

Dépendance vis-à-vis des géants du cloud: un risque systémique pour les entreprises suisses

OPINION. Le black-out des services cloud d'Amazon le 20 octobre souligne en creux l'urgence de diversifier nos prestataires de services essentiels, écrivent Claire Tistounet et Philipp Fischer, du cabinet Lenz & Staehelin

Le lundi 20 octobre 2025, un centre de données d'Amazon Web Services (AWS), la plateforme d'infrastructure cloud d'Amazon, a subi une panne majeure aux Etats-Unis. Cette interruption a touché d'innombrables services et entreprises à travers le monde, provoquant l'indisponibilité de sites bancaires, l'impossibilité de recharger des voitures électriques et l'interruption de visioconférences.

Cet événement met une nouvelle fois en lumière la dépendance de notre économie à l'égard des prestataires cloud, désormais véritablement devenus des infrastructures critiques à l'heure actuelle. Un nombre croissant d'entreprises, suisses comme internationales, ont en effet renoncé à exploiter leurs propres serveurs internes au profit de solutions d'hébergement externalisées dans des clouds publics administrés par des prestataires externes, principalement Microsoft, Amazon, Oracle et Google.

Les bienfaits de l'externalisation....

Cette externalisation permet de réduire les coûts d'investissement, de maintenance et d'énergie. Le modèle de location basé sur une facturation pay-per-use offre une flexibilité financière: payer plus lors des pics d'activité, moins en période creuse (ce qui n'est logiquement pas possible si l'infrastructure IT est internalisée). Les grands fournisseurs peuvent aussi mobiliser des ressources humaines et technologiques supérieures à ceux d'un service informatique interne, améliorant disponibilité, sécurité et sophistication des services, notamment en matière d'intelligence artificielle.

Dans ce contexte, la panne du 20 octobre a douloureusement rappelé à quel point il est indispensable pour les entreprises de diversifier leurs fournisseurs cloud afin de réduire la dépendance vis-à-vis d'un seul acteur.

Et les risques de la dépendance

Le revers de ce phénomène est une dépendance accrue à l'égard de quelques fournisseurs. En cas de défaillance, les acteurs économiques (y compris des secteurs critiques) sont fragilisés. Pour les entreprises suisses, cet enjeu est juridique, réglementaire et stratégique. Ainsi, les entités soumises à la Finma doivent démontrer leur résilience en maintenant des plans de continuité et de réversibilité clairement définis, afin d'assurer la poursuite des opérations en cas d'interruption de service ou de résiliation de contrat.

Le modèle «multi-cloud» permet de mieux gérer les risques et d'assurer la continuité des activités en cas de panne, de litige ou de contrainte réglementaire. Il limite également les risques découlant d'une position de «client captif» dépourvu de toute marge de négociation en cas d'augmentation de prix ou de dégradation du service. Toutefois, cette marge de manœuvre reste limitée: le marché est dominé par quelques acteurs américains, ce qui maintient une dépendance structurelle et des enjeux géopolitiques. Même diversifiée, cette concentration soulève des questions de souveraineté numérique et de protection des données dans un contexte transatlantique instable.

En réponse, plusieurs initiatives européennes visent à développer des alternatives: le projet franco-allemand Gaia-X vise à créer une infrastructure de données fédérée permettant aux utilisateurs européens de garder le contrôle de leurs données tout en assurant l'interopérabilité entre fournisseurs. Parallèlement, la Commission européenne développe une stratégie de fédération du

cloud pour relier des infrastructures nationales et industrielles autour de standards communs de sécurité, transparence et souveraineté («Backbone networks for pan-European cloud federations»).

La souveraineté numérique, pour améliorer la résilience

Cette réflexion autour de la souveraineté numérique rappelle celle née lors de la pandémie de Covid-19, qui avait mis en évidence la fragilité des chaînes d'approvisionnement mondiales, conduisant à diversifier les sources et à relocaliser certains segments critiques. De la même manière, l'incident du 20 octobre illustre la nécessité pour les acteurs économiques de renforcer la résilience de leurs chaînes numériques, devenues tout aussi vitales que les chaînes d'approvisionnement physiques.

En conclusion, et dans l'attente de solutions européennes matures, la responsabilité incombe aux entreprises: évaluer leurs dépendances, documenter leurs stratégies, négocier des clauses de réversibilité et d'assistance à la transition, tester régulièrement la capacité de faire face à des défaillances des prestataires matériels et maintenir en interne le know-how qui permet de surveiller les prestataires. Pour les organisations, et elles sont nombreuses, dont la donnée représente un actif essentiel, la dépendance vis-à-vis d'un fournisseur unique doit être considérée comme un risque majeur, à anticiper et à atténuer.

Le Temps publie des chroniques, rédigées par des membres de la rédaction ou des personnes extérieures, ainsi que des opinions et tribunes, proposées à des personnalités ou sollicitées par elles. Ces textes reflètent le point de vue de leurs autrices et auteurs. Elles ne représentent nullement la position du média.