



Souveraineté de l'IA

Données IA : peut-on vraiment parler de sécurité sans souveraineté ?

Données IA : peut-on vraiment parler de sécurité sans souveraineté ?

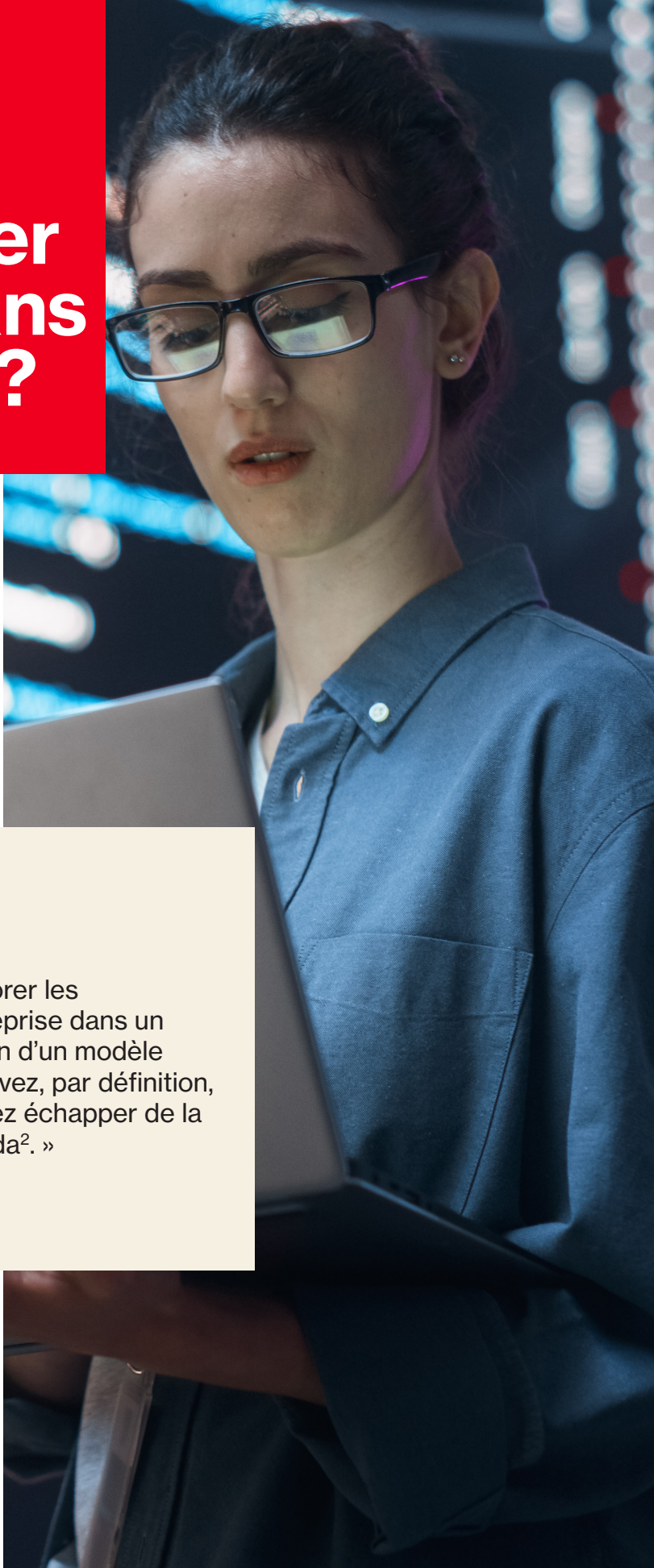
Dans cette nouvelle ère de l'IA en perpétuelle mutation, les entreprises doivent reprendre la maîtrise de leurs actifs digitaux et limiter les risques associés. Cela implique de garantir que leurs données et leurs modèles d'IA demeurent au sein de périmètres nationaux ou régionaux clairement définis. Cette exigence de souveraineté devient incontournable à mesure que les systèmes d'IA traitent des volumes croissants de données sensibles et de propriété intellectuelle, soulevant des enjeux majeurs de responsabilité, d'auditabilité et de gouvernance¹.



