BÄR & KARRER, BRIEFING AVRIL 2026

UTILISATION DU CLOUD ET SOUVERAINETÉ NUMÉRIQUE : OPTIONS À DISPOSITION DES AUTORITÉS SUISSES

Les services cloud font aujourd'hui partie intégrante du travail administratif. Parallèlement, lors de l'externalisation du traitement des données par les autorités fédérales, cantonales et communales, il convient de respecter les exigences en matière de protection des données, les obligations de confidentialité telles que le secret de fonction, ainsi que les prescriptions relatives à la sécurité de l'information, tout en garantissant la capacité d'action à long terme. Dans le débat public, qui a gagné en intensité avec les récentes évolutions politiques aux États-Unis, l'utilisation des services cloud américains par les autorités suisses dans le contexte de la souveraineté numérique[1] est actuellement au cœur des discussions.[2] Ce débat a été accentué par la résolution publiée en novembre 2025 par privatim, la Conférence des préposés suisses à la protection des données, qui peut être interprétée comme une interdiction *de facto* de l'utilisation des *hyperscalers* dans l'administration publique. Dans le domaine des marchés publics également, cette orientation se concrétise déjà ponctuellement : ainsi, l'appel d'offres de l'OFSP concernant l'infrastructure SwissHDS (février 2026) exige notamment que les composantes de l'infrastructure ne présentent aucune dépendance technique ou juridique vis-à-vis de juridictions étrangères (par ex. le CLOUD Act américain).

La souveraineté numérique des autorités suisses ne signifie ni autarcie ni isolement, mais bien la capacité de piloter et de contrôler de manière autonome le recours à des prestations numériques externes. Le présent briefing met en perspective les arguments avancés, expose les tensions existantes et offre des repères pour l'utilisation du cloud dans l'administration. L'analyse démontre qu'il n'existe pas de solution totalement exempte de risques : chaque option – qu'il s'agisse d'un service cloud américain, d'un fournisseur suisse ou européen, d'une solution *on-premises* ou open source – nécessite une évaluation au cas par cas entre fonctionnalité, sécurité, souveraineté et charges d'exploitation.

[1] Selon le Conseil fédéral 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. (rapport "Souveraineté numérique de la Suisse" du 26 novembre 2025, p. 6).

[2] La compatibilité de l'utilisation du cloud avec le secret de fonction (art. 320 CP) et la protection des données est largement clarifiée sur le plan juridique : les fournisseurs de services cloud peuvent être associés à l'exécution des tâches de l'État en tant qu'auxiliaires de l'autorité, pour autant qu'ils soient soigneusement sélectionnés, instruits et contrôlés. Ils sont ainsi eux-mêmes soumis au secret de fonction. Du point de vue du droit de la protection des données, l'externalisation auprès d'un fournisseur de services cloud est autorisée en tant que sous-traitance, aux conditions prévues à l'art. 9 LPD. Ces deux aspects ne seront pas abordés plus en détail dans la présente note d'information.

A. MESSAGES CLÉS

- **La souveraineté numérique** ne signifie ni autarcie ni isolement, mais la capacité des autorités de piloter et de contrôler de manière autonome le recours à des prestations numériques externes.
- Le **CLOUD Act américain ne confère pas** aux autorités américaines **un droit d'accès direct** aux données stockées à l'étranger. Les ordonnances de remise requièrent une décision judiciaire, un soupçon suffisant ainsi qu'un objectif concret de poursuite pénale. De plus, des limites relevant de l'État de droit restreignent leur portée.
- **Les ordres de production fondés sur le** CLOUD Act américain servent principalement à enquêter sur **des infractions graves** (tel**le**s que le terrorisme ou la cybercriminalité). Les données administratives courantes, telles que les documents de projet, les statistiques ou les dossiers du personnel, ne font généralement pas l'objet d'enquêtes américaines.
- **Les rapports de transparence** des *hyperscalers* américains le confirment : **les divulgations de données de contenu de clients professionnels étrangers** aux autorités de poursuite pénale américaines sont **extrêmement rares** (chez Microsoft, 0,008 % de l'ensemble des demandes). Aucun cas n'est connu à ce jour concernant des clients du secteur public (état : avril 2026).
- **Les fournisseurs de cloud de l'UE et de Suisse ne** garantissent **pas** non plus **une absence totale de risques**. Les sous-traitants, les chaînes d'approvisionnement mondiales ou les basculements d'urgence (*failovers*) vers des pays tiers peuvent indirectement déclencher des droits d'accès extraterritoriaux. De plus, il existe souvent des restrictions opérationnelles en matière de portefeuille de services, d'évolutivité, de support et de niveau de certification, ce qui peut engendrer des efforts supplémentaires d'intégration et de vérification.
- **Les solutions *open source* et *on-premises*** transfèrent l'entière responsabilité en matière de sécurité et d'exploitation à l'autorité et s'accompagnent de coûts considérables ainsi que de cyberrisques spécifiques. Les projets *open source* sont en outre soumis à des risques liés aux sanctions et à la chaîne d'approvisionnement. Les solutions *on-premises* offrent certes un contrôle physique, mais sont limitées en termes d'évolutivité et de résilience.
- En conséquence, tout projet (cloud) nécessite une **analyse des risques**, que l'on opte pour un fournisseur américain, européen ou suisse, ou pour une solution *open source* ou *on-premises*. Sur cette base, l'autorité doit prendre une **décision fondée sur les risques** afin de déterminer si les risques résiduels sont acceptables et si le projet peut être approuvé.

