Comme avec la sobriété numérique, la souveraineté numérique s'est finalement imposée assez rapidement dans l'agenda de la DSI. Et les chantiers ne manquent pas entre la recherche éperdue de solutions souveraines et labellisées comme telles, le soutien plus ou moins actif à de nouveaux acteurs français, et les réflexions sur le maintien de compétences internes capables le cas échéant de « reprendre la main » sur le SI.

Des stratégies qui s'élaborent dans les DSI

Les DSI sont des citoyens et, de même qu'ils ont été convaincus de la nécessité de s'engager pour la défense de l'environnement bien avant de véritablement lancer des actions pour la sobriété numérique, la prise de conscience des dangers d'une trop grande dépendance aux acteurs notamment américains a précédé le temps des actions concrètes pour s'en dégager.

Nous sommes dans cette période d'entre-deux et Capgemini Research Institute, dans une étude datant de juin 2021, avait déjà souligné que 52 % des DSI interrogés dans le monde mettaient le sujet de la souveraineté à l'ordre du jour de leur stratégie dans le cloud. Dominique Bascle, DSI de l'Université Sorbonne Paris Nord, qui intervenait récemment dans un dîner-débat de l'ANDSI (Association nationale des DSI) sur ce thème, confirme : *« Sur une échelle de un à dix concernant mes préoccupations, la souveraineté est au-delà de dix ! Il y a plusieurs axes à surveiller, sans qu'un soit prédominant. Celui de la confidentialité des données est évidemment très important, en particulier dans notre monde de la recherche où nous sommes responsables de protéger des informations sensibles, sur des projets qui ont été largement subventionnés par la puissance publique ou des entreprises privées. »*

Une échelle des risques à maîtriser

Le prisme du risque est omniprésent dans les analyses. Jusqu'à quel niveau en effet est-il souhaitable d'être indépendant, dans la mesure où cette indépendance a un coût ? Thomas Petit, que sa carrière de DSI a mené aussi bien dans le secteur hospitalier que dans le privé, voit bien la difficulté : *« Il est très difficile de demander à des Comex de ne pas céder aux sirènes du court terme et notamment des offres de cloud public, lorsque l'IT n'est pas au cœur du métier. »*

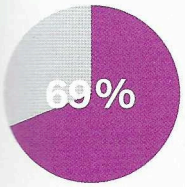
Adopter une position inverse, c'est par exemple accepter d'entretenir des compétences en interne pour assurer la réversibilité en cas de nécessité. Ce que continue de faire Dominique Bascle, qui rappelle la maxime : *« On n'externalise bien que ce que l'on maîtrise »*, et du coup se dit *« serein et en position de profiter des offres des Gafam »*.

La tentation existe aussi de construire des réponses à base de briques dont l'origine européenne ou française peut constituer des garanties. Mais Thomas Petit rappelle que *« si sur le plan technique, des solutions existent effectivement, l'assemblage reste toujours plus compliqué que d'aller chercher des services ou des produits prêts sur étagère chez les grands acteurs américains »*.

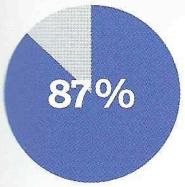
Faire grandir des offres locales

Autre possibilité, évoquée par Dominique Bascle : *« contribuer au développement d'offres qui n'existent pas encore »*. Les efforts de ces dernières années en matière d'open innovation peuvent aller dans ce sens, avec un soutien efficace à des start-up à même de servir les écosystèmes des entreprises. Il reste que leur périmètre d'action est limité et que les solutions apportées ne concernent souvent pas les cœurs de métiers. Le même bémol peut être apporté aux espoirs placés dans l'open source. Pour parvenir à grandir sans être rapidement phagocytées par la puissance de feu – en budgets et en ressources humaines – des acteurs américains, les communautés doivent rester focalisées sur des thématiques de niches, qu'elles soient techniques ou métier.

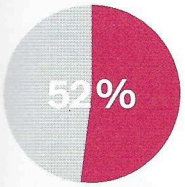
Ces stratégies, encore embryonnaires, engendrent généralement des surcoûts. Surprise, les DSI semblent prêts à faire un effort. Selon Serge Baccou, de Capgemini, les DSI sont disposés à payer un premium pour un hébergement de données sensibles qui serait juridiquement sûr – comprendre à l'abri des lois d'extraterritorialité américaines, notamment.



