ANALYSE DES SPÉCIALISTES / ACHATS

L’achat d’IA : un marché public comme un autre ?

Fournisseur | Innovation | Intelligence artificielle (IA) | Réglementations | RGPD

Publié le 27 janvier 2026 à 11h00 - par Yvon Goutal

Dans son principe, l’achat d’IA n’est pas fondamentalement différent d’un achat informatique classique. Une définition précise du besoin, la fixation d’indicateurs clés de performance (KPI) et l’intégration des « bonnes » clauses contractuelles sont les clés d’un achat réussi. Entretien avec Yvon Goutal, avocat au barreau de Paris Goutal, Alibert et Associés.

© Par Renán Vicencio Uribe - stock.adobe.com

Existe-t-il une spécificité à l’achat d’IA ?

Assez peu, en réalité. Pour l’essentiel, la mise en concurrence s’impose dès le premier euro et la définition de son besoin réel par l’acheteur (et non une offre commerciale séduisante) est la base dont on déduit exclusions, critères de sélection des candidatures et des offres, exigences contractuelles et enfin

sanctions.

Une phase de sourcing permettra le plus souvent d'écarter les fausses « innovations » (art. R. 2122-9-1 du Code de la commande publique) ou « exclusivités » (art. R. 2122-3, 3° du Code de la commande publique) : intelligence artificielle (IA) n'est pas synonyme de gré à gré. La nature propre de l'IA rend délicate la question des performances attendues et, a contrario, des erreurs tolérées.

Pour y répondre, les acheteurs doivent identifier des rapports réguliers sur des indicateurs clés de performance (KPIs). Ceux-ci devront être définis, notamment, en considération du niveau de service attendu, par exemple : taux d'erreur toléré ; disponibilité ; satisfaction usager ; consommation énergétique ; etc.

Quelle vigilance au regard de la réglementation ?

Le déploiement d'un système d'IA est très encadré : CRPA (Code des relations entre le public et l'administration, not., art. L. 312-1-3 ; L. 311-3-1 et R. 311-3-1-2), RGPD (Règlement général sur la protection des données (UE) 2016/679 du 27 avr. 2016), Loi Informatique et libertés (n° 78-17 du 6 janv. 1978, not. art. 47 et 119), RIA (Règlement sur l'intelligence artificielle (UE) 2024/1689 du 13 juin 2024), etc. ; et le contrat doit en pratique permettre de respecter l'essentiel de la réglementation.

La collectivité dépend en effet largement de son fournisseur pour assurer le respect des dispositions applicables, ce que le contrat doit refléter : le fournisseur doit s'engager à respecter le cadre juridique applicable et surtout à assister activement la collectivité dans l'exécution de ses propres obligations.

Par exemple, le plus souvent, les collectivités n'ont pas elles-mêmes la capacité d'expliquer le fonctionnement technique des dispositifs d'IA qu'elles déploient : il faut donc transférer les obligations de transparence et d'explicabilité sur le fournisseur (documentation technique détaillée, explication générale, explication individualisée), qui devra fournir des éléments

« intelligibles » (En ce sens, v. not. CJUE, 27 févr. 2025, aff. C-203/22, Dun & Bradstreet Austria) afin que les administrés puissent comprendre l'élaboration des décisions les concernant.

Propriété intellectuelle, données et cybersécurité doivent-elles inquiéter ?

La propriété intellectuelle est assurément un sujet : il est impératif de sécuriser les droits de la collectivité sur les données d'entrée et de sortie et la réutilisation des données fournies. Le fournisseur devra en outre garantir que les modèles ont été entraînés sur des jeux de données collectés de manière licite – et couvrir la collectivité en cas de contentieux.

Évidemment, les clauses limitatives de responsabilité ne doivent pas vider les garanties de toute substance. La cybersécurité est également un point non négociable.

Si une certification SecNumCloud / ISO 27001 peut être un prérequis intéressant, elle ne suffit pas. Les SIA comportent des vulnérabilités spécifiques (empoisonnement des données, extraction non autorisée d'information, introduction de biais…). Le contrat doit prévoir avec précision les mesures de sécurité mises en place, les dispositifs de détection des vulnérabilités, un plan de continuité d'activité ainsi que d'éventuelles modalités d'audit.

Dans le même esprit, devront être prévues les modalités de mises à jour et de correction des biais, la réversibilité du système, préciser les éléments à restituer, détruire ou conserver et éviter autant que possible la dépendance (la situation d'exclusivité imputable à l'acheteur n'étant pas un motif valable pour s'exonérer de mise en concurrence, CJUE, 9 janv. 2025, aff. C-578/23, République Tchèque).

Propos recueillis par Claire Demunck