



ASIN

AGENCE DES SYSTÈMES
D'INFORMATION ET DU
NUMÉRIQUE

RÉPUBLIQUE DU BÉNIN

BILLET JURIDIQUE SUR LA CONFORMITÉ JURIDIQUE, UNE CONDITION DE RÉUSSITE DU DÉPLOIEMENT DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE



“

L'intelligence artificielle (IA) s'impose progressivement comme un levier majeur de transformation des administrations publiques et des entreprises privées. Elle constitue sans nulle doute un facteur de performance et d'innovation en automatisant les processus, en améliorant l'aide à la décision et en optimisant la gestion des données. Toutefois, son intégration ne relève plus uniquement d'un choix technologique ; c'est désormais un véritable enjeu de conformité juridique.

”

Le déploiement d'un système d'IA soulève en effet des questions complexes relatives à la protection des données à caractère personnel, à la propriété intellectuelle, à la cybersécurité, à la responsabilité civile, à la transparence des algorithmes et au respect de la dignité de l'homme et des droits fondamentaux. L'entrée en vigueur du Règlement européen sur l'intelligence artificielle (AI Act) traduit cette évolution vers un encadrement juridique plus structuré de l'IA. Ce texte offre un cadre de référence utile pour mieux appréhender la gouvernance des systèmes d'intelligence artificielle.

L'AI Act repose sur une approche graduée, proportionnée et fondée sur les risques. En effet, les systèmes d'IA sont classés selon le niveau de risque qu'ils présentent pour les personnes et la société. Il distingue principalement quatre niveaux : les pratiques présentant un risque inacceptable, les systèmes d'IA à haut risque, les systèmes soumis à des obligations de transparence en raison d'un risque limité et les systèmes présentant un risque minimal ou nul.



Les pratiques à risque inacceptable correspondent aux usages considérés comme incompatibles avec la protection des droits fondamentaux, tels que certaines pratiques de manipulation ou d'exploitation des vulnérabilités, le « social scoring » ou certaines formes de catégorisation et d'identification biométriques. Les systèmes à haut risque concernent notamment certains usages susceptibles d'avoir une incidence importante sur les personnes dans des domaines tels que l'emploi ou le recrutement, l'éducation, l'accès à certains services essentiels, les services publics, la sécurité ou la justice. Les systèmes présentant un risque limité sont principalement soumis à des exigences de transparence, notamment lorsque l'utilisateur doit savoir qu'il interagit avec une IA (chatbot, assistant virtuel ...) ou qu'un contenu a été généré ou manipulé par celle-ci. Enfin, les applications à risque minimal comme des outils d'assistance à la rédaction, de correction linguistique, de traduction, d'optimisation de tâches ou de recherche documentaire, lorsque ces outils ne prennent pas de décision affectant substantiellement une personne, peuvent généralement être utilisées avec des exigences réglementaires plus limitées, sous réserve du respect des règles générales applicables.

Cette classification détermine les obligations qui incombent aux fournisseurs, développeurs, intégrateurs, distributeurs et utilisateurs professionnels. Les systèmes

à haut risque sont notamment soumis à des exigences strictes en matière de gouvernance des données, de documentation technique, de supervision humaine, de transparence, de cybersécurité, de gestion des risques et d'évaluation de conformité.

Dans ce contexte, la contractualisation devient un outil essentiel de maîtrise des risques juridiques. Les contrats encadrant le développement, l'acquisition ou l'utilisation de solutions d'IA doivent préciser les responsabilités respectives des parties et organiser une répartition claire des obligations de conformité.

À cet égard, plusieurs clauses méritent une attention particulière.



En premier lieu, les clauses relatives aux données doivent identifier les catégories de données utilisées (données d'entraînement, de validation, d'entrée et de sortie), définir les droits d'utilisation, imposer le respect des règles applicables en matière de protection des données personnelles, prévoir les mesures de minimisation, de qualité (source authentique) et de sécurité des données ainsi que les modalités de transfert et de conservation.