B. CLOUD ACT AMÉRICAIN : PORTÉE, LIMITES ET PERTINENCE PRATIQUE POUR LES AUTORITÉS SUISSES

I. CADRE JURIDIQUE : IMPORTANCE DU CLOUD ACT

Entré en vigueur en mars 2018, le CLOUD Act américain concrétise le *Stored Communications Act* (SCA) et précise que les autorités américaines, dans le cadre d'enquêtes liées à des infractions graves telles que le terrorisme, la criminalité violente, l'exploitation sexuelle des enfants et la cybercriminalité, peuvent exiger, sur la base d'un mandat judiciaire (*warrant*), d'un mandat de comparution (*subpoena*) ou d'une ordonnance du tribunal (*court order*), la remise de données de communication stockées ou traitées par un fournisseur soumis au CLOUD Act, même si ces données sont hébergées sur des serveurs situés en dehors des États-Unis. Le CLOUD Act a donc notamment pour objectif de faciliter les enquêtes portant sur des infractions graves.

Le champ d'application personnel du CLOUD Act est large : il couvre tous les fournisseurs de services de communication électronique (*electronic communication services*) ou de services informatiques à distance (*remote computing services*) qui sont domiciliés aux États-Unis, y possèdent une succursale ou y exercent une activité commerciale.

L'applicabilité de cette loi dépend de l'interprétation que fait le droit américain des notions de "*possession, custody, or control*". Selon cette interprétation, il suffit qu'un fournisseur exerce un contrôle de fait ou de droit sur les données, même si celles-ci sont hébergées dans des centres de données situés en Suisse ou en Europe. Le CLOUD Act établit ainsi des obligations de remise extraterritoriales susceptibles d'entrer en contradiction avec les garanties juridiques suisses (telles que l'entraide administrative et judiciaire).

Le CLOUD Act étant au centre des débats actuels, le présent briefing se concentre sur ce texte. Il convient de le distinguer de la section 702 du *Foreign Intelligence Surveillance Act* (FISA), qui permet aux services de renseignement américains de collecter de manière programmatique des données de renseignement étranger. Contrairement au CLOUD Act, aucune décision judiciaire individuelle n'est requise. Le droit d'accès repose sur un cadre programmatique approuvé par la *Foreign Intelligence Surveillance Court*, qui oblige les fournisseurs américains à coopérer.

II. PAS DE CARTE BLANCHE : LES LIMITES CONSTITUTIONNELLES DU CLOUD ACT

Malgré les risques liés à un ordre de production, il n'est pas justifié de remettre globalement en cause ou d'interdire de manière générale l'utilisation des services cloud américains par les autorités suisses. Pour l'appréciation des risques, ce n'est pas seulement la portée théorique des lois américaines qui est déterminante, mais surtout les obstacles juridiques existants qui limitent et encadrent les demandes de remise de données stockées par les autorités suisses, ainsi que la probabilité concrète que les autorités américaines accèdent effectivement à ces données.

