

La souveraineté : un enjeu majeur pour les gouvernements du monde entier

Une nouvelle stratégie de survie pour les organismes publics

Pour les organismes publics hors des États-Unis, la souveraineté numérique est passée du statut de liste de contrôle réglementaire à celui de stratégie de survie. Les gouvernements se rendent compte aujourd'hui que la souveraineté ou le respect des réglementations nationales ne suffit pas. Ils visent donc un nouvel objectif de souveraineté numérique, ou d'autonomie stratégique, qui repose sur la capacité de faire fonctionner, d'entretenir et de développer les services essentiels de manière indépendante, même en cas de retrait de l'aide extérieure ou de perturbation des chaînes d'approvisionnement mondiales.

D'après un rapport récent de la Conférence des Nations unies sur le commerce et le développement (CNUCED), « 79 % des pays qui disposent de lois en matière de confidentialité et de protection des données sont préoccupés par la souveraineté numérique¹ ». Les gouvernements ne peuvent plus se permettre d'ignorer les dépendances indissociables des systèmes propriétaires et fermés. Trois grands facteurs influent sur la transformation vers une autonomie stratégique :

- ▶ **Risques géopolitiques** : en temps de paix, la dépendance vis-à-vis des hyperscalers mondiaux reste maîtrisable. Mais en cas de conflit, la dépendance envers une aide extérieure devient une vulnérabilité majeure. Les dégâts matériels ou les pannes d'Internet peuvent paralyser les infrastructures qui dépendent du cloud. Les nations doivent pouvoir agir de manière indépendante lorsque la coopération internationale est peu fiable, voire impossible. Cette approche nécessite des systèmes capables de fonctionner dans des environnements confrontés à des problèmes de réseau (refus, déconnexion, intermittence et faible bande passante), afin d'assurer la continuité des fonctions essentielles de la mission (systèmes de défense et de contrôle, services d'urgences pour les citoyens, etc.) même si le pays est déconnecté du réseau Internet mondial.
- ▶ **Cyber-résilience** : les cyberattaques commanditées par des États sont de plus en plus fréquentes, puissantes et sophistiquées. La souveraineté garantit la résilience des infrastructures essentielles (réseaux électriques, systèmes de santé, réseaux de systèmes de défense) face aux ingérences extérieures et aux sabotages des chaînes d'approvisionnement. Les risques incluent le vol de données, ainsi que l'injection de code malveillant dans les mises à jour logicielles en transit. Les pays ont besoin d'une assurance de leur souveraineté : ils doivent pouvoir vérifier de manière indépendante l'intégrité de leur chaîne d'approvisionnement des logiciels afin d'empêcher l'espionnage étranger, et s'assurer que les systèmes n'ont pas été compromis.
- ▶ **Compétitivité économique** : les gouvernements considèrent de plus en plus la souveraineté numérique comme un fondement de la sécurité nationale. Lorsque le développement de l'intelligence artificielle (IA) et la gouvernance des données s'effectuent au niveau local, les moteurs de la croissance économique future dépendent des compétences nationales plutôt que d'agents extérieurs. L'utilisation de modèles d'IA de type « boîte noire » développés à l'étranger inquiète : elle pourrait entraîner une perte de propriété intellectuelle et de pertinence culturelle. L'autonomie stratégique permet aux pays de développer ces capacités numériques, en favorisant les écosystèmes d'innovation locaux et en veillant à conserver la valeur économique générée par leur transformation numérique au sein de l'économie nationale.

¹ « [Data protection and privacy legislation worldwide](#) », CNUCED, 17 février 2026

Une demande mondiale, des réalités régionales

Si la demande de contrôle se retrouve dans le monde entier, les influences et les obstacles auxquels sont confrontés les différents organismes publics varient considérablement d'une région à l'autre.