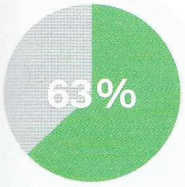
des DSI placent «*l'exposition potentielle à des lois d'extraterritorialité* et/ou la possibilité d'accès aux données par un gouvernement étranger» en tête de leurs préoccupations concernant leur stratégie cloud



des organisations voient la question de la souveraineté du cloud gagner en importance à l'avenir, soit via des solutions autonomes, soit via des modèles hybrides



intégreront la question de la souveraineté à leurs stratégies cloud globales dans les douze prochains mois (déclaration en juin 2021)



considèrent qu'un cloud souverain fournira un cadre sûr et sécurisé pour les données

SOURCE CAPGEMINI RESEARCH INSTITUTE (JUIN 2021, 1000 ORGANISATIONS INTERROGÉES DANS LE MONDE)

L'agilité plutôt que le château fort

«Nous n'avons pas ou plus les moyens de construire des châteaux forts. La solution, c'est d'être agiles. Par exemple, dans le secteur public, en mutualisant autant que possible», ajoute Dominique Bascle, tout en regrettant *«le manque de règles et de cadres posés, qui rend compliqué le travail en commun»*. Autre question qui mérite d'être soulevée, jusqu'où aller dans la recherche de solutions «continentales», et plus généralement, d'une moindre dépendance vis-à-vis des fournisseurs américains, si cette stratégie mène à des surcoûts trop importants pour le SI par rapport aux concurrents de l'entreprise, ou si elle n'est pas applicable à l'international ?

En attendant, les consultants sont déjà au travail, et ils ont l'oreille de nombreux DSI. C'est sans doute sur la question du cloud – la plus urgente ? – qu'ils ont le plus affiné leurs réponses à la question «que faire ?». Chez Octo Technology, le consultant Benjamin Bayart propose par exemple de considérer le cloud souverain comme un cloud sous contraintes (réglementaires, juridiques, politiques, économiques, etc.). Il en déduit une série d'attitudes possibles, qui vont du no-go s'il y a trop de contraintes – en attendant des offres souveraines compétitives – jusqu'au cloud US sous licence (S3ns ou Bleu par exemple), en passant par les clouds privés ou le choix d'opérateurs français. Capgemini, qui pousse l'offre Bleu avec Orange sur une base cloud Microsoft, ne dit pas autre chose en proposant de réfléchir dès maintenant à une hybridation, c'est-à-dire *«une stratégie multicloud, dans laquelle le cloud de confiance [ici sous licence US, NDLR] vient compléter le continuum de souveraineté où l'on retrouve aux deux extrêmes le cloud public et le cloud privé»*. En attendant le cloud souverain qui complétera la palette, aux DSI de déterminer aujourd'hui où sont les risques sur les données ou le MCO des SI et d'adapter leurs réponses en fonction des budgets disponibles, des risques tolérés et des priorités assumées au niveau du Comex. L'important, comme avec la sobriété numérique à ses prémisses, c'est de ne pas insulter l'avenir. ■

3 QUESTIONS À **Éric Le Quellenec,** avocat associé au sein du cabinet Simmons & Simmons

Depuis quand l'avocat que vous êtes s'intéresse-t-il à la souveraineté numérique ?

Depuis douze ans, c'est-à-dire depuis que je suis consulté par des clients signant des contrats avec des cloud providers, dont j'examine notamment les clauses de réversibilité. Avec le RGPD, puis les différentes évolutions des textes américains, jusqu'à cet accord d'adéquation, début juillet, entre l'Europe et les USA qui me paraît rétablir un équilibre plus sain, il y a eu beaucoup à faire.

Pensez-vous que l'émergence d'un cloud souverain européen soit indispensable du point de vue du droit ?

Elle l'est un peu moins depuis cet accord transatlantique, mais n'oublions pas le reste du monde ! Le problème reste le prix actuel des solutions SecNumCloud et demain, si un accord est trouvé entre les États européens, des solutions EUCS. Le surcoût d'un cloud souverain reste substantiel et un frein à son développement pour beaucoup d'entreprises, parfois dans un ratio de un à dix.

Quels conseils opérationnels pouvez-vous donner à nos lecteurs ?

En attendant une offre compétitive et sûre en Europe, je conseille d'investir sur des stratégies de cryptage efficace des données stockées chez les cloud providers. Et de ne pas se focaliser seulement sur les problématiques autour du cloud : il y a aussi beaucoup à surveiller au niveau des contrats, par exemple lorsque Microsoft propose encore à ses clients français de se référer au droit irlandais. Les flux transfrontaliers de données, les chaînes de sous-traitance et, bien sûr, les clauses de réversibilité, y compris dans leurs descriptions techniques précises, méritent aussi qu'on s'y arrête.