administratives

Les principes suivants déclinent les principes directeurs communs de la Charte des usages de l'intelligence artificielle de l'Université Paris 8 dans le champ des activités administratives, organisationnelles et des fonctions support.

Ils visent à garantir un usage de l'intelligence artificielle conforme aux exigences du service public universitaire, notamment en matière de responsabilité, de transparence, de sécurité juridique, de protection des données et de protection des usagers.

1. Responsabilité humaine dans les processus administratifs

L'usage de systèmes d'intelligence artificielle dans les activités administratives ne modifie pas la responsabilité des agents et des services.

Les agents demeurent pleinement responsables :

- des données utilisées et de leur licéité ;
- des contenus produits dans un cadre professionnel ;
- des décisions prises sur la base des résultats issus de ces outils ;
- de la vérification, de la validation et, le cas échéant, de la correction des informations produites.

Le recours à un système d'intelligence artificielle ne saurait exonérer l'utilisateur de sa responsabilité, ni être interprété comme un transfert de responsabilité ou de paternité vers le système.

Aucune décision administrative, financière, juridique ou organisationnelle ne peut être entièrement automatisée sans contrôle humain effectif, adapté et documenté.

Les systèmes d'intelligence artificielle doivent demeurer des outils d'assistance à la décision et ne peuvent se substituer à l'appréciation, au discernement et à la responsabilité des agents et des services.

2. Transparence et explicabilité des usages

Le recours à l'intelligence artificielle dans un processus administratif, organisationnel ou décisionnel doit pouvoir être identifié, expliqué et documenté.

Cette exigence implique notamment :

- la capacité à justifier le recours à ces outils ;
- la conservation des éléments permettant de comprendre les processus de production ;
- la possibilité d'identifier les contenus générés ou assistés par un système d'intelligence artificielle lorsque cela est nécessaire ;
- l'information des usagers lorsqu'un traitement algorithmique contribue de manière significative à une décision les concernant.

Ces principes participent à la confiance dans l'action administrative et à la conformité aux exigences réglementaires applicables aux établissements publics.

3. Maîtrise des outils et vigilance critique

Les agents doivent exercer une vigilance particulière quant aux limites des systèmes d'intelligence artificielle.

Cette vigilance est notamment nécessaire en raison :

- des risques d'erreurs ou d'informations inexactes ;
- des biais potentiels ;
- des phénomènes d'hallucination ;
- de l'absence de compréhension réelle des situations par les systèmes utilisés ;
- des limites des modèles en matière de contextualisation et d'interprétation.

Aucun contenu généré ne peut être utilisé sans vérification préalable adaptée à son niveau de sensibilité, en particulier lorsqu'il contribue :

- à une décision administrative ;
- à une communication institutionnelle ;
- à une analyse juridique ou financière ;
- à un traitement impliquant des données personnelles ou sensibles.

Les agents doivent veiller à conserver une distance critique vis-à-vis des résultats produits par les systèmes d'intelligence artificielle et à ne pas considérer ces technologies comme neutres, objectives ou infaillibles.

III. Protection des données, confidentialité et cadre juridique applicable

Les informations saisies par l'utilisateur dans un système d'intelligence artificielle (instructions, questions, documents, images, données structurées ou non structurées) sont, dans la plupart des cas, transmises au fournisseur du service. Elles peuvent être conservées, analysées ou réutilisées pour l'amélioration des modèles.

Cette situation peut entraîner :

- une violation des obligations relatives à la protection des données à caractère personnel au sens du Règlement (UE) 2016/679 du 27 avril 2016 (RGPD), notamment des principes de licéité, de minimisation des données (article 5), de sécurité du traitement (article 32) et des règles relatives aux transferts hors Union européenne (articles 44 et suivants) ;
- une atteinte aux droits de propriété intellectuelle régis par le Code de la propriété intellectuelle ;
- la divulgation involontaire d'informations confidentielles, contractuelles ou stratégiques.

En l'état actuel des outils disponibles, le niveau de protection des données transmises n'est pas toujours vérifiable. Les données peuvent être hébergées sur des serveurs situés hors de l'Union européenne, conservées pour réentraînement ou réapparaître indirectement dans des réponses produites pour d'autres utilisateurs.

La transmission d'un document administratif à un service d'IA privé peut juridiquement être analysée comme une communication à un tiers.

En application :

- des articles L.311-1 à D.312-11 du Code des relations entre le public et l'administration relatifs à la communication des documents administratifs ;
- des articles L.213-1 à L.213-8 du Code du patrimoine relatifs aux archives publiques ;
- et notamment de l'article L.213-2 du Code du patrimoine fixant les délais de communicabilité ;
- Les documents transmis en entrée et ceux générés en sortie dans le cadre d'une mission de service public peuvent être qualifiés d'archives publiques et soumis aux obligations légales de conservation, de communicabilité et de protection.

Il en résulte que, sauf usage d'une infrastructure institutionnelle validée et sécurisée, ne doivent être saisis dans un outil d'intelligence artificielle externe que des contenus pouvant être rendus publics sans restriction.

Les principes relatifs aux catégories de données, aux niveaux de sensibilité, aux conditions de recours aux différentes solutions d'intelligence artificielle ainsi qu'aux exigences de sécurité, de confidentialité et de validation institutionnelle des environnements techniques sont précisés dans le guide « *Données, outils et usages des systèmes d'intelligence artificielle* ».