En deuxième lieu, les stipulations relatives à la propriété intellectuelle doivent déterminer le régime juridique applicable aux résultats générés par l'IA (outputs), aux modèles développés, aux jeux de données enrichis ainsi qu'aux licences concédées entre les parties.

En troisième lieu, les contrats doivent organiser la gouvernance des données et des systèmes d'IA. Cela suppose la définition des rôles et responsabilités, la mise en place de procédures de validation des données, de mécanismes d'audit, de traçabilité des traitements, de gestion des versions et d'archivage des documents de conformité.

Les clauses relatives à la sécurité numérique revêtent également une importance particulière. Elles doivent prévoir les exigences de cybersécurité, les obligations de notification des incidents, les audits de sécurité, la gestion des sous-traitants ainsi que les garanties offertes contre les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données.

Les contrats gagneraient également à intégrer des mécanismes spécifiques de gestion des biais algorithmiques. Il s'agit notamment d'imposer des contrôles réguliers sur la qualité des données, des procédures d'évaluation des performances du système, des mesures destinées à prévenir les discriminations ainsi qu'une supervision humaine effective lorsque les décisions produisent des effets significatifs sur les personnes.

Enfin, les clauses de responsabilité, de garantie et d'indemnisation doivent être adaptées aux spécificités des systèmes d'IA. Elles permettront de déterminer les responsabilités en cas de dysfonctionnement, d'erreur algorithmique, de violation des droits de tiers, de non-conformité réglementaire ou d'atteinte aux données utilisées.

Au-delà des contrats, la conformité juridique suppose la mise en place d'une véritable gouvernance de l'intelligence artificielle. Celle-ci repose sur une cartographie des usages de l'IA, une classification des systèmes selon leur niveau de risque, des procédures internes de contrôle, des audits réguliers, une politique documentaire adaptée ainsi qu'une sensibilisation continue des acteurs concernés.

Pour notre pays le Bénin, où l'adoption de l'intelligence artificielle s'accélère dans les secteurs public et privé, cette approche présente un intérêt particulier. Si le Code du numérique et le régime de protection des données personnelles en vigueur constituent le socle juridique national, un renforcement des règles spécifiques applicables à la gouvernance, à la responsabilité et à la conformité des systèmes d'IA apparaît désormais indispensable afin d'assurer un développement de l'innovation respectueux des droits fondamentaux et de la sécurité juridique.



Des usages tels que l'utilisation de l'IA pour l'assistance aux agents publics, l'exploitation de données issues de plusieurs administrations, l'aide à la décision dans les secteurs de la santé, de l'éducation ou des services sociaux, le recrutement, l'analyse biométrique ou encore la vidéosurveillance algorithmique peuvent présenter des niveaux de risques très différents.

L'enjeu n'est donc pas de réglementer indistinctement toutes les applications d'IA, mais de mettre en place une gouvernance proportionnée au risque, fondée notamment sur la protection des données à caractère personnel, la sécurité, la transparence, la supervision humaine, la traçabilité, la maîtrise des biais et la responsabilité des acteurs.

Cette approche pourrait utilement conduire à l'élaboration progressive d'une doctrine nationale de classification des systèmes d'IA, permettant d'identifier les usages interdits ou particulièrement sensibles, les systèmes soumis à une évaluation renforcée et les applications pouvant être déployées sous réserve d'obligations de

transparence et de sécurité.

En définitive, la conformité juridique ne doit plus être perçue comme une contrainte pesant sur l'innovation. Elle constitue au contraire un facteur de confiance, de sécurité et de compétitivité. Une intelligence artificielle juridiquement maîtrisée est une intelligence artificielle durable, responsable et créatrice de valeur pour l'ensemble des parties prenantes.

Suivez-nous sur nos canaux digitaux



@asinbenin