



Livre blanc **Souveraineté numérique** Exploiter l'innovation et garder le contrôle



Contenu

Souveraineté numérique – une question clé de notre époque	3
La souveraineté numérique dans l’œil de l’expert: entretien avec le professeur Matthias Stürmer	6
Leviers importants pour la souveraineté numérique: stockage et chiffrement des données	8
La souveraineté numérique dans l’œil de l’expert: entretien avec David Rosenthal	11
Conclusion: celui qui garde la capacité d’agir est souverain	12

Souveraineté numérique – une question clé de notre époque

Les technologies numériques façonnent presque tous les domaines de la vie et de l'économie. Les activités de l'État, la création de valeur économique et le quotidien de la société reposent sur les infrastructures numériques. Dans le même temps, le marché technologique mondial est dominé par quelques grands prestataires. Ils font avancer les innovations, mais créent également des dépendances. C'est pourquoi la souveraineté numérique occupe une place de plus en plus centrale.

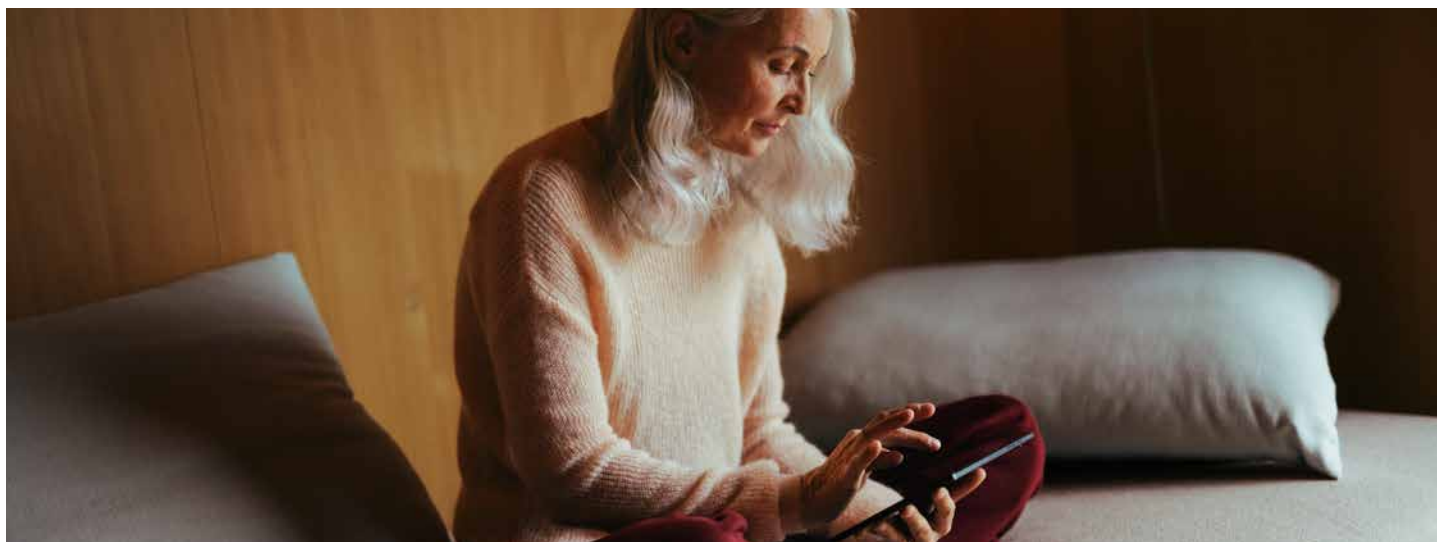
Une chose est sûre: les entreprises et la société ne peuvent plus se passer des possibilités numériques. Un renoncement total à des solutions étrangères n'est pas non plus réaliste ou pertinent sur le marché globalisé.

Ce livre blanc pose donc la question de l'équilibre: comment les autorités, les entreprises et les organisations peuvent-elles profiter de l'innovation tout en gardant le contrôle sur leurs données, leurs systèmes et leurs ressources numériques? En bref: comment parvenir à la souveraineté numérique dans un monde globalisé et connecté?

