Souveraineté numérique : de l'enjeu politique à la nécessité stratégique

Face à des dépendances technologiques croissantes, la souveraineté numérique devient un véritable enjeu de maîtrise, de résilience et de continuité pour les organisations. Bertrand Merlier, Architecte solution et expert IA chez Sopra Steria Suisse, en décrypte les principaux enjeux et les leviers d'action.

Souveraineté numérique : Sujet purement politique ou nécessité pour toute organisation ?

Bertrand Merlier : La souveraineté numérique s'impose aujourd'hui comme un enjeu stratégique majeur dans un contexte géopolitique marqué par des tensions croissantes et une compétition accrue autour des données, des infrastructures et des technologies critiques. En Europe ou en Suisse, la dépendance de nombreux acteurs à des fournisseurs étrangers soulève des questions de maîtrise, de sécurité et de résilience. Face à ces défis, les organisations doivent arbitrer entre innovation, conformité réglementaire, et maîtrise des risques.

Les autorités se sont saisies du sujet. En décembre 2025, le Conseil fédéral a fait de la souveraineté numérique la priorité de sa stratégie Suisse numérique 2026, avec des lignes directrices pour l'administration fédérale et la confirmation du Swiss Government Cloud. Aux Swiss Cyber Security Days de février 2026, le chancelier de la Confédération Viktor Rossi a livré la formule suivante : est souverain celui qui connaît ses dépendances. Non pas celui qui s'isole, mais celui qui se crée des options et les réduit là où c'est utile.

—

Le mot souveraineté numérique s'est donc visiblement installé dans les discours publics. Mais au-delà des décisions politiques ou stratégiques, la souveraineté s'applique-t-elle à toutes les organisations ?

Bertrand Merlier : La définition du chancelier que nous venons de citer se rapproche fortement de notre vision chez Sopra Steria. La souveraineté numérique n'est pas une nécessité absolue pour tous, ni nécessaire au même niveau pour toute organisation. Se poser la question, en revanche, est indispensable.

Ce sujet doit être étudié avec un objectif clair : conserver la capacité de fonctionner de manière indépendante là où cela est nécessaire, protéger ce qui est stratégique, penser à la souveraineté mais aussi à la résilience numérique.

Un point mérite d'être clarifié, car la confusion est fréquente : souveraineté et résilience sont deux sujets distincts. La première porte sur la maîtrise : qui décide, qui opère, sous quelle loi. La seconde porte sur la continuité, la capacité à absorber un incident et à repartir. Elles se renforcent souvent, mais peuvent aussi s'opposer : reprendre en interne un service que l'on ne sait pas bien exploiter, ou renoncer à une redondance assurée par un tiers, augmente la maîtrise et la souveraineté, mais peut diminuer la résilience en fragilisant la continuité.

Souveraineté et résilience doivent donc être traitées ensemble, et arbitrées.

Les réponses et les choix sont donc propres à chaque entité publique ou privée, car construits à partir de contraintes multiples : stratégiques, opérationnelles, légales, ou politiques.

—

La souveraineté est donc un sujet à facettes multiples. Comment une organisation peut-elle concrètement s'approprier ce sujet ?

Bertrand Merlier : Derrière le concept de souveraineté se dessinent quatre dimensions complémentaires. Les examiner individuellement est nécessaire pour comprendre les enjeux, évaluer la position et les risques, et définir les chantiers prioritaires.

La souveraineté stratégique. C'est la capacité à maîtriser les ressources pour préserver son autonomie de décision et d'action. Le point central est de définir ce que la souveraineté signifie pour soi, quels sont les risques dans la situation actuelle, et dans quelle mesure ils sont acceptables ou doivent faire l'objet de plans de mitigation. Un bon exemple est celui d'une organisation publique dont la stratégie et le rôle impliquent une disponibilité permanente des services à la population. Elle doit donc s'assurer qu'ils sont opérables et adaptables, quelles que soient les décisions commerciales d'un fournisseur, l'environnement légal sous lequel il opère, ou les décisions politiques extérieures.



Bertrand Merlier,
Architecte solution et expert IA,
Sopra Steria Suisse

© Sopra Steria Suisse

La souveraineté des données. Au cœur des enjeux numériques, elle repose sur la maîtrise des processus associés à leur collecte, leur stockage, leur accès et leur utilisation. Certains services peuvent être opérés par des fournisseurs externes, ce qui est un choix légitime, à condition de savoir précisément ce qui est délégué. La question centrale est où résident les données les plus sensibles, et qui définit les règles d'accès, de partage et d'usage ? Exemple : pour le dossier RH d'un employé ou les données médicales d'un citoyen, savoir qui administre les comptes, qui détient les clés de chiffrement et sous quel régime légal, local ou étranger, est placé le fournisseur du service doit faire l'objet d'une analyse.

