SPOTLAB / ANALYSE P21

IA souveraine : comment arbitrer cloud, modèles ouverts et contrôle des données ?

La souveraineté d'une IA se prouve : données, opérations, juridique, modèles, réversibilité et qualité métier.

Analyse / P21

Novembre 2026

Sources consultées au 2 novembre 2026

ANALYSE P21

Sommaire

01	Trois convictions à retenir	3
02	Ce que signifie « souverain » pour une entreprise	3
03	Six dimensions, des preuves et des conditions éliminatoires	4
04	Cloud européen, cloud de confiance, cloud privé : ne pas les confondre	5
05	Les modèles aux poids ouverts élargissent les choix, pas les garanties	6
06	L'Europe facilite la portabilité, mais ne remplace pas le test de sortie	7
07	Trois architectures à comparer, sans vainqueur universel	8
08	Simulation : un contrôle interne en assurance	8
09	Un exercice de sortie en cinq étapes	10
10	La souveraineté n'efface pas les autres obligations	11
11	Ce que doit décider le comité de direction	11
12	Sources et limites	12

FICHE DE L'ANALYSE

ÉDITEUR
Spotwork.AI — Spotlab, Research & Insights

RÉFÉRENCE
P21

TYPE
Revue documentaire et méthode de décision

COLLECTION
Fiabilité & gouvernance

SOURCES CONSULTÉES
2 novembre 2026

PUBLICATIONS LIÉES
I0-01 · P06

EN BREF

Héberger des données en Europe, utiliser un modèle aux poids accessibles ou déployer un service chez un fournisseur français ne suffit pas, pris isolément, à garantir la souveraineté d'une IA. Une entreprise doit surtout savoir qui peut accéder aux données et au système, quelles dépendances elle accepte et dans quelles conditions elle pourrait changer de solution sans interrompre son activité. La souveraineté se décide donc par usage, se démontre par des preuves et se réévalue dans le temps.

> *La souveraineté ne se réduit pas à l'hébergement. Elle suppose une analyse des dépendances, de la portabilité, des contrats et de la réversibilité.*
>
> CE QU'IL FAUT RETENIR

01 Trois convictions à retenir

1

La localisation n'est qu'une dimension du contrôle.

Les administrateurs, les sous-traitants, les clés, les journaux, les transferts éventuels et les régimes juridiques comptent autant que l'emplacement des serveurs. Une région européenne ne vaut pas, à elle seule, une analyse juridique et technique complète.

2

Poids ouverts et logiciel open source ne sont pas synonymes.

Accéder à un modèle et pouvoir l'exploiter localement ouvre des options ; les droits de modification, de redistribution et les informations nécessaires à sa compréhension doivent être examinés séparément.

3

La réversibilité ne se décrète pas dans un contrat.

Elle exige des formats exportables, des données récupérables, des outils remplaçables, des tests d'équivalence métier et un plan de transition effectivement essayé.

02 Ce que signifie « souverain » pour une entreprise

Le terme couvre plusieurs ambitions qui peuvent entrer en tension : maîtriser les données personnelles et confidentielles, limiter certaines dépendances géopolitiques, conserver la maîtrise de l'exploitation, protéger des connaissances propres et garantir la continuité des usages professionnels. Aucune de ces ambitions ne résulte automatiquement de la nationalité d'un fournisseur.

Pour raisonner correctement, il faut distinguer résidence des données, contrôle des accès et des opérations, exposition juridique, maîtrise des composants technologiques, portabilité et qualité/coût de service. Une solution peut obtenir un bon niveau sur l'une de ces dimensions et être insuffisante sur une autre. La notion pertinente n'est donc pas un label global, mais un profil de maîtrise établi pour un cas d'usage.

> Une organisation peut héberger ses données dans l'UE et dépendre d'un fournisseur non européen pour les outils, l'administration, l'inférence, les identités et les mises à jour. Inversement, un modèle aux poids accessibles hébergé localement peut rester insuffisant pour un usage professionnel sensible si l'exploitation, la sécurité ou la qualité ne sont pas maîtrisées.