Swiss Post Digital – pour une Suisse numérique forte

Pour la Poste, la souveraineté numérique signifie utiliser l'innovation tout en gardant le contrôle sur les données, la sécurité et les processus critiques. Il est essentiel que les organisations comprennent leurs risques, gèrent consciemment les dépendances et restent capables d'agir à tout moment. La Poste propose différentes solutions pour la communication numérique sécurisée, des solutions logicielles interopérables et des services de cybersécurité. Des architectures de solutions ouvertes, la protection des données et des méthodes de chiffrement ultramodernes garantissent la souveraineté numérique des solutions de la Poste.

En outre, la Poste s'engage dans le réseau «SDS – Suisse numérique souveraine», tant au sein du comité consultatif que du réseau, afin de promouvoir l'échange et de contribuer à façonner la souveraineté numérique en Suisse.



Du mot-clé à la définition concrète

Il n'existe pas encore de définition uniforme de la souveraineté numérique. Selon la perspective, elle comprend différentes attentes en matière de technologie, de données et d'infrastructure. Il est largement admis que la souveraineté numérique décrit la capacité à utiliser les technologies numériques de manière autonome et à garder le contrôle sur les données, les systèmes et les processus numériques.

Le Conseil fédéral définit la souveraineté numérique comme suit: «La souveraineté numérique recouvre le fait de disposer d'une capacité de contrôle et d'action nécessaire dans l'espace numérique afin de garantir l'exécution des tâches publiques.»¹

Découvrez dans le livre blanc d'autres solutions concrètes pour une numérisation efficace et sûre.

IncaMail

IncaMail est le service de chiffrement d'e-mails sécurisé de la Poste. Avec IncaMail, les entreprises, les autorités et les particuliers peuvent envoyer par e-mail des informations et des documents confidentiels chiffrés, traçables et conformes à la protection des données (conformes à la LPD et au RGPD).



- L'infrastructure par laquelle passent la réception et la transmission globales de messages IncaMail aux destinataires est exploitée en Suisse.
- Le portail client via lequel les messages IncaMail peuvent également être consultés en ligne est hébergé dans le cloud. Toutefois, aucune donnée n'est conservée dans le cloud. Chaque requête passe par l'infrastructure locale, qui est chiffrée.



¹ Conseil fédéral (2025): Souveraineté numérique de la Suisse. Rapport du Conseil fédéral en réponse au postulat 22.4411 Z'graggen «Souveraineté numérique de la Suisse», Berne, 26 novembre 2025, chapitre 5.1 Définition.

La souveraineté numérique repose sur quatre principes

Avec des architectures de solutions ouvertes, les organisations peuvent éviter les dépendances afin de rester opérationnelles à tout moment. Quatre principes servent d'instructions opérationnelles:

1 Identifier les données critiques

Les données doivent être classées en fonction du besoin de protection et des exigences réglementaires. Toutes les informations ne nécessitent pas les mêmes mesures de protection. Une approche différenciée est particulièrement décisive pour l'utilisation de services de cloud.

2 Protéger efficacement les données

Un chiffrement fort, une propre gestion des clés, des architectures Zero Trust ainsi que des concepts d'accès et d'autorisation clairs constituent la base de la protection des données.

3 Créer des alternatives

Quiconque planifie des scénarios de sortie, réduit les dépendances vis-à-vis des différents prestataires et mise sur des interfaces ouvertes et des normes conserve sa capacité d'agir.

4 Renforcer les compétences dans l'entreprise

La souveraineté numérique ne naît pas uniquement de la technologie. Il est essentiel que les membres du personnel et les cadres comprennent les opportunités, les risques et les dépendances et puissent prendre des décisions fondées.

La lettre numérique



La Poste met à disposition une infrastructure pour l'envoi et la réception numériques de lettres et fait ainsi entrer le secret épistolaire dans l'ère numérique. La lettre numérique fait partie du mandat de service universel de la Poste depuis 2026.