Europe, Moyen-Orient, Afrique (EMEA) et Canada

Dans la région EMEA, le principal problème est le conflit entre le besoin de technologies avancées et la dépendance vis-à-vis de fournisseurs hors de l'Union européenne. Cette situation expose les gouvernements à des risques liés à l'application des différentes règles, en particulier les lois extraterritoriales comme celles édictées par les États-Unis, notamment la loi [CLOUD](#) (Clarifying Lawful Overseas Use of Data Act) ou la loi [FISA](#) (Foreign Intelligence Surveillance Act) de 1978.

Les organismes européens sont confrontés à un ensemble complexe de réglementations strictes, notamment la directive [NIS 2](#) de l'UE pour la cybersécurité et le règlement DORA (Digital Operational Resilience Act) pour la résilience opérationnelle, ainsi que d'autres [impératifs nationaux](#) comme la qualification SecNumCloud en France. Les infrastructures de défense sont fragmentées, car l'interopérabilité insuffisante de l'OTAN (Organisation du traité de l'Atlantique nord) retarde l'échange des données. Par ailleurs, les pays manquent cruellement de main-d'œuvre disposant des autorisations de sécurité nécessaires pour exploiter les environnements souverains. Bien qu'il se situe en Amérique du Nord, le Canada partage les défis de la région EMEA en matière d'infrastructures obsolètes. Son ministère de la Défense nationale doit gérer un ensemble hétérogène et fragmenté d'infrastructures, notamment l'IRSC (Infrastructure du réseau secret consolidé), et des obstacles administratifs qui ralentissent l'adoption de capacités modernes. Ce niveau de risque incite les organismes publics à isoler les données sensibles des ingérences juridiques étrangères et à combler le retard en matière de logiciels en développant leurs propres capacités.

Asie-Pacifique (APAC)

La région APAC est soumise à des exigences strictes de protection et à d'importantes normes de conformité pour atteindre l'autosuffisance technologique.

- ▶ **Emplacement des données** : des pays tels que la Chine, l'Inde et l'Indonésie imposent de stocker les données critiques à l'intérieur de leurs frontières nationales, limitant ainsi l'utilisation de clouds publics mondiaux.
- ▶ **Responsabilité élevée** : Singapour applique des normes strictes de sécurité de bout en bout, qui exposent les agents publics à des sanctions pénales en cas d'utilisation abusive ou de perte de données, ce qui favorise une culture axée sur la prudence.
- ▶ **Exigences mondiales et locales** : les modèles globaux et locaux (« glocaux ») sont souvent privilégiés. Ils reposent sur des partenariats dans le cadre desquels une technologie mondiale est fournie par des entreprises locales afin de garantir un contrôle souverain.

L'une des priorités des pays de l'APAC est de développer des capacités natives qui permettent de réduire la dépendance à long terme vis-à-vis des puissances étrangères, en considérant la souveraineté numérique comme un garde-fou contre la vulnérabilité géopolitique.

Amérique latine (LATAM)

Dans la région LATAM, la modernisation dépend de la continuité de l'exploitation et est souvent freinée par l'instabilité structurelle plutôt que par les politiques mises en œuvre.

- ▶ **Instabilité et manque de continuité** : les changements fréquents au niveau des instances du pouvoir politique et l'instabilité économique mettent en péril la planification informatique à long terme et les contrats d'approvisionnement pluriannuels dans un contexte géopolitique incertain.
- ▶ **Renforcement de la sécurité interne** : les organismes de défense de la région LATAM accordent la priorité à la sécurité interne (protection des frontières, lutte contre le narcotrafic) et préfèrent des outils de surveillance agiles à une infrastructure stratégique lourde².

2 «[New Pentagon strategy to focus on homeland, Western Hemisphere](#)», DefenseNews, 25 septembre 2025

- ▶ **Risques en matière d'approvisionnement :** les risques liés à l'inefficacité et à la corruption dans le domaine des achats publics réduisent la valeur réelle des budgets technologiques. Cette situation fait apparaître le besoin d'adopter des systèmes ouverts, flexibles et rentables qui peuvent subsister en dépit des coupes budgétaires et des changements politiques, tout en évitant d'enfermer les pays dans une dépendance vis-à-vis de fournisseurs propriétaires rigides et coûteux.