03 Six dimensions, des preuves et des conditions éliminatoires

La grille suivante est une proposition méthodologique Spotwork.AI, non un standard de certification. Les exigences minimales doivent être définies par le métier, le RSSI, le DPO et les responsables des achats avant de classer des fournisseurs.

Dimension	Question à poser	Preuve à demander
Données	Où vont prompts, fichiers, embeddings, journaux et sauvegardes ?	Carte des flux, rétention, chiffrement, sous-traitants, suppression
Contrôle opérationnel	Qui exploite le service, accède aux consoles et détient les clés ?	Identités, droits d'administration, journal d'accès, modalités d'escalade
Exposition juridique	Quelles entités et quelles lois sont pertinentes ?	Contrats, chaîne de sous-traitance, analyse des transferts et risques
Indépendance technique	Peut-on remplacer le modèle, les API, les outils et les index ?	Licences, interfaces, formats, dépendances et composants exportables
Réversibilité	Peut-on migrer dans un délai et un coût acceptables ?	Export testé, reprise des droits, qualité comparée, procédure de retour arrière ; exercices de continuité documentés
Performance et coût complet	La solution atteint-elle les exigences métier ?	Jeux de tests, incidents, latence, coûts d'exploitation et de supervision

POINT DÉCISIF

Les six dimensions ne doivent pas être additionnées naïvement. **Une violation de droits, un transfert incompatible avec les exigences applicables ou l'impossibilité de récupérer une donnée essentielle peut être éliminatoire**, même si la solution obtient une excellente note moyenne.

Méthode d'arbitrage

1. Une fiche par cas d'usage
2. Caractériser données et actions
3. Exigences minimales et veto
4. Comparer les options admissibles
5. Simuler la migration

L'échelle de maîtrise est une grille interne à fixer par les responsables métier et sécurité. Ce raisonnement prolonge les deux portes du cadre de sélection Spotwork.AI (voir « Comment choisir un modèle d'IA pour son entreprise ? Six critères et une méthode de décision») : les conditions éliminatoires s'appliquent avant toute comparaison.

04 Cloud européen, cloud de confiance, cloud privé : ne pas les confondre

Un hébergement dans l'Union européenne renseigne sur la localisation de certaines ressources. Il ne prouve pas automatiquement la maîtrise des accès distants, des prestataires de support ou des obligations juridiques susceptibles de s'appliquer. Les lignes directrices du Comité européen de la protection des données (EDPB) sur les transferts internationaux rappellent l'importance d'identifier concrètement les situations de transfert et les acteurs concernés [3].

EDPB · LIGNES DIRECTRICES 05/2021 — VERSION 2.0 DU 24 FÉVRIER 2023

Elles encadrent l'articulation entre le champ territorial du RGPD (article 3) et les règles de transfert du chapitre V. Qualifier un transfert demande d'examiner les acteurs et circonstances précises : la localisation d'un serveur n'est pas un test juridique suffisant.

ACCÈS PAR DES AUTORITÉS ÉTRANGÈRES : UN RISQUE À ÉVALUER, PAS À PRÉSUMER

Selon le pays de rattachement d'un fournisseur ou de ses sous-traitants, des législations étrangères peuvent permettre à des autorités d'un pays tiers de demander l'accès à des données, y compris lorsqu'elles sont hébergées dans l'Union européenne. Ces cadres évoluent, parfois rapidement, au gré du contexte géopolitique ; leur portée réelle dépend de la structure du fournisseur et de son contrôle effectif sur les données, les clés et le support. Le RGPD encadre la réponse à de telles demandes, et le Comité européen de la protection des données a publié des lignes directrices sur son article 48. [9]

Questions à poser avant de choisir une offre : quelles entités contrôlent les données, les clés de chiffrement et le support, et quelles juridictions s'appliquent à chacune ? Comment le fournisseur traite-t-il une demande d'accès d'une autorité étrangère, et vous en informe-t-il ? Ces engagements sont-ils contractuels et révisés dans le temps ? L'évaluation d'une offre précise relève d'un juriste, à la date de la décision.