- La lettre numérique est traitée en Suisse. L'infrastructure cloud moderne permet le traitement sécurisé de gros volumes d'envois et une protection élevée contre les cyberrisques. Grâce à une gestion des clés séparée, le fournisseur de services de cloud n'a pas accès aux contenus des lettres.
- Si la lettre est distribuée, elle n'est lisible que par la ou le destinataire. Ni la Poste ni des tiers n'ont la possibilité d'accéder aux contenus des lettres.
- La plateforme respecte les dispositions de l'ordonnance sur la poste, a été soumise à une analyse d'impact relative à la protection des données auprès du PFPDT et a été contrôlée par la PostCom.

La souveraineté numérique dans l'œil de l'expert:

entretien avec le professeur Matthias Stürmer

Deux experts, deux perspectives: le professeur Matthias Stürmer et David Rosenthal font le point et partagent leur vision des opportunités, des risques et des options d'action. Découvrez l'entretien avec Matthias Stürmer ci-dessous, celui avec David Rosenthal en page 11.

Monsieur Stürmer, les critiques disent que la souveraineté est un signe d'isolement. Où s'arrête la souveraineté et où commence l'autarcie?

Nous vivons dans une société connectée et il ne serait ni judicieux ni réaliste de vouloir tout produire ou exploiter soi-même. La souveraineté numérique n'est pas synonyme d'isolement, mais d'indépendance et de liberté décisionnelle. Concrètement, l'important est la capacité à changer de fournisseurs car, en fin de compte, il en résulte davantage de concurrence et d'innovation. En Suisse et dans le secteur informatique en général, nous avons un important retard à rattraper à cet égard. Un changement est possible si nous l'abordons concrètement.

Quelles questions les autorités et les organisations devraient-elles donc se poser aujourd'hui?

Une question centrale est la suivante: comment pouvons-nous réduire les dépendances vis-à-vis des entreprises informatiques, c'est-à-dire le «Vendor Lock-In»? Cela commence par s'informer sur le marché suisse des prestataires informatiques. On part souvent du principe que seuls les fournisseurs informatiques américains connus proposent les services de cloud demandés. Mais si l'on regarde autour de nous, on constate que nous avons aussi beaucoup d'entreprises informatiques compétentes et innovantes en Suisse.

«La souveraineté numérique n'est pas synonyme d'isolement, mais de liberté décisionnelle»

Un argument fréquent est que les hyperscalers sont meilleurs en matière de cybersécurité. Qu'en pensez-vous?

Les grands prestataires disposent sans aucun doute de davantage de ressources. Mais ils constituent aussi une cible plus attrayante. Si une attaque réussit, de très nombreuses données sont potentiellement concernées. La cybersécurité n'est pas un argument pour ou contre un prestataire – c'est une mission permanente pour toutes et tous. En fin de compte, les autorités, les entreprises et les petits prestataires poursuivent le même objectif.

D'autres pays sont-ils plus avancés que la Suisse en matière de souveraineté numérique?

Oui. Depuis des années, l'Allemagne investit de manière ciblée dans des solutions cloud indépendantes et des logiciels open source et elle a créé son propre centre pour la souveraineté numérique, ZenDiS, qui propose openDesk comme alternative à M365. Avec «La Suite», la France poursuit elle aussi une approche étatique courageuse pour mettre concrètement en œuvre la

souveraineté numérique. En Suisse, on pense encore souvent que seuls les grands groupes Big Tech peuvent fournir de bonnes prestations informatiques.

Que doit faire concrètement la Suisse au cours des trois prochaines années pour gagner en souveraineté sur le plan numérique?

Nous avons besoin d'un centre national pour la souveraineté numérique. Un service qui regroupe les connaissances spécialisées, conseille les autorités et assure le transfert de savoir-faire. Avec la création du centre SDS – Suisse numérique souveraine, nous avons franchi une première étape à la BFH. Le besoin est énorme: je reçois chaque jour des demandes de la part de l'administration, du monde politique et des organisations. La pression politique augmente sensiblement, de gauche à droite. Il faut maintenant investir dans les bases et dans une mise en œuvre coordonnée.



À propos de l'expert:

Le professeur Matthias Stürmer est responsable de l'Institut Public Sector Transformation de la Haute école spécialisée de Berne (BFH) et professeur à l'Institut d'informatique de l'Université de Berne. Il est l'un des experts suisses les plus connus en matière de souveraineté numérique, d'open source et de numérisation de l'État et de la société.