Les ordres de production formels prévus par le CLOUD Act se heurtent à diverses limites constitutionnelles et garanties procédurales qui restreignent et structurent les demandes de production. Ainsi, les données ne doivent être remises que sur la base d'une décision d'un tribunal américain, lorsqu'elles sont pertinentes pour une enquête pénale en cours aux États-Unis. Pour qu'une telle décision soit rendue, il doit exister un soupçon suffisant ("*probable cause*") d'une infraction pénale concrète, et les données demandées doivent contribuer concrètement à l'élucidation ou à la poursuite de cette infraction. Une demande de données générale, forfaitaire ou motivée uniquement par des intérêts ne satisfait pas aux exigences du CLOUD Act.

Le CLOUD Act ne prévoit pas non plus que les données doivent être automatiquement communiquées. Au contraire, le texte de loi ouvre expressément la possibilité de contester ou de faire modifier un ordre du tribunal si un fournisseur relevant du champ d'application du CLOUD Act a des raisons fondées de craindre que la communication des données ne viole le droit d'un autre État. Cette "*comity analysis*" exige qu'un tribunal américain, en cas d'objections correspondantes, examine si une obligation de production est contraire aux lois de l'État étranger concerné et, si certaines conditions sont réunies, le processus, voire l'annule. En pratique, cela signifie que les ordonnances qui ne satisfont pas aux exigences légales ne sont pas automatiquement exécutées, mais font l'objet d'un contrôle, ce qui relativise considérablement la portée théorique du CLOUD Act en raison de garanties relevant de l'État de droit.

Enfin, le CLOUD Act n'interdit pas de manière générale aux fournisseurs de services cloud d'informer les clients concernés de la production de leurs données. Dans certains cas, toutefois, une ordonnance administrative ou judiciaire peut restreindre ou interdire temporairement une telle notification (*gag orders*), ces mesures devant être motivées et limitées en termes de portée et temps.

III. RAPPORTS DE TRANSPARENCE DES FOURNISSEURS DE SERVICES CLOUD AMÉRICAINS : LES DIVULGATIONS CONSTITUENT UNE EXCEPTION RARE

L'expérience pratique acquise depuis 2018 concernant ce type de demandes est également déterminante. Les rapports de transparence des grands fournisseurs de services cloud américains montrent que les divulgations effectives de données concernant des clients professionnels sont rares.

Chez Microsoft[3], au premier semestre 2025 (comme les années précédentes[4]), moins de 0,7 % des demandes mondiales émanant des autorités de poursuite pénale concernaient des données de clients professionnels. Dans la majorité des cas, ces demandes ont été rejetées, retirées ou redirigées de telle sorte que les autorités ont dû s'adresser directement au client. Lorsque des données de clients professionnels ont été transmises, la majeure partie concernait des données non liées au contenu (par ex. des informations de base sur les abonnés ou des journaux IP), tandis que les données de contenu n'ont été divulguées que dans une minorité de cas. Les divulgations transfrontalières de données de contenu sont restées rares : Microsoft a transmis dans cinq cas des données de contenu aux autorités américaines concernant des clients professionnels non américains dont les données étaient hébergées en dehors des États-Unis. Un seul de ces cas concernait un client ayant son siège dans l'UE, qui était un sous-traitant du gouvernement américain.

Si l'on met ces chiffres en rapport avec le nombre total de demandes reçues par Microsoft depuis l'entrée en vigueur du CLOUD Act, la rareté des demandes fondées sur le CLOUD Act devient encore plus tangible : les divulgations de données de contenu de clients professionnels étrangers aux autorités de poursuite pénale américaines ne représentaient que 0,008 % de l'ensemble des demandes mondiales.[5] Selon les informations fournies par Microsoft, aucune autorité ni institution publique n'a été concernée dans ces rares cas.[6]

Amazon Web Services (AWS) indique n'avoir divulgué, depuis le début de la collecte des données, aucune donnée provenant de clients professionnels ou d'autorités situés en dehors des États-Unis en vertu d'ordres de production fondés sur le CLOUD Act,[7] et applique une pratique consistant à adresser les demandes, dans la mesure du possible, au client lui-même en premier lieu. Cette pratique reflète le fait qu'une obligation de production n'existe