Si vous ne parvenez pas à incorporer les connaissances tacites d'une entreprise dans un ensemble de pondérations, au sein d'un modèle sous votre contrôle, alors vous n'avez, par définition, aucune souveraineté – Vous laissez échapper de la valeur au profit d'un modèle lambda². »

Satya Nadella,
CEO, Microsoft

La souveraineté dépasse désormais la simple notion de résidence des données : elle englobe aussi et surtout la question de savoir qui gère l'emplacement physique des processus de calcul³. En décentralisant les capacités d'IA et en s'affranchissant de la mainmise externe sur ces processus, les entreprises peuvent s'appuyer sur des modèles open source pour préserver leur autonomie en matière de sécurité des données, renforcer leur résilience opérationnelle et rester compétitives.



¹. Stanford University, AI Sovereignty's Definitional Dilemma, <https://hai.stanford.edu/news/ai-sovereignitys-definitional-dilemma>, 2026

². The Registrar, Speed: Microsoft CEO: AI sovereignty isn't where it runs, it's who controls it, <https://www.theregister.com/software/2026/01/21/nadella-talks-ai-sovereignty-at-the-world-economic-forum/5128191>, 2026

³. Red Hat, What is Sovereign AI? <https://www.redhat.com/en/topics/ai/sovereign-ai>, 2026



Le contrôle de l'IA doit être multicouche

Dans cet environnement complexe et dynamique, les notions de contrôle globales et unidimensionnelles ne suffisent plus. Les dirigeants doivent élaborer une stratégie multicouche visant à couvrir les différents aspects de leurs opérations⁴. À titre d'exemple, un rapport Cisco souligne qu'un agent IA a généré 450 % de trafic réseau supplémentaire par rapport à un humain effectuant manuellement la même tâche⁵. À l'avenir, il pourrait donc s'avérer nécessaire de séparer le trafic humain du trafic agentique sur des infrastructures réseau distinctes, lesquelles pourraient inclure d'autres composants spécifiques (résidence des données, propriété des modèles, gouvernance opérationnelle, etc.), et d'appliquer à chacune des approches ciblées et réfléchies.

Quelques concepts clés à cet égard :

- Contrôle territorial – Déterminer l'emplacement physique des données et ressources de calcul.
- Contrôle opérationnel – Gérer et sécuriser ces ressources critiques.
- Contrôle technologique – Posséder l'infrastructure, les algorithmes et la propriété intellectuelle sous-jacents.



IDC prévoit que, d'ici 2028, les DSI d'entreprises multinationales augmenteront de 65 % leurs investissements dans des environnements cloud et de localisation des données modulaires, compatibles avec les exigences croissantes de souveraineté⁶.

⁴ Kyndryl, Lovejoy, The physical foundations of digital sovereignty: How to reclaim control in the age of AI, <https://www.kyndryl.com/gb/en/insights/articles/2026/04/ai-sovereignty-enterprise-control>, 2026

⁵ Cisco, AI Impact on Wide Area Networks, <https://www.cisco.com/c/dam/en/us/solutions/collateral/artificial-intelligence/mass-scale-infrastructure/ai-network-traffic-report.pdf>, 2026

⁶ IDC, Claps et Nasir, Dispelling the myth of a silver bullet in sovereign, <https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/>, 2026



Les données de confiance transforment les supply chains européennes

Par exemple, BMW reste connecté numériquement à sa supply chain via Catena-X, un écosystème de données ouvert et collaboratif qui assure une circulation sécurisée et standardisée des informations⁷.

Cette solution permet au groupe munichois d'accroître la transparence, par exemple en calculant l'empreinte carbone des pièces, et de renforcer la résilience en détectant rapidement les points de blocage. Les premiers projets pilotes montrent qu'en optimisant les flux d'information, cette initiative améliore à la fois la durabilité et l'efficacité de la supply chain digitale de BMW, redéfinissant ainsi les chaînes de valeur dans le secteur automobile⁷.

Dans l'aéronautique, Airbus élabore un data space dédié visant à connecter de façon sécurisée son vaste réseau

d'environ 10 000 fournisseurs⁸. Fondée sur les principes de Gaia-X, l'initiative européenne de souveraineté des données, cette plateforme permet de préserver le contrôle des données opérationnelles et techniques sensibles au sein de l'écosystème européen, tout en limitant les risques de dépendance à un fournisseur unique et en renforçant la confiance entre les acteurs.