IV. Règles d'usage institutionnel

Indépendamment du choix des infrastructures et des catégories de données traitées, l'usage institutionnel d'un outil d'intelligence artificielle doit respecter les règles suivantes :

- Ne pas automatiser une prise de décision administrative, financière, juridique ou organisationnelle sans contrôle humain effectif et documenté.
- Informer les usagers lorsqu'un traitement algorithmique intervient de manière significative dans un processus les concernant.
- Ne pas imposer à des étudiants ou à des agents l'usage d'un service d'intelligence artificielle grand public nécessitant la création d'un compte personnel ou l'acceptation de conditions générales non maîtrisées par l'établissement.
- Vérifier systématiquement l'exactitude, la pertinence et la conformité des contenus produits avant toute diffusion interne ou externe.
- S'assurer que l'usage de l'outil est proportionné à l'objectif poursuivi, au regard notamment de son impact environnemental et des risques associés.

Ces règles visent à encadrer les usages de l'intelligence artificielle au-delà des seules dimensions techniques liées aux infrastructures, aux outils et aux données. Elles participent également à la protection des droits des personnes, à la préservation des principes d'équité, de transparence et de responsabilité, ainsi qu'au respect des exigences réglementaires et institutionnelles applicables.

Les usages susceptibles d'affecter de manière significative les droits des personnes, l'accès à une formation, les modalités d'évaluation, l'orientation, le recrutement, la gestion des personnels, l'accès à un service ou la situation

administrative d'un usager ou d'un agent doivent faire l'objet d'une analyse préalable renforcée.

De tels usages ne peuvent être déployés qu'après consultation des services et référents institutionnels compétents mentionnés dans la section suivante. Lorsque des données personnelles sont concernées, le référent Protection des données (DPO) doit être associé à l'analyse. Le cas échéant, une analyse d'impact relative à la protection des données ainsi qu'une évaluation spécifique au regard du règlement européen sur l'intelligence artificielle (« AI Act ») doivent être réalisées.

V. Gouvernance et validation des outils

L'usage institutionnel d'un outil d'intelligence artificielle doit faire l'objet d'une évaluation préalable lorsqu'il :

- traite des données internes ;
- intervient dans un processus décisionnel ;
- implique des données personnelles ;
- est intégré à un système d'information institutionnel.

Cette évaluation associe :

- la **Direction des Systèmes d'Information et du Numérique (DSIN)** de l'établissement, pour les questions de sécurité technique, d'hébergement et de conformité des environnements numériques ;
- le **référént Sécurité des Systèmes d'Information (RSSI)** de l'établissement, pour les questions relatives à la Politique de sécurité des systèmes d'information (PSSI) ;
- le **référént Protection des Données (DPO)** de l'établissement, pour les questions relatives au RGPD, aux données sensibles et à la protection des données personnelles ;
- le **Service Juridique** de l'établissement, pour l'analyse des conditions d'utilisation des outils, des clauses contractuelles et des questions réglementaires ;

VI. Gestion des risques et incidents

Dans le prolongement des principes de responsabilité et de protection des données exposés précédemment, tout usage institutionnel d'un outil d'intelligence artificielle doit s'inscrire dans une démarche de maîtrise des risques.

Tout incident lié à l'usage d'un système d'IA doit être signalé sans délai aux services compétents, notamment en cas :

- de fuite ou de suspicion de fuite de données ;
- d'atteinte à la confidentialité ;
- d'erreur substantielle ayant un impact administratif, financier ou juridique ;
- de violation ou suspicion de violation de données à caractère personnel.

Les usages doivent être compatibles avec :

- la politique de sécurité des systèmes d'information de l'établissement ;

- les procédures internes de gestion des incidents ;
- les obligations légales de notification prévues par le RGPD.

Cette vigilance contribue à la sécurisation juridique et organisationnelle des usages de l'intelligence artificielle au sein de l'établissement.

VII. Articulation avec les volets

Formation et Recherche

Les services support ont pour mission d'encadrer et de sécuriser les usages institutionnels de l'intelligence artificielle dans leurs dimensions techniques, juridiques et organisationnelles.

L'appréciation scientifique des contenus de recherche ainsi que l'évaluation pédagogique des productions des étudiants relèvent des instances et équipes académiques compétentes. Les services support interviennent en appui, dans leurs domaines d'expertise, afin de garantir un cadre sécurisé et conforme aux exigences réglementaires.

Dans cette perspective, ils accompagnent les équipes de formation et de recherche notamment pour :

- le choix d'infrastructures adaptées au niveau de sensibilité des données ;
- l'analyse des risques juridiques et contractuels ;
- la conformité au cadre applicable en matière de protection des données ;
- la sécurisation des partenariats et des dispositifs mobilisant des outils d'IA ;
- le respect des exigences réglementaires et institutionnelles.

Cette articulation vise à assurer une complémentarité des responsabilités : aux équipes académiques la conduite scientifique et pédagogique des projets ; aux services support la sécurisation technique, juridique et organisationnelle des usages.

VIII. Accompagnement, formation et partage des pratiques

L'Université Paris 8 s'engage à accompagner les personnels administratifs et les services support dans la compréhension, l'encadrement et la maîtrise des usages de l'intelligence artificielle dans les activités administratives, organisationnelles et de gestion de l'établissement.

Cet accompagnement vise à développer des pratiques professionnelles responsables, sécurisées et adaptées aux exigences du service public universitaire, notamment en matière de protection des données, de confidentialité, de sécurité des systèmes d'information, de conformité réglementaire et de maîtrise des risques liés à l'usage des outils d'intelligence artificielle.

Il concerne en particulier la compréhension des limites des systèmes d'intelligence artificielle, les risques liés à la transmission et à la réutilisation des données,

les biais, les règles de confidentialité, les réflexes de vérification humaine, les procédures de signalement, les obligations applicables en matière de protection des données et les conditions d'usage des outils et infrastructures validés par l'établissement.

L'Université encourage également le partage des pratiques et des retours d'expérience entre services, la mutualisation des ressources et le développement d'une culture commune de vigilance et de maîtrise des usages numériques dans les activités administratives et les fonctions support.