[3] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H1-2025.pdf
[4] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H2-2024.pdf
[5] https://news.microsoft.com/source/emea/2026/02/how-microsoft-is-addressing-digital-sovereignty-in-switzerland/
[6] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/CLOUD-Act-What-it-is-and-is-not.pdf
[7] https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/whitepapers/compliance/Amazon_AWS_Information_Request_Report_H2_2025.pdf

que s'il existe un ordre juridiquement valable et contraignant, et non pas automatiquement pour chaque demande de production. En outre, AWS précise expressément que ni le gouvernement américain ni aucun autre gouvernement ne se voit accorder un accès illimité ou automatique aux données des clients – y compris aux données hébergées dans le cloud.[8]

IV. FAIBLE INCIDENCE DES ORDONNANCES CLOUD ACT SUR LES DONNÉES ADMINISTRATIVES TYPIQUES

En principe, le CLOUD Act ne limite pas les catégories de données pouvant faire l'objet d'un ordre de production; toutes les données stockées chez un fournisseur soumis au CLOUD Act sont potentiellement concernées, quel que soit leur lieu de stockage. Toutefois, comme mentionné précédemment, l'objectif déclaré de la loi est de permettre l'accès aux communications électroniques dans le cadre d'enquêtes portant sur des infractions graves, notamment le terrorisme, la criminalité violente, l'exploitation sexuelle des enfants et la cybercriminalité. En pratique, les ordonnances de divulgation approuvées par un juge dans le cadre de procédures pénales américaines portent généralement sur le contenu des communications (courriels, chats, messages), les métadonnées relatives aux communications ainsi que les données d'identité, car celles-ci présentent la plus grande valeur probante pour les enquêtes pénales. Les données de communication sont généralement pertinentes pour mettre au jour des ententes ou la planification d'infractions, tandis que les données d'identité servent à attribuer des comptes à des personnes réelles. En revanche, les données techniques du système, les documents internes ou les dossiers du personnel ne devraient présenter un intérêt que dans des contextes d'enquête spécifiques et être concernés bien plus rarement.

Les autorités suisses stockent quant à elles principalement des données administratives : documents internes, correspondance, dossiers de projets, statistiques ou dossiers du personnel. Ces types de données ne présentent généralement pas d'intérêt pour les enquêtes sur le terrorisme, la criminalité violente ou la cybercriminalité et sont dès lors nettement moins exposés que, par exemple, les données de communication des utilisateurs privés.

V. UNE ÉVALUATION DIFFÉRENCIÉE DES RISQUES PLUTÔT QU'UNE EXCLUSION GÉNÉRALE

Dans ce contexte, le risque d'une remise effective de données de contenu aux autorités de poursuite pénale américaines est nettement inférieur à ce que suggérerait une analyse purement théorique du CLOUD Act. Certes, les demandes des autorités américaines ne sont pas exclues, et cette possibilité doit être prise en compte dans l'évaluation des risques. Cependant, les chiffres concrets et les processus établis montrent que les demandes des autorités américaines concernant des contenus de services cloud stockés en dehors des États-Unis sont, dans des scénarios réels, rares et fortement réglementées. Cela relativise la pertinence pratique des obligations théoriques de production, en particulier pour l'utilisation de services cloud par les autorités.

Cela ne signifie toutefois pas qu'un risque statistique faible constitue en soi un risque acceptable. Dans le contexte du droit public notamment, un seul incident – par exemple la divulgation d'informations relevant des services de renseignement ou de documents sensibles sur le plan de la politique étrangère – peut déjà entraîner des conséquences considérables sur le plan de l'État de droit et sur le plan politique. Ce n'est donc pas seulement la probabilité de survenance qui est déterminante, mais l'interaction entre cette probabilité et l'ampleur potentielle du préjudice. L'analyse des besoins de protection que l'autorité doit réaliser sert précisément cet objectif : elle définit le niveau de protection requis pour les informations concernées. Des exigences de confidentialité accrues s'appliquent aux données soumises au secret de fonction. Les résultats doivent être documentés de manière compréhensible dans un concept SIPD (sécurité de l'information et protection des données). L'analyse des besoins de protection garantit ainsi que les données nécessitant une protection renforcée bénéficient d'un niveau de protection approprié, indépendamment de la rareté statistique d'un accès. Cela peut également impliquer, dans certains cas, le recours à des mesures de protection techniques supplémentaires ou le renoncement à une externalisation dans le cloud. Une analyse d'impact relative à la protection des données (AIPD) doit en outre être effectuée régulièrement. Elle évalue les risques liés au traitement des données du point de vue des personnes concernées, complète le concept SIPD et peut donner lieu à un contrôle préalable par l'autorité de surveillance de la protection des données.