Cloud sécurisé Tresorit



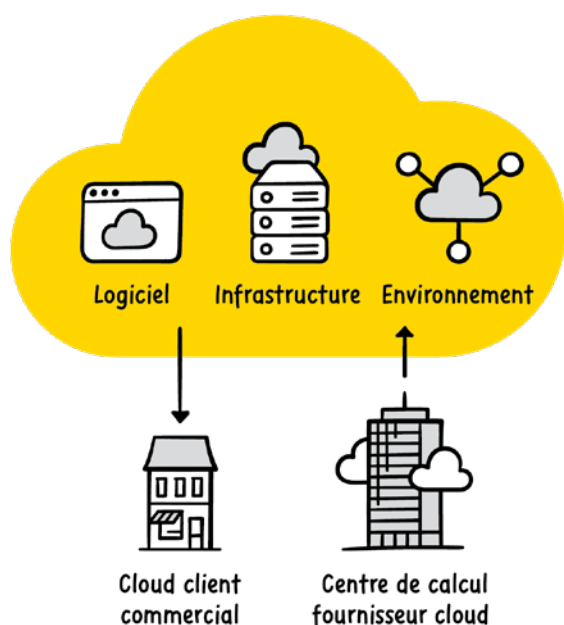
En tant que composante de la souveraineté numérique, la souveraineté des données se manifeste particulièrement là où les données sont partagées et traitées en commun. Qu'il s'agisse de la collaboration avec des équipes, une clientèle et des partenaires ou de l'échange sécurisé de documents sensibles: avec des solutions comme le cloud sécurisé de Tresorit, les entreprises organisent la collaboration numérique de manière sûre et efficace tout en conservant la maîtrise de leurs données, des droits d'accès et des lieux de stockage.

- Le chiffrement de bout en bout garantit que seules les personnes autorisées peuvent accéder aux contenus. L'architecture Zero Knowledge garantit que les entreprises conservent le contrôle de leurs clés cryptographiques.
- Pour que les entreprises puissent honorer leurs obligations réglementaires et organisationnelles individuelles, des options flexibles de localisation des données sont disponibles dans l'UE, en Suisse et dans d'autres régions.

Leviers importants pour la souveraineté numérique:

stockage et chiffrement des données

Plateformes numériques, analyses de données et intelligence artificielle: le développement et l'exploitation de solutions numériques nécessitent des infrastructures performantes. Les organisations peuvent utiliser de manière flexible la puissance de calcul, l'espace de stockage et les logiciels en tant que prestation via des services cloud. Elles ont ainsi accès aux technologies les plus modernes, peuvent mettre des innovations plus rapidement en œuvre et adapter l'utilisation aux besoins.



Civetica Cloud



Civetica est la plateforme e-government de la Poste qui rassemble les processus administratifs communaux de bout en bout dans un environnement uniforme, sûr et contrôlé. Elle remplace des solutions individuelles isolées par une solution globale intégrée. Environ 20% des communes suisses misent sur la solution ERP Civetica.

- Civetica Cloud stocke exclusivement les données dans des centres de calcul en Suisse.
- La solution garantit une localisation contrôlée des données et une approche adaptée aux exigences de souveraineté des organisations suisses.

Cloud mais pas vraiment cloud

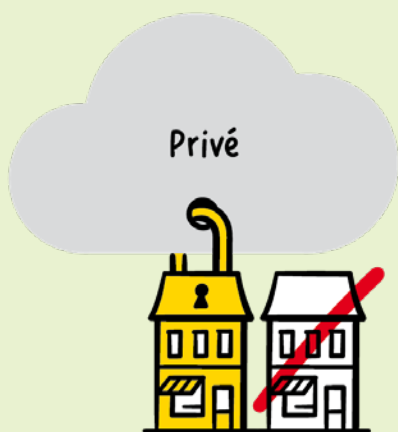
Dans le contexte des services de cloud et de la souveraineté numérique, la question centrale est la suivante: qui peut accéder à l'infrastructure de cloud et comment les données sont-elles protégées dans le cloud?