En adoptant un modèle fédéré et souverain, Airbus assure à chaque participant la pleine maîtrise de ses données. Cette démarche renforce la résilience, la sécurité et la collaboration au sein de l'écosystème aéronautique européen, et impulse l'innovation tout en préservant la souveraineté numérique.

⁷. BMW Group, On the way to a digitally connected supply chain with Catena-X, <https://www.bmwgroup.com/en/news/general/2025/catena-x-connects-digital-supply-chains.html>, 2025

⁸. Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, <https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x>, 2024

Les entreprises seront-elles un jour réellement propriétaires de leur IA ?



En privilégiant le déploiement de leurs propres modèles plutôt que la souscription à des services tiers onéreux, les entreprises font évoluer leur rapport à l'intelligence artificielle. L'IA ne relève plus seulement d'un poste de dépenses, mais devient un actif stratégique créateur de valeur. Une évolution d'autant plus nécessaire que de nombreuses grandes entreprises peinent à démontrer le ROI de leurs initiatives. Certaines sont même contraintes de revoir leurs ambitions à la baisse face à l'ampleur des coûts engagés. Uber, par exemple, aurait consommé l'intégralité de son budget IA 2026 en seulement quatre mois⁹. C'est dans ce contexte que des acteurs comme Mistral entendent démocratiser l'accès à l'IA grâce à des modèles, des produits et des solutions open source alliant innovation, efficacité et maîtrise des coûts¹⁰.

Comme le souligne Hanah-Marie Darley, cofondatrice et CAIO de Geordie AI : « Pour concrétiser leurs initiatives de souveraineté de l'IA, les entreprises devront vraisemblablement nouer des partenariats avec des acteurs privés et étatiques, au lieu d'y aller seules et de développer leurs propres modèles. Même si vous pouvez garantir l'hébergement des données, vous ne pourrez pas garantir les fonctionnalités. Par conséquent, si vous développez vos modèles vous-même, vous ne parviendrez sans doute pas à rivaliser avec les modèles de frontière qui bénéficient de milliards d'investissements¹¹. »



Je pense que [les entreprises] voudront emprunter cette voie. Après avoir investi massivement dans leurs propres modèles d'IA, elles n'ont pas nécessairement intérêt à les exploiter dans le cloud public. D'un point de vue économique, un déploiement dans un environnement privé peut s'avérer plus pertinent, tout en offrant davantage de garanties pour la protection des données et des algorithmes. »

Colin Wilson
Enterprise Architect, Verizon Business

⁹. Fortune, Angelo, Uber burned through its entire 2026 AI budget in four months. Now its COO is questioning whether it's worth it, <https://fortune.com/2026/05/26/uber-coo-ai-spending-tokens-claude-code/>, 2026

¹⁰. Matt Turck, Post LinkedIn, disponible sur : https://www.linkedin.com/posts/turck_while-silicon-valley-obsesses-over-agi-mistral-ugcPost-7427752521298821120-BLOm/, 2026

¹¹. IT Brew, Monsanto, What is AI sovereignty and why are companies chasing after it? <https://www.itbrew.com/stories/2026/04/27/what-is-ai-sovereignty-and-why-are-companies-chasing-after-it>, 2026



Maîtriser la souveraineté de l'IA : une approche multicouche

Détenir l'infrastructure qui sous-tend l'IA en fait un actif stratégique de premier plan. Pour autant, la souveraineté ne se décrète pas à renfort de politiques : elle repose sur une maîtrise complexe de multiples couches technologiques. Dans ce contexte, la tokenisation numérique permet de maintenir l'interopérabilité des systèmes et le flux des informations, tout en assurant une protection totale des données personnelles ou réglementées. Les données peuvent ainsi circuler librement entre les outils d'analyse, les pipelines d'IA et les écosystèmes partenaires, sans jamais exposer les informations sous-jacentes¹².