Notre approche en matière de souveraineté numérique

Pour mener à bien leur mission, les organismes publics du monde entier doivent aborder la souveraineté sous tous ces aspects. Chez Red Hat, nous proposons les outils et l'écosystème nécessaires pour comprendre chacun d'entre eux.

Souveraineté des données et IA

Nous avons compris l'importance de l'autonomie et du contrôle complet sur les données critiques et les modèles d'IA, pour garantir la résidence des données au sein des frontières nationales et une gouvernance conforme aux réglementations locales. Les organismes publics doivent mettre en œuvre des stratégies d'IA souveraine pour conserver la propriété de leurs modèles et de leurs données d'entraînement, en les déployant sur une infrastructure locale plutôt qu'en utilisant des API pour accéder à des modèles contrôlés par des acteurs étrangers. La solution Red Hat® OpenShift® AI permet de déployer des capacités d'IA souveraines là où sont stockées les données. Nous renforçons le contrôle sur l'accès aux données et leur emplacement en utilisant l'informatique confidentielle pour protéger les données en cours d'utilisation, et ainsi garantir la conformité avec des réglementations telles que la loi sur l'IA de l'UE.

Souveraineté technologique

Pour garantir l'indépendance à long terme et déplacer les applications sans restrictions, il faut pouvoir exécuter des charges de travail sans dépendre de l'infrastructure ou des logiciels propriétaires d'un fournisseur spécifique. Les gouvernements doivent éviter toute dépendance vis-à-vis d'un fournisseur en adoptant des normes ouvertes et des plateformes de conteneurisation portables. En cas de changement des politiques d'un fournisseur de services cloud ou de hausse des tensions géopolitiques, les charges de travail peuvent être migrées vers une autre infrastructure sans remaniement. Chez Red Hat, nous limitons la dépendance vis-à-vis d'un fournisseur grâce aux normes Open Source. Notre plateforme prend en charge plusieurs architectures matérielles (x86, ARM et RISC-V), ce qui permet aux gouvernements de faire évoluer et mettre à jour leurs systèmes nationaux selon leur propre calendrier, en faisant abstraction des dépendances externes.

Souveraineté de l'exploitation

Pour survivre et fonctionner même en cas de déconnexion, les organismes publics doivent conserver tout le contrôle administratif de l'infrastructure informatique ainsi qu'une indépendance totale. L'infrastructure essentielle et de défense doit accorder la priorité à la résilience opérationnelle. Cette infrastructure implique l'automatisation des plans de récupération après sinistre qui tiennent compte des conditions liées aux temps de guerre. Elle implique aussi de s'assurer que l'assistance et l'exploitation sont gérées par des citoyens locaux qui disposent des autorisations de sécurité nécessaires. À titre d'exemple, nous proposons une assistance souveraine vérifiée, c'est-à-dire une assistance technique fournie par des citoyens locaux habilités (par exemple, au sein de l'UE) avec la garantie qu'aucune des données auxquelles l'équipe d'assistance peut accéder ne quitte le territoire. Par ailleurs, la solution Red Hat Ansible® Automation Platform automatise la résilience et accélère la récupération et l'application des correctifs, même dans les environnements confrontés à des problèmes de réseau (refus, déconnexion, intermittence et faible bande passante).