En France, SecNumCloud 3.2 est un référentiel de qualification de l'ANSSI pour certaines offres de services cloud. Un arrêté du 12 août 2026, publié le 14 août, en approuve la version 3.2 et la rend opposable lorsque les administrations, les opérateurs de l'État et les groupements d'intérêt public confient à un prestataire des données d'une sensibilité particulière. Il convient de vérifier l'offre précise et son statut de qualification, pas seulement le nom du fournisseur. La qualification ne signifie pas qu'une application IA utilisant ce cloud est automatiquement conforme, fiable ou entièrement souveraine [4][5].

CE QUE VISE L'ARRÊTÉ

Les services de l'État, ses opérateurs et les groupements d'intérêt public, pour les données dont la compromission pourrait porter atteinte à l'ordre public, à la sécurité publique, à la santé, à la vie des personnes ou à la propriété intellectuelle. Il met en œuvre l'article 31 de la loi du 21 mai 2024 (SREN).

CE QU'IL NE DIT PAS

Un éditeur ne peut pas conclure que son service IA est qualifié au seul motif que son fournisseur cloud exploite ailleurs une offre qualifiée. La liste des offres qualifiées et celle des projets de qualification doivent être distinguées : seul compte le périmètre de l'offre effectivement utilisée.

La bonne architecture dépend donc des traitements. Une entreprise peut réserver un environnement plus contrôlé aux dossiers les plus sensibles et utiliser un service cloud managé pour des contenus non confidentiels, si les règles internes et juridiques le permettent.

05 Les modèles aux poids ouverts élargissent les choix, pas les garanties

Exploiter un modèle aux poids accessibles peut faciliter l'inférence dans un environnement choisi, l'ajustement sur un domaine et certaines stratégies de continuité. Mais il faut encore contrôler sa licence, les composants d'inférence, les outils de sécurité, les dépendances matérielles et les coûts de maintenance.

L'Open Source AI Definition 1.0 de l'Open Source Initiative (OSI) distingue les libertés d'utiliser, d'étudier, de modifier et de partager. Elle demande des informations sur les données d'entraînement, le code et les paramètres nécessaires à la modification du système. « Open-weight » n'implique donc pas nécessairement « open source » selon cette définition [1].

Question	API propriétaire	Modèle aux poids accessibles auto-hébergé
Déploiement	Opérations gérées par le fournisseur	Choix de l'infrastructure et responsabilité d'exploitation
Licence	Contrat de service et conditions de l'API	Licence des poids, du code et des données ; redistribution à examiner
Sécurité	Assurance et interfaces dépendant du prestataire	Correctifs, supervision et tests à organiser soi-même
Coût	Prix d'appel, volumes, dépendance et support	Capacité de calcul, disponibilité, exploitation, énergie, mises à jour
Portabilité	Formats, SDK et outils peuvent verrouiller	Des dépendances matérielles ou de frameworks peuvent subsister

La qualité n'est pas non plus constante : le Stanford AI Index 2026 signale qu'après un rapprochement en 2024, l'écart entre les meilleurs modèles ouverts et fermés s'est à nouveau élargi sur le classement étudié en mars 2026. Ce constat est lié à ce benchmark et à cette date, et ne préjuge pas des performances sur un dossier juridique, un rapport de conseil ou un contrôle interne spécifique [2].

MAI 2023

174 pts

écart sur Arena entre le meilleur modèle fermé et le meilleur ouvert

AOÛT 2024

7 pts

écart quasi refermé

MARS 2026

49 pts

1 503 contre 1 454 : l'écart s'est rouvert

Source : Stanford HAI, AI Index 2026, chapitre 2 [2]. Données Arena, valeur indicative et datée.