En revanche, une exclusion générale de l'utilisation des services cloud américains ne tient pas compte de cette réalité : les risques varient considérablement selon la catégorie de données, les besoins de protection et les mesures de sécurité mises en place, et les obstacles techniques, contractuels et juridiques réduisent encore davantage la probabilité que des données doivent effectivement être remises à la suite de demandes émanant des autorités américaines. Le fait que ces obstacles ne puissent pas éliminer complètement tous les risques ne plaide pas contre l'utilisation des services cloud américains en tant que telle, mais en faveur d'une décision nuancée et fondée sur les risques prise par l'autorité au cas par cas.

[8] https://aws.amazon.com/compliance/cloud-act/

C. Alternatives aux services cloud américains : opportunités, limites et risques spécifiques

Le débat s'intéresse de plus en plus aux solutions alternatives, allant des offres cloud de fournisseurs européens et suisses aux solutions *open source* et aux infrastructures *on-premises*. Chacune de ces options comportant ses propres risques juridiques, techniques et opérationnels, il serait erroné de les considérer globalement comme des alternatives moins risquées à l'utilisation de services cloud américains. Là encore, il convient d'évaluer soigneusement la faisabilité et le profil de risque.

I. OFFRES DE CLOUD COMPUTING PROPOSÉES PAR DES FOURNISSEURS EUROPÉENS/SUISSES

1. Persistance des obligations de production extraterritoriales

L'utilisation d'offres cloud de fournisseurs de l'UE ou de Suisse réduit le risque d'un ordre de production fondé sur le CLOUD Act, pour autant que le fournisseur ne soit pas lui-même soumis au CLOUD Act. Cela étant, même ces modèles ne sont pas exempts de risques en ce qui concerne l'accès depuis des pays tiers. Ainsi, les sociétés étrangères du groupe, le recours à des sous-traitants ayant leur siège dans des pays tiers ou l'implication de fournisseurs mondiaux – par exemple via des chaînes CDN/DNS mondiales, un support 24h/24 et 7j/7 ou un basculement d'urgence (*failover*) dans des régions hors UE/Suisse – peuvent indirectement déclencher des droits d'accès extraterritoriaux ou des obligations de production.

L'affaire OVHcloud en est un exemple récent : fin septembre 2025, la Cour supérieure de justice de l'Ontario a confirmé un ordre de production à l'encontre de la société mère française d'OVHcloud, lui enjoignant de transmettre à la Gendarmerie royale du Canada des données clients hébergées en Europe. Cette décision s'appuyait notamment sur la "présence virtuelle" présumée de l'entreprise au Canada par l'intermédiaire de sa filiale locale. Cette affaire démontre qu'une telle présence d'entreprise dans un pays tiers peut déjà déclencher des ordres de production extraterritoriaux, même en cas de conflit avec le droit local.

En outre, le règlement de l'UE relatif aux injonctions européennes de production et de conservation de preuves électroniques (*règlement "e-evidence"*) prévoit qu'à l'avenir, les autorités des États membres de l'UE pourront, sous certaines conditions, adresser des injonctions de production transfrontalières directement aux fournisseurs de services situés dans d'autres États membres.

Indépendamment de cela, les accès des autorités par le biais de l'entraide administrative et judiciaire internationale (par ex. sur la base du deuxième protocole additionnel à la Convention de Budapest) restent possibles. Ceux-ci ne s'effectuent pas directement par l'intermédiaire du fournisseur de services cloud, mais s'adressent à l'autorité nationale compétente et sont soumis aux règles de procédure de l'entraide administrative et judiciaire (y compris la loi fédérale sur l'entraide pénale internationale, EIMP).

2. Efforts d'intégration accrus en raison d'un portefeuille et d'une maturité de plateforme limités

Par ailleurs, les fournisseurs de l'UE et de Suisse présentent également des risques factuels et opérationnels par rapport aux *hyperscalers* américains. Le portefeuille de services et d'applications est souvent moins large ou moins abouti, notamment dans le domaine de l'IA, des fonctions d'analyse ainsi que des services de plateforme et des services gérés, ce qui peut entraîner des efforts d'intégration supplémentaires ou des restrictions fonctionnelles. Les interfaces et les intégrations sont souvent moins standardisées, ce qui rend les migrations, les automatisations et l'exploitation d'architectures complexes – nécessaires dans le domaine de l'administration moderne – plus longues, plus coûteuses et plus sujettes aux erreurs.