En fonction des exigences et des conditions-cadres réglementaires, différents environnements cloud sont recommandés. Le chiffrement des données et la gestion des clés sont également décisifs.

Quels sont les services de cloud existants?

Privé

Un environnement cloud dédié qui n'est utilisé que par une seule organisation. Il peut être exploité dans le propre centre de calcul ou par un prestataire tiers externe et offre un contrôle et une sécurité accrus.



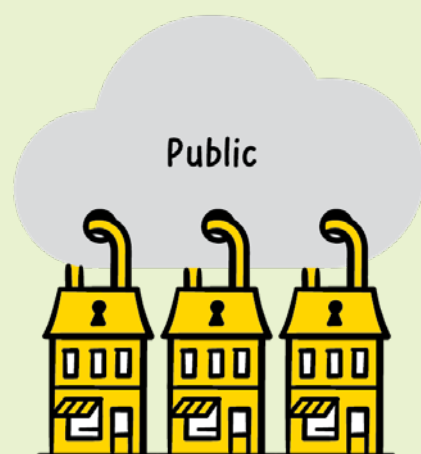
Forme mixte

Combinaison de cloud public et privé dans laquelle les données et les applications peuvent être migrées entre les deux environnements en fonction des exigences.



Public

Les ressources informatiques sont mises à disposition par un prestataire tiers externe via l'Internet public et utilisées en commun par plusieurs clientes et clients.



Sécurité de vos données

Le prestataire peut-il consulter les données enregistrées dans le cloud? Si des données sensibles sont traitées dans un environnement cloud, des mesures organisationnelles et techniques devraient garantir que seuls les services autorisés ont accès aux données. Le fournisseur de services de cloud peut être explicitement exclu de l'accès par une gestion séparée des clés.

Les mesures suivantes protègent les données et les services dans le cloud:

- **Propre gestion des clés:** l'organisation gère elle-même les clés de chiffrement et garde ainsi le contrôle sur l'accès aux données.
- **Chiffrement des données:** les données restent protégées pendant l'enregistrement et la transmission et ne sont pas lisibles par des tiers.
- **Concepts d'accès et d'autorisation:** seules les personnes autorisées ont accès aux systèmes et aux informations.
- **Contrôle continu des risques et de la sécurité:** des assessments réguliers garantissent que les exigences en matière de sécurité, de protection des données et de compliance sont respectées.

Souveraineté avec un prestataire de services cloud global?

Les grandes entreprises mondiales jouent un rôle central sur le marché du cloud. Elles exploitent des infrastructures réparties dans le monde entier et investissent chaque année des montants élevés dans la sécurité, le développement et l'innovation technologique. Elles permettent ainsi un accès rapide aux technologies modernes, une disponibilité élevée et une utilisation économique efficace des ressources informatiques.

Les organisations qui souhaitent profiter de ces avantages tout en garantissant l'indépendance de leurs services et la protection de leurs données devraient opter sciemment pour l'environnement cloud:

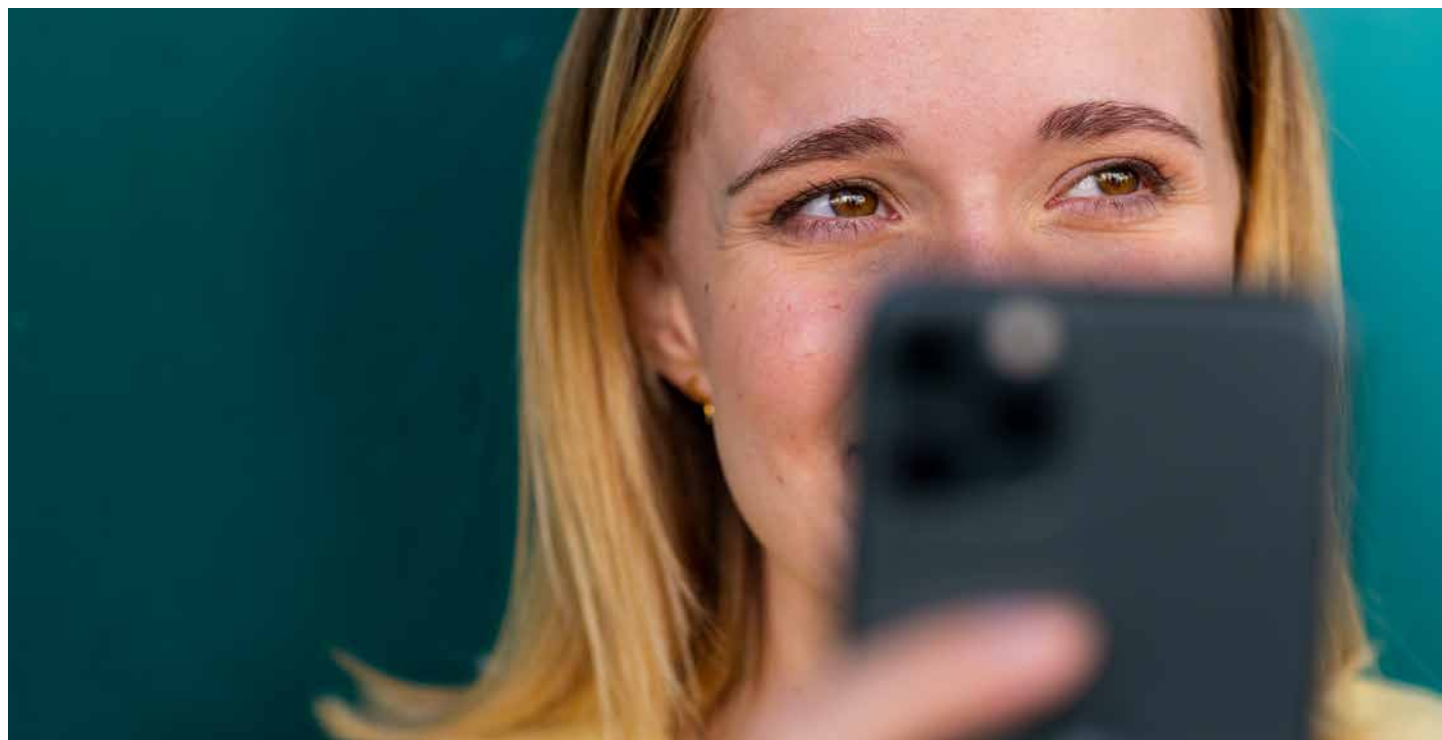
- Choisir l'environnement cloud: cloud privé, cloud public, forme mixte
- Définir le concept d'accès et de chiffrement et assurer un examen continu de la sécurité et des risques

Certificats TLS

Les certificats TLS (Transport Layer Security) confirment l'identité et l'authenticité des sites web (domaines) et des organisations et permettent la transmission chiffrée de données entre utilisatrices/utilisateurs et services en ligne. En tant qu'élément central d'une infrastructure sécurisée, ils constituent la base de la confiance sur Internet et dans la communication numérique. Seul fournisseur suisse de certificats TLS, le Trust Service Provider SwissSign contribue à un écosystème numérique digne de confiance.



- L'infrastructure de confiance est exploitée par SwissSign en Suisse et sous son propre contrôle dans des centres de calcul géographiquement redondants.
- Avec ce produit, les organisations peuvent utiliser des certificats TLS reconnus au niveau international, tandis que la gouvernance, le contrôle et la compétence juridique restent en Suisse.



La souveraineté numérique dans l'œil de l'expert:

entretien avec David Rosenthal

Monsieur Rosenthal, beaucoup mettent en garde contre les dépendances vis-à-vis des fournisseurs de cloud américains. À votre avis, ce risque est-il surestimé ou sous-estimé?

Il est mal placé. La plupart craignent cette dépendance parce que les prestataires viennent des États-Unis. Pour moi, le plus gros problème vient de la position dominante et du cumul des risques. Ceci étant, l'informatique a toujours été tributaire de certaines interdépendances, qui n'ont jamais été bonnes, mais qui sont inévitables. Il n'y a pas de recette miracle.