06 L'Europe facilite la portabilité, mais ne remplace pas le test de sortie

Le Data Act européen impose, dans son champ d'application, des exigences visant à faciliter le changement de fournisseur de services de traitement de données, notamment certaines obligations de transparence et d'export. Il prévoit la suppression des frais de changement de fournisseur à compter du 12 janvier 2027, sous réserve des dispositions et exceptions applicables. Au 2 novembre 2026, cette échéance est donc encore future [6].

Mais exporter des données n'équivaut pas à reconstruire une application IA : il faut souvent récupérer les prompts et politiques, les index de recherche, les schémas d'outils, les évaluations, les journaux requis et les modalités d'authentification. Un contrat de portabilité ne garantit pas la même qualité métier chez un prestataire de remplacement.

Inventaire minimal des dépendances

Données et versions · Embeddings · Schémas de documents · Règles d'ingestion · Prompts · Politiques d'autorisation · Outils et agents · Évaluations · Journaux · Identification · Gestion des secrets · Sauvegardes · Capacités GPU · Coûts et temps de migration

EXPORTABLE	RECONSTRUCTIBLE	À ADAPTER	NON PORTABLE
Ce qui peut être extrait tel quel	Ce qui peut être reconstruit, par exemple des index	Ce qui nécessite une adaptation	Ce qui est juridiquement ou techniquement non portable

Certains composants, par exemple un modèle d'embedding distinct, peuvent imposer une reconstruction des index ; les sorties des modèles ne sont pas strictement identiques à l'octet. L'équivalence recherchée est métier, sous critères prédéfinis, et non une identité textuelle systématique.

Pour les entités financières concernées, DORA impose notamment des stratégies de sortie documentées, testées et revues périodiquement pour les services TIC soutenant des fonctions critiques ou importantes. Cela ne signifie pas que les mêmes obligations s'appliquent indistinctement à toutes les entreprises ou à tous les outils IA [7].

07 Trois architectures à comparer, sans vainqueur universel

Architecture	Atout principal	Compromis à vérifier
API managée	Accès rapide aux capacités de modèles et à une exploitation mutualisée	Flux, conditions contractuelles, verrouillage API et réversibilité
Modèle aux poids accessibles sur infrastructure maîtrisée	Contrôle accru des opérations d'inférence et des données dans l'environnement retenu	Licence, coûts GPU, exploitation, mises à jour, sécurité et qualité
Approche hybride gouvernée	Affecter des traitements différents à des environnements adaptés	Complexité de routage, traçabilité, prévention des transferts non autorisés

Une architecture multi-modèle peut améliorer la capacité de substitution, mais ne rend pas un système réversible à elle seule. Les connecteurs, les embeddings, le traitement documentaire, la gouvernance des agents et les règles d'accès peuvent encore constituer des dépendances fortes. Le Le sujet approfondit ainsi notre publication « Multi-LLM ou modèle unique : quand l'orchestration de plusieurs IA crée-t-elle vraiment de la valeur ?».

08 Simulation : un contrôle interne en assurance

CAS FICTIF sans référence client ni résultat expérimental

Une direction de contrôle interne souhaite analyser des justificatifs sensibles et générer des constats. Elle compare trois options : service managé européen, inférence locale d'un modèle aux poids accessibles et architecture hybride. Le choix dépend des types de pièces, des accès autorisés, des obligations de conservation et des résultats des tests métier.

Une proposition raisonnable consiste à classer les données et actions d'abord : les pièces très sensibles restent dans le périmètre autorisé ; un service externe n'est appelé que pour les opérations explicitement compatibles avec la politique. Le système conserve les identifiants de sources, les décisions d'autorisation et une preuve des traitements réalisés. La validation du constat reste un acte métier distinct de la génération.