Enjeux

Dans une économie pilotée par l'IA, les entreprises ont de plus en plus intérêt à maîtriser leurs données stratégiques et leur infrastructure d'IA. L'absence de souveraineté les expose à des défis critiques, à une spirale des coûts et à un manque de flexibilité porteurs de nombreux risques :

- Compromission de la responsabilité, de l'auditabilité et de la gouvernance des données sensibles et des modèles propriétaires
- Risques de « fuite » de la valeur pour les entreprises qui ne maîtrisent pas les modèles intégrant leurs connaissances et savoir-faire tacites

- Incapacité à entraîner l'IA sur leurs propres données, et à ainsi valoriser ce précieux capital.

Implications

La souveraineté de l'IA ne se limite pas à la résidence des données : elle englobe aussi la maîtrise des processus de calcul. Cela exige :

- Une prise de contrôle des capacités d'IA en favorisant des architectures décentralisées et en éliminant toute dépendance à des acteurs externes. La tokenisation numérique contribue à sécuriser les traitements, y compris dans des environnements distribués.
- Pour certaines entreprises, la création de leur propre infrastructure d'IA full-stack.
- Une stratégie de contrôle multicouche, intégrant les enjeux territoriaux (lieu), opérationnels (modalités de gestion) et technologiques (propriété de l'infrastructure/PI).
- Le recours à des modèles open source pour préserver l'autonomie en matière de sécurité des données, renforcer la résilience opérationnelle et développer sa compétitivité.

¹² ALTR, AI sovereignty demands more than borders—it requires control over how data behaves. Digital tokenization is the key to that control, <https://altr.com/blog/without-digital-tokenization-there-is-no-sovereign-ai/>, 2026

Conséquences

Une IA souveraine n'est plus une simple dépense opérationnelle, mais un atout stratégique précieux pour l'entreprise. Cependant :

- Si une souveraineté complète et la capacité à rester au niveau des modèles d'IA de frontière peuvent s'avérer indispensables dans certains domaines régaliens (sécurité nationale, infrastructures critiques, etc.), la tokenisation numérique joue un rôle clé dans de nombreux autres cas d'usage. Elle permet de partager et d'exploiter les données en toute sécurité sans exposer les informations sous-jacentes.
- La création de modèles avancés en totale autonomie demeure complexe sur le plan technologique et fonctionnel, dans un contexte où les principaux acteurs du secteur drainent des milliards d'investissements.

À savoir

Les dirigeants doivent élaborer des stratégies multicouches sophistiquées pour exercer un contrôle précis sur leurs environnements d'IA.

- D'ici 2028, les DSI d'entreprises multinationales devraient accroître de 65 % leurs investissements dans des environnements cloud modulaires, compatibles avec les exigences de souveraineté. Dans ce contexte, la tokenisation numérique devrait s'imposer comme une technologie fondamentale pour sécuriser les flux de données au sein de ces environnements sous contrôle¹³.
- Si les solutions open source d'acteurs comme Mistral contribuent à démocratiser l'IA, les approches collaboratives demeureront essentielles pour atteindre une souveraineté complète¹⁴.



¹³ IDC, Claps and Nasir, Dispelling the myth of a silver bullet in sovereign, <https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/>, 2026

¹⁴ Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, <https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x>, 2024

Souveraineté de l'IA : Quel impact sur le réseau ?

L'IA souveraine, définie comme une approche multicouche qui englobe la maîtrise territoriale, opérationnelle et technologique, dépasse désormais le cadre d'une simple ambition stratégique : elle constitue un impératif concret

aux implications majeures sur les plans opérationnel et infrastructurel pour les entreprises. Le tableau ci-dessous illustre la manière dont ces enjeux se traduisent en exigences spécifiques pour l'IA et les capacités réseau nécessaires pour en garantir la maîtrise.