Souveraineté de l'assurance

La vérification indépendante de l'intégrité, de la sécurité et de la fiabilité des systèmes et processus numériques permet aux organismes de garantir leur conformité. Il leur faut passer d'une approche de confiance absolue à une confiance vérifiable, ce qui nécessite un audit rigoureux de la chaîne d'approvisionnement des logiciels et la preuve de sa conformité avec différentes normes (Critères communs, FIPS, NIS 2, etc.). Chez Red Hat, nous proposons une chaîne d'approvisionnement des logiciels fiable, permettant de distribuer des logiciels signés de manière cryptographique, dont la

provenance est vérifiée et qui sont accompagnés d'une nomenclature logicielle. Les organismes peuvent ainsi vérifier chaque composant et s'assurer qu'aucun code malveillant n'a été injecté. Grâce à ces mesures de sécurité, ils peuvent s'assurer de respecter les nouvelles exigences, notamment la loi européenne sur la cyberrésilience.

L'autonomie stratégique grâce à l'Open Source

Chez Red Hat, nous nous appuyons sur une base ouverte et flexible pour relever les défis et offrir aux organismes publics davantage de choix et de contrôle. Cette approche flexible tient compte du fait qu'il est rare qu'un seul fournisseur puisse garantir la souveraineté numérique. C'est pourquoi nous offrons la possibilité de créer un cloud souverain qui englobe plusieurs fournisseurs d'infrastructure et zones de cloud computing, afin de contourner les limites d'une solution unique.

Depuis plus de 30 ans, nous fournissons aux entreprises des solutions Open Source fiables qui respectent les exigences les plus strictes en matière de sécurité et de conformité. Plus que de simples technologies, les logiciels Open Source d'entreprise offrent aux organismes publics une base architecturale essentielle pour mettre en place une véritable souveraineté numérique et une autonomie stratégique. Contrairement aux solutions propriétaires qui s'appuient sur des systèmes fermés et opaques et qui exigent une confiance absolue, nos solutions aident les organismes publics à garder un contrôle total sur leur évolution numérique au lieu de dépendre d'autres acteurs. Cette approche ouverte permet à l'ensemble du secteur public de maîtriser la vitesse de l'innovation mondiale, de la périphérie tactique du réseau à l'IA souveraine, tout en veillant à ce que les charges de travail restent portables et résilientes. L'adoption d'une approche Open Source permet également d'éviter la dépendance vis-à-vis d'un fournisseur ainsi que l'obsolescence technologique. En utilisant des technologies Open Source, nous nous alignons sur le principe de l'ouverture par défaut qui est répandu dans des régions telles que l'UE. Ce modèle permet d'éviter la dépendance vis-à-vis d'un seul fournisseur ainsi que d'effectuer des inspections et des modifications du code, des aspects qui deviennent essentiels pour renforcer la sécurité nationale et la confiance.

▶ **Confiance et transparence**

Notre modèle Open Source est totalement transparent et laisse aux organismes publics la liberté d'inspecter le code source, de contrôler la sécurité et de vérifier les chaînes d'approvisionnement des logiciels. Ce niveau d'auditabilité est essentiel pour répondre aux exigences d'assurance dans les régions EMEA et APAC. En outre, nous proposons des logiciels signés de manière cryptographique dont la provenance a été vérifiée afin de répondre aux nouvelles exigences, notamment la [loi européenne sur la cyberrésilience](#).

▶ **Souveraineté de l'exploitation et assistance locale**

Pour gérer les risques liés à l'application des différentes règles, nous aidons les entreprises à contrôler les utilisateurs en charge de l'infrastructure et ainsi garantir la souveraineté de l'exploitation.

- ▶ **Assistance souveraine** : comme nous l'avons déjà mentionné, nous proposons une assistance souveraine vérifiée au sein de l'UE, avec la garantie que l'assistance technique est fournie exclusivement par des citoyens habilités qui sont situés dans l'Union européenne. Cette assistance technique permet de s'assurer qu'aucune des données auxquelles l'équipe d'assistance peut accéder ne quitte la région.
- ▶ **Écosystèmes locaux** : nous proposons un écosystème de partenaires composé de fournisseurs locaux de services cloud qui sont certifiés, pour donner accès à des fonctionnalités de cloud souverain qui respectent les réglementations strictes en matière de résidence nationale des données.