L'US CLOUD ACT est souvent au cœur des débats: dans quelle mesure le danger d'un accès aux données suisses est-il réel en pratique?

Ce danger est surestimé. Premièrement, le CLOUD Act n'a rien de spécial; nous avons pratiquement la même chose en Suisse. Deuxièmement, il existe des mesures correctives, même sans chiffrage de bout en bout; malheureusement, certains avertisseurs l'ignorent systématiquement. Troisièmement, les autorités américaines reçoivent des données de Suisse, même sans CLOUD Act, et ce de manière tout à fait légale via l'entraide judiciaire. Se focaliser comme on le voit souvent sur le CLOUD Act détourne l'attention de risques nettement plus importants, tels que le danger des hackers: il existe un peu partout une grande réserve vis-à-vis des solutions cloud et nos données restent ainsi sur nos propres serveurs, où elles sont souvent moins bien protégées.

À quoi reconnaît-on qu'une organisation est suffisamment souveraine et à quel moment la dépendance devient-elle critique?

L'organisation a-t-elle un plan B, voire un plan C, si un prestataire devait disparaître ou être abandonné? Existe-t-il des sauvegardes – et

«Se focaliser sur le CLOUD Act détourne l'attention de risques bien plus importants»

sont-elles ailleurs? L'organisation a-t-elle réparti délibérément ses composantes de solutions informatiques entre différents prestataires, et donc pas tout misé sur le même cheval? Dispose-t-elle d'un savoir-faire suffisant pour comprendre et mettre en œuvre ses options? Je préfère donc parler de résilience numérique plutôt que de souveraineté numérique.

Quelles fausses idées rencontrez-vous le plus souvent dans le débat public?

Que les États-Unis ont un libre accès à nos données en cas d'utilisation de fournisseurs de services de cloud américains.



À propos de l'expert:

David Rosenthal est l'un des principaux experts suisses en droit des données et des technologies. Il est associé chez VISCHER et conseille les entreprises et les autorités autour de la protection des données, du droit informatique et du droit de l'IA.

Conclusion: celui qui garde la capacité d'agir est souverain

La souveraineté numérique signifie concevoir consciemment l'utilisation des technologies numériques, gérer les risques et conserver sa capacité d'action même dans un monde connecté. Quiconque connaît ses données, comprend les interdépendances et conserve des alternatives technologiques peut utiliser l'innovation sans perdre le contrôle:

- 1** Les organisations qui réussissent associent des technologies et des modèles d'exploitation différents en fonction de leurs exigences et des prescriptions légales.
- 2** Dans des cas particuliers ou lorsque la conservation des données est ancrée dans la loi, des infrastructures locales ou des modèles d'exploitation spéciaux peuvent être judicieux pour les données particulièrement sensibles.
- 3** Pour les applications standardisées, les plateformes cloud offrent souvent des avantages décisifs en termes d'innovation et d'efficacité.
- 4** En outre, des composants open source peuvent contribuer à augmenter la transparence et à réduire les dépendances.

La souveraineté numérique est garantie dès lors que les organisations comprennent leurs dépendances technologiques, gèrent activement les risques et conservent à tout moment leur capacité d'action. C'est précisément cette approche consciente et différenciée de la technologie qui constitue le fondement de la souveraineté numérique.

Vote électronique



Le système de vote électronique de la Poste permet de participer aux votations et aux élections par voie électronique en toute sécurité. Des dispositifs cryptographiques et techniques de sécurité spéciaux garantissent le secret du vote tout en permettant de s'assurer qu'aucune manipulation n'a eu lieu dans le cadre du scrutin dans son ensemble. Le vote électronique est utilisé avec succès dans plusieurs cantons depuis 2023.

- Le logiciel de vote électronique ainsi que les serveurs et les données sont exploités en Suisse.
- La Poste met à la disposition du public les composants et documents essentiels du système et invite des spécialistes à le contrôler. Par le biais d'un programme «bug bounty», elle met également en place des incitations financières pour le contrôle public et le signalement des vulnérabilités.
- La Poste met à disposition des parties importantes du code sous une licence open source libre. Il est ainsi possible d'utiliser et de développer librement les parties correspondantes du code source.

