



ASIN

AGENCE DES SYSTÈMES
D'INFORMATION ET DU
NUMÉRIQUE

RÉPUBLIQUE DU BÉNIN

BILLET JURIDIQUE SUR L'USAGE DES OUTILS D'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE PAR LES AGENTS PUBLICS AU SEIN DE L'ADMINISTRATION



“

Le développement des usages de l'intelligence artificielle générative par les agents publics, souvent en dehors de tout cadre institutionnel formalisé, impose une attention accrue aux exigences de protection des données personnelles, de confidentialité des informations sensibles, de sécurité des infrastructures numériques et de préservation de la souveraineté numérique de l'État.

”

Il est désormais établi qu'un nombre croissant d'agents publics recourent, à titre personnel et sans encadrement formalisé, à des outils d'intelligence artificielle générative dans l'accomplissement de leurs missions quotidiennes. De telles pratiques, en l'absence de cadre sécurisé et approprié, soulèvent des enjeux juridiques majeurs, portant principalement sur la protection des données personnelles, la souveraineté numérique, la confidentialité des informations stratégiques, la sécurité des systèmes et infrastructures ainsi que la dépendance technologique.

Dans ce contexte, l'analyse met en évidence que ces risques, bien que significatifs, peuvent être maîtrisés à condition de mettre en œuvre un cadre rigoureux de gouvernance et de conformité, structuré autour de plusieurs axes complémentaires qui oscillent entre :

➤ **Des mesures immédiates**

Elles consistent notamment en la cartographie des divers usages de l'IA au sein de l'administration ; le recensement des collaborateurs utilisant des outils d'intelligence artificielle au moyen de comptes personnels afin d'organiser leur migration vers un dispositif sécurisé ; la limitation, voire la suspension encadrée, des usages non autorisés ; la souscription à des offres professionnelles permettant de bénéficier de garanties contractuelles renforcées en matière de protection des données ; ainsi que l'adoption de charte harmonisée contraignante encadrant l'utilisation des outils d'intelligence artificielle dans l'exercice des fonctions publiques, y compris les rôles et responsabilités de chaque acteur impliqué (collaborateurs, prestataires et partenaires, etc.) ;

➤ **Un encadrement contractuel strict des prestataires externes**

L'encadrement contractuel repose sur la signature d'un accord de traitement de données personnelles. À cela s'ajoutent des clauses spécifiques interdisant toute utilisation des données à des fins d'entraînement ou d'optimisation de modèles d'IA, la conclusion d'accords de confidentialité (NDA), l'intégration de mécanismes de réversibilité et de restitution complète des données, ainsi que l'interdiction de tout transfert vers des juridictions extraterritoriales, notamment celles soumises au Cloud Act ou au FISA. Enfin, des garanties contractuelles doivent assurer un niveau de protection équivalent aux exigences du droit béninois en matière de transferts internationaux de données ;

➤ *Une conformité aux exigences légales*

Cela implique d'une part, la réalisation d'une Analyse d'Impact relative à la Protection des Données (AIPD), en raison de la sensibilité des données traitées et de l'introduction d'une nouvelle technologie basée sur l'IA, afin d'identifier en amont les risques pour les droits et libertés des personnes concernées, d'en évaluer la gravité et la probabilité, et de définir des mesures d'atténuation appropriées. D'autre part, elle suppose la déclaration des traitements à l'Autorité de Protection des Données Personnelles (APDP), la mise en œuvre de mécanismes de pseudonymisation ou d'anonymisation des données sensibles avant tout traitement, le respect du principe de minimisation, la limitation des traitements aux finalités déterminées, la définition de durées de conservation, ainsi que, le cas échéant, le recueil du consentement des personnes concernées ;

➤ *Le déploiement de mesures techniques et de sécurité robustes*

Il inclut notamment (a) de privilégier un hébergement souverain des données sur des infrastructures localisées sur le territoire national ou présentant un niveau de protection équivalent, (b) de garantir le chiffrement intégral des données, tant au repos qu'en transit, et (c) d'exiger des prestataires le respect des normes internationales pertinentes, telles que ISO/IEC 27001 (sécurité des systèmes d'information), ISO/IEC 27701 (protection des données personnelles) et ISO/IEC 42001 (gouvernance de l'IA) ;

➤ *L'implémentation de mesures organisationnelles et opérationnelles*

Les mesures organisationnelles et opérationnelles consistent notamment en la réalisation d'audits périodiques des systèmes d'IA, ainsi qu'en la diversification des prestataires pour réduire le risque de dépendance technologique (« vendor lock-in »).

Par ailleurs, dans l'hypothèse du développement de modèles d'IA propres à l'administration, une vigilance particulière doit être accordée à la qualité des données d'entraînement, afin de prévenir la diffusion d'informations erronées, ainsi qu'à l'intégration du principe d'« ethics by design », en vue de limiter les biais algorithmiques.

En définitive, l'usage ou le déploiement de solutions d'intelligence artificielle dans les administrations apparaît juridiquement envisageable, sous réserve du respect strict des mesures recommandées et d'un encadrement effectif des usages par les agents. Néanmoins, des risques résiduels subsistent, notamment en matière de souveraineté numérique et de dépendance technologique, ce qui implique que toute décision de déploiement opérationnel soit prise en pleine connaissance de ces enjeux, dans une logique de gestion maîtrisée des risques et sous contrôle institutionnel renforcé.

Suivez-nous sur nos canaux digitaux



@asinbenin