08 / SIMULATION — SUITE

Avant d'étendre l'usage, l'équipe simule le retrait d'un fournisseur : peut-elle reconstruire le pipeline, récupérer les données utiles, rejouer les évaluations, maintenir les droits et conserver la qualité des résultats ? Aucune option n'est déclarée gagnante avant les essais.

Sept tests à appliquer aux trois options

T01	**Résidence et données.** Lister chaque type de donnée, les destinations et les sous-traitants, ainsi que les entités qui contrôlent les données, les clés de chiffrement et le support ; empêcher l'envoi vers une destination non autorisée.
T02	**Permission.** Un utilisateur sans droit ne peut ni faire récupérer la pièce, ni obtenir une réponse fondée sur elle.
T03	**Journaux.** Les preuves d'exécution sont conservées sans exposer les secrets.
T04	**Fournisseur indisponible.** L'activité doit pouvoir s'arrêter proprement ou passer à une option autorisée.
T05	**Migration.** Export et reconstruction des composants critiques, puis reprise des droits.
T06	**Qualité.** Rejouer les cas d'extraction, de citation et d'abstention ; documenter les pertes ou gains sans inventer de chiffres.
T07	**Conformité.** Revue des obligations spécifiques au dossier et aux traitements.

REGISTRE DE PREUVES

Une décision favorable doit reposer sur un dossier par usage, non sur une brochure : carte des flux réels (inférence, stockage, index, journaux), entités et sous-traitants, droits d'administration, licences, résultats des essais de sortie. Pour chaque document, distinguer preuve reçue, contrôle réellement effectué et conclusion approuvée. Le même jeu de cas, les mêmes exigences de sécurité et une définition commune du coût complet doivent être utilisés pour les trois architectures.

09 Un exercice de sortie en cinq étapes

1

Délimiter le scénario

Un fournisseur indisponible, une hausse tarifaire, une obligation de transfert ou une modification contractuelle.

Pré-enregistrer les tâches, versions, droits, seuils métier, budget et raisons d'arrêt.

2

Exporter les actifs pertinents

Documents, métadonnées, prompts, configurations, index ou procédure de reconstruction, schémas d'outils et journaux requis.

Vérifier la complétude et les restrictions de propriété.

3

Reconstituer les droits et les contrôles

Identités, autorisations, secrets, politiques, approbations et conservation.

Inclure la supervision, la validation humaine et la continuité du service cible.

4

Rejouer des cas métier représentatifs

Exactitude, sécurité, latence, coût complet et comportement d'abstention.

Mêmes cas, mêmes données autorisées et mêmes barèmes ; répéter lorsque la variabilité le justifie, avec un nombre d'essais borné.

5

Décider

Bascule contrôlée, correction et nouvel essai, ou impossibilité documentée de sortir sans risque disproportionné.

BASCULE CONTRÔLÉE | CORRECTION PUIS RETEST | IMPOSSIBILITÉ DOCUMENTÉE

La réversibilité doit être démontrée sur le périmètre critique et avec des critères prédéfinis. Un test ponctuel de connexion à une seconde API ne suffit pas. **Une violation d'ACL, un flux interdit ou une perte de données requises impose un veto sur la configuration concernée.** Les seuils de coût et de performance sont définis par le métier ; les essais répétés sont limités en nombre, coût, durée et appels d'outils.

10 La souveraineté n'efface pas les autres obligations

Le cadre juridique de l'IA est lui-même évolutif. Le règlement européen (UE) 2026/1744, entré en vigueur le 27 juillet 2026, a modifié plusieurs dispositions et échéances de l'AI Act. Il faut donc analyser les obligations en fonction du rôle de l'entreprise, du cas d'usage et de la date applicable — sans assimiler souveraineté, conformité au RGPD et conformité à l'AI Act [8]. La conformité au RGPD, à DORA et à l'AI Act ne se déduit jamais mécaniquement du choix d'un fournisseur cloud (voir P07).