3. Limites en matière d'évolutivité, de niveau de support et de couverture des certifications

De plus, le rythme d'innovation et de publication est plus lent. L'évolutivité et la résilience tendent également à être limitées : les fournisseurs de l'UE et de Suisse disposent de moins de régions et de zones de disponibilité, ainsi que d'une couverture réseau mondiale plus restreinte, ce qui se traduit par des latences plus élevées, des limites de capacité plus basses et une plus grande dépendance vis-à-vis de certains centres de données.

Au niveau opérationnel, on observe des restrictions en matière de gestion des incidents et de support 24h/24 et 7j/7, notamment concernant les délais de réponse, les procédures d'escalade ou la couverture linguistique. De plus, les certifications et les preuves de conformité couvrent moins souvent les référentiels réglementaires spécifiques à chaque secteur. Alors que les grands fournisseurs de cloud bien établis disposent généralement de certifications reconnues telles que ISO 27001 ou SOC 2 Type II et les étendent de manière proactive aux exigences sectorielles supplémentaires, les petits fournisseurs manquent souvent non seulement des preuves formelles correspondantes, mais aussi des structures de gouvernance internes qui permettraient de garantir de manière fiable le respect effectif de ces référentiels.

4. Charge accrue en matière d'audit et de validation en raison d'un effet de transfert

Cette lacune a pour conséquence que la charge liée aux audits et à la validation se transfère *de facto* vers l'autorité adjudicatrice, qui doit alors s'assurer elle-même, dans le cadre d'audits de *due diligence*, de droits d'audit contractuels et de procédures de validation individuelles, que les exigences réglementaires et techniques en matière de sécurité sont respectées. Pour les autorités

qui opèrent déjà avec des ressources humaines et techniques limitées dans les domaines de la sécurité informatique, du droit de la protection des données et des marchés publics, cela représente une charge supplémentaire. Cette charge s'alourdit particulièrement lorsque plusieurs petits prestataires doivent être contrôlés et surveillés en parallèle, car chaque prestataire nécessite des analyses de risques individuelles, des clauses contractuelles sur mesure et des mécanismes de contrôle continus, sans qu'il ne soit possible de bénéficier des effets de synergie qui résultent généralement de la collaboration avec un grand prestataire certifié.

En pratique, cela conduit souvent soit à une réduction de la profondeur des contrôles, ce qui augmente le risque de lacunes de conformité non détectées, soit à des retards considérables dans les procédures d'adjudication, car les processus de validation internes nécessaires dépassent les capacités disponibles. Enfin, les petits fournisseurs sont davantage exposés aux fluctuations de prix, à la consolidation du marché et aux risques d'insolvabilité, ce qui doit être pris en considération dans la planification à long terme.

II. SOLUTIONS OPEN SOURCE

1. Risques opérationnels et juridiques liés à une exploitation sous sa propre responsabilité

Les solutions *open source* propres à l'administration permettent un haut degré de contrôle sur l'exploitation, l'architecture et la gestion des clés. Elles peuvent ainsi conduire à une plus grande indépendance opérationnelle et offrir une protection contre les demandes de production fondées sur le CLOUD Act. Toutefois, même avec des solutions *open source*, il n'est pas possible d'exclure totalement de telles demandes, par exemple lorsque l'exploitation s'effectue via l'infrastructure d'un fournisseur soumis au CLOUD Act. Indépendamment de cela, l'exploitation sous sa propre responsabilité nécessite en permanence du personnel qualifié, des processus de sécurité et d'exploitation clairement définis ainsi qu'un fonctionnement fiable 24h/24 et 7j/7.

Outre les risques opérationnels, il existe également des risques juridiques et factuels spécifiques : il s'agit notamment des failles de sécurité résultant de mises à jour retardées, des erreurs de configuration dans des piles logicielles complexes, d'une surveillance insuffisante (par ex. absence de surveillance des vulnérabilités, suivi insuffisant des dépendances) ainsi que des risques de non-conformité en cas d'absence de gestion des licences, en particulier en ce qui concerne les licences *copyleft*. À cela s'ajoutent des questions de responsabilité et de garantie, car les logiciels *open source* sont généralement fournis "tels quels" (as is), ce qui confère aux autorités la responsabilité correspondante. L'autorité assume ainsi l'entière responsabilité de l'exploitation : les pannes de système, les violations de conformité ou les incidents de sécurité résultant d'une documentation insuffisante de l'architecture et des dépendances, de la concentration du savoir-faire sur quelques individus ou de l'application tardive des correctifs sont entièrement à sa charge.