▶ **Indépendance technologique**

Avec une stratégie de cloud hybride ouvert, les charges de travail peuvent s'exécuter dans divers environnements, par exemple sur site, dans un cloud privé, à la périphérie tactique du réseau ou dans un environnement air gap.

- ▶ **Portabilité** : cet aspect est essentiel pour éviter la dépendance vis-à-vis d'un fournisseur, une préoccupation majeure pour les organismes publics, en particulier dans les régions LATAM et APAC. La capacité de ces régions à migrer efficacement les charges de travail et les données est primordiale pour garantir la continuité des services et une réponse efficace aux évolutions géopolitiques, tels que les basculements politiques ou économiques qui peuvent nécessiter un changement de fournisseur technologique.
- ▶ **Environnements d'exploitation déconnectés** : pour les organismes de défense, nos solutions telles que Red Hat Device Edge et Red Hat OpenShift permettent aux systèmes de fonctionner de manière autonome dans des environnements déconnectés et confrontés à des problèmes de réseau (refus, déconnexion, intermittence et faible bande passante), pour ainsi garantir l'exécution des missions, même lorsque le cloud central est inaccessible.

Nous proposons aux organismes publics une base ouverte pour créer un cloud souverain qui peut résister à l'incertitude, assurer la sécurité des données et garantir le bon fonctionnement du pays.

▶ IA souveraine

Pour faciliter la mise en place de l'IA souveraine, nous proposons une plateforme aux gouvernements qui cherchent à développer l'IA. Cette plateforme aide les pays à conserver la propriété de leurs modèles et de leurs données d'entraînement, en les déployant sur une infrastructure locale pour respecter les réglementations (notamment la loi européenne sur l'IA), plutôt qu'en utilisant des API pour accéder à des modèles contrôlés par des acteurs étrangers.

Les avantages de Red Hat pour les organismes publics

Partenaire de confiance des organismes publics, nous proposons des solutions qui sont déployées dans l'intégralité des départements exécutifs des États-Unis³, et largement utilisées dans les pays de l'OTAN et d'autres ministères de la défense. Grâce à notre modèle de licence et à notre engagement envers les normes ouvertes, les organismes publics ne sont jamais liés à un fournisseur de façon perpétuelle. Ils conservent le droit d'utiliser des logiciels indéfiniment et d'en assurer le bon fonctionnement, ce qui leur permet de protéger leurs investissements à long terme contre les feuilles de route changeantes de leurs fournisseurs ou les restrictions géopolitiques.

Tandis que les dépenses augmentent, en particulier dans le secteur de la défense, notre gamme de solutions et de services permet de générer un réel retour sur investissement. Les engagements en matière de dépenses des pays membres de l'[OTAN](#) vont doubler, pour atteindre 5 % du PIB national d'ici 2035⁴. En utilisant une plateforme unifiée pour standardiser leurs systèmes, les organismes publics peuvent réallouer les investissements auparavant consacrés à la maintenance de systèmes conventionnels fragmentés à la génération de nouvelles capacités de mission, et réduire ainsi considérablement les coûts d'exploitation et le coût total de possession.

Et maintenant ?

- ▶ Découvrez les [solutions de Red Hat pour le secteur public dans le monde entier](#) et parlez avec un représentant Red Hat.
- ▶ Vous souhaitez évaluer votre niveau de préparation à la souveraineté numérique ? [Lisez cet article de blog](#) pour en savoir plus.



À propos de Red Hat

Premier éditeur mondial de solutions logicielles Open Source d'entreprise, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et à automatiser des environnements complexes. [Conseiller de confiance auprès des entreprises du Fortune 500](#), Red Hat propose des services d'assistance, de formation et de consulting [primés](#) qui apportent à tous les secteurs les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

3 Données clients Red Hat, septembre 2025

4 « [Dépenses de défense et engagement des 5 %](#) », OTAN, 18 décembre 2025