Besoin de l'entreprise	Besoin de l'IA	Impact sur le réseau
Garantir la responsabilité, l'auditabilité et la gouvernance des données.	Implémenter des contrôles stricts du traitement et de la résidence des données, afin de garantir que les données sensibles et les modèles propriétaires demeurent au sein des périmètres de sécurité définis par la réglementation.	Requiert une segmentation réseau robuste, des mécanismes de geofencing, ainsi que des connexions privées, chiffrées et sécurisées pour assurer la localisation des données et empêcher tout transfert au-delà des périmètres autorisés.
Empêcher la « fuite de la valeur » et protéger sa propriété intellectuelle.	Entraîner, déployer et gérer des modèles d'IA de façon sécurisée, en gardant une maîtrise technologique totale des algorithmes, des pondérations et des connaissances tacites intégrées.	Exige des environnements réseau isolés et hautement sécurisés pour le développement et l'inférence des modèles, complétés par des mécanismes rigoureux de filtrage des flux sortants et de détection des intrusions afin de protéger la propriété intellectuelle et de préserver l'intégrité des modèles.
Développer une résilience opérationnelle et réduire la dépendance à des acteurs externes.	Assurer le pilotage opérationnel de déploiements IA décentralisés, y compris l'edge computing et l'apprentissage fédéré, à travers différents sites physiques et instances de clouds souverains pour préserver l'autonomie.	Nécessite une architecture réseau distribuée, scalable, à faible latence et hautement résiliente, capable de gérer différents types de charges et de garantir des performances homogènes sur les équipements IA décentralisés.
Faciliter un échange de données fiable et sécurisée avec les partenaires.	Permettre un partage contrôlé et auditable des données et contenus générés par les modèles, tout en garantissant à chaque acteur la maîtrise de ses contributions grâce à des mécanismes de protection tels que la tokenisation numérique.	Le partage sécurisé des données repose sur des liaisons réseau de confiance, une architecture Zero Trust (ZTNA) et des passerelles API sécurisées, complétées par des politiques d'accès granulaires garantissant la conformité et la protection des informations.
Créer une stratégie de contrôle multicouche pour la conformité.	Appliquer des politiques distinctes pour le contrôle territorial (lieu), le contrôle opérationnel (modalités de gestion) et le contrôle technologique (propriété de l'infrastructure/PI).	L'implémentation d'infrastructures réseau flexibles et pilotées par logiciel est essentielle pour appliquer les politiques de sécurité, maîtriser les flux de données et garantir la conformité dans l'ensemble des environnements de calcul.
Faire évoluer l'IA d'une dépense opérationnelle vers un actif stratégique.	Soutenir le développement, l'entraînement et le déploiement de capacités d'IA internes, notamment par l'intégration de modèles open source au sein d'un écosystème souverain.	Réoriente les capacités réseau vers des environnements internes à haute performance afin de traiter les workloads d'IA les plus exigeants, de réduire les coûts de transfert de données internes et de maximiser l'efficacité de l'infrastructure propriétaire pour les workloads IA.

Accompagner les entreprises dans leur parcours vers une IA souveraine

Une chose est sûre, ces cas d'usage ne sont qu'un début. Le champ des possibles est tel que, pour nous comme pour d'autres entreprises dans le monde, l'IA reste un chantier en cours.

Transparence, explicabilité, supervision humaine... ces trois grands principes nous ont appris à renforcer la confiance dans les systèmes d'IA et à aider les collaborateurs à en faire un levier de réussite et d'épanouissement. Notre expérience souligne l'importance d'une stratégie holistique pour une IA souveraine qui, outre les aspects techniques, englobe les dimensions humaine et éthique, ouvrant ainsi la voie à une intégration de l'IA plus responsable et bénéfique.

À mesure que vous évoluez vers l'edge computing et les modèles open source pour renforcer la souveraineté de vos données, votre réseau devient votre nouveau périmètre de sécurité. Or, une stratégie d'IA distribuée exige une infrastructure mondiale à la fois agile et intelligente. Verizon propose la solution Network as a Service (NaaS) et l'architecture managée nécessaires pour router, sécuriser et traiter dynamiquement vos données d'IA souveraines au sein des périmètres autorisés, sans compromis sur les performances ou la conformité.

Si l'autonomie complète et la souveraineté absolue de l'IA peuvent s'avérer trop complexes pour certains secteurs, un contrôle accru et un certain degré d'indépendance – notamment pour les données propriétaires – figurent parmi les priorités de nombreuses entreprises.

En savoir plus

Aujourd'hui, il est impératif de comprendre comment monétiser l'IA souveraine et bâtir le réseau capable de répondre à ses exigences spécifiques. Partout dans le monde, Verizon aide les entreprises à exploiter le

plein potentiel de l'IA pour accélérer l'innovation, optimiser leurs services, générer des insights et renforcer leur business intelligence. Découvrez comment Verizon peut vous accompagner.