Contrat de gouvernance et responsabilités

Une fiche d'arbitrage doit désigner les responsables de la classification des données, de l'analyse juridique et des transferts, de l'architecture et des dépendances, des licences, de la sécurité, des opérations, du coût complet et de la validation métier. L'absence d'une preuve critique doit apparaître comme « non démontré », et non comme « conforme ». Les qualifications visent une offre et un périmètre donnés ; les versions de lois et de contrats sont datées. Les revues périodiques réexaminent les prestataires, sous-traitants, usages, modèles, incidents et exercices de sortie.

11 Ce que doit décider le comité de direction

> *La bonne question n'est pas « faut-il une IA souveraine ? », mais « de quelles dépendances voulons-nous garder le contrôle, pour quels usages, à quel coût et avec quelle preuve ? ».*
>
> 11 / CE QUE DOIT DÉCIDER LE COMITÉ DE DIRECTION

L'entreprise gagne à fixer ses conditions éliminatoires, comparer quelques architectures réalistes et vérifier régulièrement les capacités de sortie.

Au fond, la souveraineté utile protège moins un lieu d'hébergement abstrait que la capacité durable de l'organisation à faire évoluer ses connaissances, ses outils et ses choix de modèles.

12 Sources et limites

Cette publication est une revue documentaire accompagnée d'une méthode de décision proposée par Spotwork.AI. Elle ne constitue ni une certification juridique, ni un benchmark propriétaire, ni une attestation de fonctionnalités disponibles dans Spotwork.AI. Les scénarios sont fictifs. Toute conclusion de conformité doit faire l'objet d'une revue spécialisée à la date de décision.

[1] OSI — Open Source AI Definition 1.0 (28 octobre 2024).
opensource.org/ai/open-source-ai-definition

[2] Stanford HAI — AI Index 2026, Technical Performance.
hai.stanford.edu/ai-index/2026-ai-index-report/technical-performance

[3] EDPB — Guidelines 05/2021 on the interplay between Article 3 and Chapter V GDPR, version 2.0 (24 février 2023).
edpb.europa.eu/documents/guideline/guidelines-052021-on-the-interplay-between-the-application-of-article-3-and-the_en

[4] Légifrance — Arrêté du 12 août 2026 portant approbation du référentiel d'exigences relatif aux prestataires de services d'informatique en nuage (JO du 14 août 2026).
legifrance.gouv.fr/eli/arrete/2026/8/12/PRMD2617964A/jo/texte

[5] ANSSI — catalogue des solutions certifiées et qualifiées ; liste distincte des prestataires SecNumCloud en cours de qualification.
Seule une offre figurant au catalogue des solutions qualifiées prouve une qualification acquise.
cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/decouvrir-les-solutions-certifiees-qualifiees/ · cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/prestataires-secnumcloud/

[6] Commission européenne — Data Act explained.
digital-strategy.ec.europa.eu/en/factpages/data-act-explained

[7] DORA — Règlement (UE) 2022/2554, article 28.
eur-lex.europa.eu/eli/reg/2022/2554/oj

[8] Règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act, texte de base) et règlement modificatif (UE) 2026/1744.
eur-lex.europa.eu/eli/reg/2024/1689 · eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1744

[9] EDPB — Guidelines 02/2024 on Article 48 GDPR, version 2.1 (5 juin 2025).
Réponse d'un responsable de traitement à une demande d'autorité d'un pays tiers.
edpb.europa.eu/documents/guideline/guidelines-022024-on-article-48-gdpr_en

Spotwork.AI

L'IA professionnelle de confiance

Mieux travailler aujourd'hui,
construire votre intelligence de demain.

SPOTLAB · RESEARCH & INSIGHTS · ANALYSE P21

IA souveraine : comment arbitrer cloud, modèles ouverts et contrôle des données ?

La souveraineté d'une IA se prouve

© 2026 SPOTWORK.AI