L'exploitation sous sa propre responsabilité entraîne en outre des coûts considérables : outre les frais de personnel courants pour le personnel spécialisé, il faut compter les dépenses liées à l'infrastructure, aux audits de sécurité, à la conformité des licences et au développement continu. Le coût total de possession (*Total Cost of Ownership*) des solutions *open source* est souvent sous-estimé, car il ne résulte pas de frais de licence, mais de frais d'exploitation et de maintenance.

2. Risques liés aux sanctions, à la chaîne d'approvisionnement et à la cybersécurité

Il existe en outre des risques liés aux sanctions en rapport avec le développement (continu) et, par conséquent, indirectement aussi avec l'utilisation de logiciels *open source*. Les principaux opérateurs actuels de plateformes d'hébergement de logiciels *open source* sont basés aux États-Unis ou cotés en bourse. À ce titre, ils sont soumis au régime de sanctions américain, ce qui peut les obliger à restreindre l'accès aux développeurs visés par des sanctions afin d'éviter toute violation de ce régime. Si une autorité suisse se procure des logiciels *open source* auprès de ces plateformes d'hébergement, des modifications du régime de sanctions – par exemple par l'extension des listes de sanctions ou l'inclusion de nouveaux pays et organisations – peuvent entraîner des risques considérables pour l'exploitation, la maintenance et le développement. L'exemple du noyau Linux illustre le fait que ces risques ne sont pas seulement de nature théorique : en octobre 2024, onze développeurs russes du noyau ont été démis de leurs fonctions pour des raisons de conformité, ce qui met en évidence la dépendance opérationnelle de grands projets open source vis-à-vis de la situation de sanctions de certains développeurs.

À cela s'ajoutent des cyberrisques spécifiques : les logiciels *open source* peuvent faire l'objet d'examens ciblés visant à détecter des vulnérabilités en raison de leur base de code accessible au public. Il existe également un risque d'attaques de la chaîne d'approvisionnement (*supply chain attacks*), dans lesquelles du code malveillant est introduit via des dépendances compromises ou des contributions manipulées – comme l'illustre la porte dérobée (*backdoor*) découverte en mars 2024 dans la bibliothèque xz-utils, qui avait été intégrée avec succès dans le code par l'acteur non identifié à ce jour "Jia Tan", mais qui a été détectée à temps, soit avant qu'elle ne puisse se propager à grande échelle.

Des considérations similaires s'appliquent au matériel *open source*, dont l'utilisation comporte également des risques liés à la disponibilité et à la chaîne d'approvisionnement.

III. SOLUTIONS ON-PREMISES

1. Limites en matière d'évolutivité, de résilience et de dépendances matérielles

Les solutions *on-premises*, dans lesquelles les systèmes sont entièrement sous le contrôle des autorités (dans leur propre salle de serveurs, dans leur propre centre de données ou chez un fournisseur de colocation auquel seules les autorités ont accès), renforcent le contrôle physique sur l'infrastructure et les données. Elles s'accompagnent toutefois de risques opérationnels, juridiques et économiques spécifiques. Ainsi, l'évolutivité est souvent limitée en cas de besoins supplémentaires à court terme, le risque de panne est plus élevé par rapport aux grandes infrastructures cloud et il existe des dépendances vis-à-vis des chaînes d'approvisionnement matérielles.

2. Responsabilité exclusive en matière de sécurité et d'exploitation sans partage des tâches

De plus, il faut davantage de personnel qualifié pour assurer l'exploitation d'une solution *on-premises*. L'autorité doit satisfaire elle-même à toutes les exigences opérationnelles et de sécurité – y compris la protection contre les cyberrisques – et en apporter la preuve. Contrairement au *modèle de responsabilité partagée* (*Shared Responsibility Model*), dans lequel le fournisseur de cloud et le client se répartissent les responsabilités et où le fournisseur prend en charge les tâches essentielles de sécurité et d'exploitation, l'autorité assume, dans le cas des solutions *on-premises*, la responsabilité exclusive de la disponibilité et de la restauration, de l'intégrité et de la traçabilité des données, des obligations d'archivage et de conservation, ainsi que de la protection des données et de la sécurité de l'information dans son ensemble. Cela comprend notamment les mesures de sécurité techniques et organisationnelles, les contrôles de l'accès aux données, les concepts de rôles et de séparation des tâches, ainsi que les processus d'urgence et de reprise.