La souveraineté technique. Elle est la capacité d'une organisation à conserver la maîtrise de ses infrastructures, plateformes et applications numériques. Elle repose également sur sa faculté à changer de fournisseurs, de technologies ou d'environnements sans dépendance excessive, garantissant ainsi son autonomie et sa liberté de choix. L'analyse de ce sujet implique une cartographie de l'exposition : identifier l'ensemble des composants, les compétences internes et sous-traitances, les contrats et les régimes juridiques applicables, les conditions de sortie... Exemple courant : une application métier soutient une activité qualifiée d'essentielle, mais elle est exploitée par un fournisseur unique, dans un format de données propriétaire et sans accès aux journaux techniques. La question à trancher sera de savoir si le niveau de souveraineté attendu sur cette activité est adéquat.

La souveraineté opérationnelle. Elle est la capacité d'une organisation à maintenir la continuité, la maîtrise et l'efficacité d'activités qu'elle va qualifier d'essentielles, ceci indépendamment de ses fournisseurs, partenaires ou prestataires technologiques, donc même en situation de dépendance technologique ou de perturbation externe. Par exemple, une entreprise qui exploite des services cloud peut garder une souveraineté opérationnelle dans la mesure où elle conserve en interne des compétences et des rôles clés pour l'administrer, des procédures de bascule vers un mode de maintien des services en cas de défaut, et conserve le choix et la capacité à remplacer ces services le cas échéant.

—

On voit que les sujets à analyser sont nombreux, les décisions à prendre peuvent être complexes. Comment peut-on mettre en place une démarche pertinente et efficace ?

Bertrand Merlier : Ce chantier ne se construit pas du jour au lendemain. C'est un vrai projet qui va devoir être mis en place, de l'analyse initiale à la mise en œuvre des transformations choisies. L'essentiel est de savoir quoi prioriser et comment rester maître de ses décisions dans la durée. Sopra Steria propose une démarche pour accompagner les organisations en trois étapes.

Définir les priorités. Obtenir une vision claire des processus, données et systèmes les plus stratégiques, et des domaines où l'autonomie est essentielle. Le livrable utile est un registre des actifs critiques, validé par les métiers autant que par l'informatique.

Évaluer les risques et les dépendances. Identifier ce qui pourrait fragiliser la conformité, les opérations ou l'autonomie, et comprendre où se logent les dépendances : technologies, fournisseurs, données, écosystèmes tiers. Une matrice croisant dépendance, impact métier et délai de substitution met en évidence les priorités et objective les arbitrages entre maîtrise.

Construire sa feuille de route. Séquencer les évolutions selon leur urgence, en tenant compte des exigences réglementaires à plus long terme. Une feuille de route lisible distingue ce qui relève du contrat, ce qui relève de l'architecture et ce qui suppose une transformation. C'est aussi le moment où un regard extérieur apporte les comparaisons qui font gagner du temps.

Cette démarche doit être accompagnée d'une gouvernance claire, qui définit les responsabilités et assure le pilotage du projet dans la durée.

—

Et l'intelligence artificielle ?

Bertrand Merlier : L'IA rejoue les quatre dimensions précédentes, plus rapidement et quelquefois sur les données les plus sensibles. La question est : quelle maîtrise a-t-on de la logique de décision, de la conformité légale et de l'infrastructure qui héberge les traitements ? Poser un cadre de l'utilisation de l'IA, pendant que les usages restent peu nombreux, évite de reconstituer en quelques mois des dépendances que l'on vient de réduire ailleurs.

C'est dans cette logique que nous avons développé l'IA Backbone, notre plateforme IA qui sépare les usages métiers du fournisseur de modèle : un cas d'usage développé reste exploitable si le modèle sous-jacent évolue ou change. C'est le principe de réversibilité appliqué à la couche la plus mouvante du système d'information.

—

Les organisations en Suisse ont-elles intérêt à attendre que l'offre souveraine publique se structure davantage, ou peuvent-elles passer à l'action dès aujourd'hui ?

Bertrand Merlier : Notre préconisation est que la démarche peut et doit démarrer aujourd'hui, à l'échelle qui convient. Aucun programme extérieur ne remplace le travail d'analyse propre à chaque organisation. Une bonne gouvernance intégrera au cours de la démarche les événements externes et les possibilités qui s'offrent.

L'offre souveraine en Europe et en Suisse se structure en effet rapidement. Le Swiss Government Cloud, destiné aux collectivités publiques, délivrera ses premiers services opérationnels en 2027, et est déjà planifié jusqu'en 2032. En Europe, plusieurs initiatives - auxquelles Sopra Steria participe comme acteur de référence dans la cybersécurité, la défense, la data, et l'IA de confiance - structurent l'écosystème : Gaia-X, Digital Europe ou l'European Sovereign Tech Industry Alliance (ESTIA).

Reste une bonne nouvelle : ce qui renforce la souveraineté et la résilience d'une organisation, à savoir des formats ouverts, une réversibilité éprouvée, une documentation à jour et une architecture modulaire, est exactement ce qui la rend modernisable. La souveraineté n'est pas un coût de protection, c'est une opportunité qui crée la base de l'agilité, de la capacité d'innover, et donc de la longévité.