AYI NEDJIMI Consultants

Souveraineté IA — pourquoi les entrepris

16 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3046 mots •

Décryptez les enjeux de la souveraineté IA en 2026 : risques RGPD des LL vLLM/Ollama/Scaleway, ROI du rapatriement pour les ETI françaises.

À RETENIR

A retenir -- Souverainete IA et LLM on-premise

La **souverainete IA** est devenue un imperatif strategique pour de nombreuses entreprises europeennes ont initie ou planifie un rapatriement de tout ou par premise ou souveraines en 2026 (Gartner). Les motivations sont multiples -- de la propriete intellectuelle, independance technologique -- mais converger donnees traitees par les LLM. Les solutions techniques sont matures : vLLM, performances proches des APIs cloud avec une maitrise totale des donnees.

La **souverainete IA dans les entreprises** est un sujet 2026. Apre APIs LLM cloud (OpenAI, Anthropic, Google), de non ions franç

strategique et securitaire qui les pousse a rapatrier tout ou partie de leurs usages raisons sont multiples : obligations RGPD sur les transferts de donnees hors UE, ri client et salarie, dependance technologique vis-a-vis d'acteurs americains ou asia face aux incertitudes sur l'utilisation des donnees soumises aux APIs cloud. En pa (Llama 3.3, Mistral, Qwen) et des outils de serving (vLLM, Ollama, TGI, SGLang) a aux ETI sans grandes equipes ML. Cet article decrypte les enjeux juridiques et str des differentes options, et guide les RSSI et DSI dans leur decision cloud versus o

Risques confidentialite des LLM cloud -- OpenAI, Azure et AWS Bedrock

Les **risques de confidentialite des LLM cloud** sont reels mais souvent mal compris

OpenAI API : les donnees soumises via l'API ne sont pas utilisees par defaut po pour les utilisateurs API depuis 2023). Mais les donnees transitent vers des ser permet aux autorites americaines d'y acceder sur requete judiciaire, independa europeens.

Microsoft Azure OpenAI Service : offre des garanties supplementaires via les c europeennes (data residency en Europe, engagement de non-utilisation pour l' Microsoft Corporation.

AWS Bedrock : similar a Azure, avec des engagements contractuels forts mais Amazon.

Scaleway AI / OVH AI : solutions europeennes echappant au CLOUD Act ameri en France. Moins de modeles disponibles mais couverture suffisante pour la plu

La question cle n'est pas seulement "les conditions d'utilisation permettent-elles l pour les services enterprise), mais "mes donnees sont-elles accessibles a des aut judiciaires". Pour les donnees sujettes au secret prof e, medical, premise ou souverain.

Réponse sous 24h

Devis gratuit →