De plus, cela entraîne des coûts d'investissement et d'exploitation considérables ainsi que des défis supplémentaires en matière d'acquisition et d'exploitation, notamment en ce qui concerne les cycles de renouvellement, les dépendances vis-à-vis des fabricants ainsi que les contrats de maintenance et de support.

D. Conclusion : une décision au cas par cas fondée sur les risques, clé d'une utilisation du cloud conforme au droit

L'analyse qui précède démontre que le CLOUD Act ne constitue pas un obstacle général à l'utilisation des services cloud américains par les autorités suisses : les données concrètes et les procédures établies attestent que les ordres de production des autorités américaines concernant des données de contenu stockées en dehors des États-Unis sont, en pratique, rares et fortement limités sur le plan juridique. Néanmoins, le contexte du droit public exige justement une évaluation nuancée : étant donné qu'un seul incident peut déjà entraîner des conséquences considérables sur le plan de l'État de droit et sur le plan politique, ce n'est pas seulement la probabilité de survenance qui compte, mais son interaction avec l'ampleur potentielle du préjudice – ce qui plaide en faveur d'une décision au cas par cas de l'autorité, fondée sur les risques, et non d'une exclusion générale des services cloud américains.

Chaque projet (cloud) dépend donc d'une décision de l'autorité compétente en matière de risques, qui doit se fonder sur une analyse des risques propre et approfondie. Toute solution cloud – qu'elle provienne d'un fournisseur américain, suisse ou européen – comporte, tout comme les solutions *open source* et *on-premises*, des défis juridiques, factuels et opérationnels spécifiques. L'autorité doit recenser systématiquement les risques concrets en tenant compte des besoins de protection des informations concernées, examiner les possibilités d'atténuation et, dans le cadre d'une décision éclairée, évaluer si les risques résiduels sont acceptables et si le projet peut être approuvé.

L'analyse des risques peut révéler que, pour certains projets – par exemple lorsqu'il s'agit d'informations sensibles relevant des services de renseignement ou de documents délicats sur le plan de la politique étrangère –, une approche hybride constitue la solution la plus appropriée. Dans ce cas, un service de cloud public est par exemple combiné de manière ciblée avec une solution *on-premises* ou *open source* afin de répondre à différentes exigences de protection.

Ce constat repose également sur une conception moderne de la souveraineté numérique : pour les autorités suisses, la souveraineté numérique ne signifie ni autarcie ni isolement, mais la capacité délibérée de piloter et de contrôler de manière autonome le recours à des prestations numériques externes. Les relations avec des prestataires de services externes font partie intégrante de la pratique administrative moderne et ne constituent pas une perte de souveraineté tant qu'elles restent transparentes, clairement délimitées et efficacement contrôlables. Une stratégie cloud pérenne pour le secteur public ne se heurtera donc pas à la question de savoir si les services cloud peuvent être utilisés, mais à celle de savoir si les autorités créent les conditions institutionnelles, techniques et juridiques nécessaires pour organiser cette utilisation de manière autonome, en fonction des risques et en conformité avec les exigences de l'État de droit.

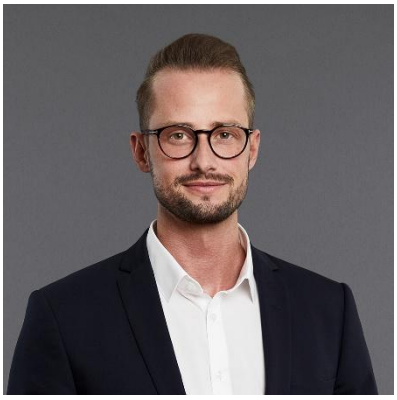
AUTEURS

Dr. Christian Kunz

Partner

christian.kunz@baerkarrer.ch

T: +41 58 261 52 66



Ferdinand Rombach

Associate

ferdinand.rombach@baerkarrer.ch

T: +41 58 261 54 12

Dr. Katharina Cardon

Associate

katharina.cardon@baerkarrer.ch

T: +41 58 261 52 82