L'INFORMATICIEN

PAYS :France
PAGE(S) :50-51
SURFACE :144 %
PERIODICITE :Mensuel

DIFFUSION :(15000)
JOURNALISTE :Victor Miget

► 1 octobre 2022 - N°210

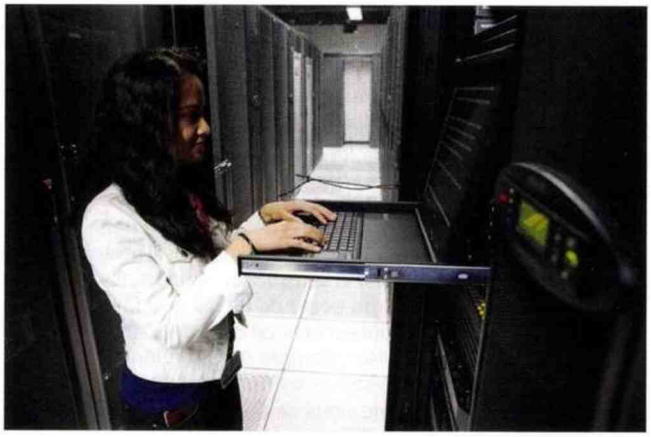
Cloud Act

Crise de confiance pour le Cloud de confiance

D'après une étude réalisée par le cabinet d'avocats Green Traurig, les offres hybrides de cloud computing pourraient être menacées par le Cloud Act, une loi permettant aux autorités américaines d'exiger, sous certaines conditions, la divulgation de données hébergées par des entreprises américaines. Les offres tricolores S3NS et Bleu, dont les services reposeront sur les technologies de Google et Microsoft, posent question.

Elles sont très attendues dans l'écosystème du cloud français. Ces offres dites « de confiance », dont les tricolores S3NS et Bleu sont les ambassadeurs, sont respectivement portés par Thales avec Google, et par Orange et Capgemini avec Microsoft.

Alors même que S3NS et Bleu n'existent pas encore — leur mouture finale est attendue pour 2024 —, l'Etat encourage déjà les institutions publiques, ministères, agences publiques, collectivités territoriales ou encore établissements de santé, à les adopter.



Selon S3NS, le rôle de Google se limitera essentiellement à faire en sorte que leur offre soit conforme au label SecNumCloud, à développer un catalogue de services, puis de délivrer des MAJ (mises à jour) fonctionnelles.

Et pour cause, ces offres dites « hybrides » doivent garantir une protection contre l'extraterritorialité de certains textes de loi, parmi lesquels le Clarifying Lawful Overseas Use of Data Act américain (Cloud Act). Pour synthétiser, le Cloud Act prévoit, dans certaines conditions (nous y reviendrons), que les données hébergées par des entreprises basées aux États-Unis soient accessibles aux autorités américaines, par exemple lorsqu'un juge en ferait la demande. Et ce, même si les données sont stockées sur des serveurs de l'entreprise basés à l'étranger.

Si le Cloud Act venait à s'appliquer aux offres françaises de cloud souverain en plus de nuire à leur raison d'être desdits cloud, la souveraineté numérique des entités recourant à ces cloud hybrides se verrait sérieusement égratigner.

L'étude de la discorde

Sur ce point, un rapport du cabinet d'avocats américain Greenberg Traurig LLP, commandé par les autorités néerlandaises, a semé le doute. Les travaux d'investigation révélés par La Tribune, concluent que *« les entités de l'UE peuvent être à la portée du Cloud Act, même si les entités de l'UE sont situées en dehors des États-Unis. »* Pour se prémunir d'une telle éventualité, l'ensemble des données traitées devront l'être *« en utilisant une entité non américaine »*. Celle-ci ne doit pas avoir de relation d'entreprise avec une société basée aux États-Unis ni de contacts trop importants avec ce continent, afin d'éviter *« qu'il soit raisonnable pour les États-Unis d'affirmer leur compétence sur l'entité de l'UE/entité non américaine »*. Ce dernier point implique notamment de ne pas vendre non plus de produits ni de services à des clients au pays de l'Oncle Sam.

Très logiquement, selon les conclusions du cabinet, l'entité européenne, si elle devait entretenir des relations avec une société américaine, ne devrait pas laisser à cette dernière la garde ou le contrôle des données stockées en Union européenne.

Google et Microsoft, des chevaux de Troie ?

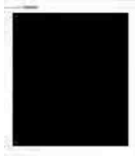
Problème : les offres tricolores S3NS et Bleu utiliseront toutes les deux des services créés par des entreprises américaines. Respectivement Google Cloud de Google, et Azur et Office 365 pour Bleu. De quoi semer le doute dans la presse, mais aussi du côté des politiques. Le député Modem Philippe Latombe a, par exemple, envoyé un courrier à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et à la Commission nationale de l'informatique et des libertés (Cnil), leur demandant si,

L'INFORMATICIEN

PAYS :France
PAGE(S) :50-51
SURFACE :144 %
PERIODICITE :Mensuel

DIFFUSION :(15000)
JOURNALISTE :Victor Miget

► 1 octobre 2022 - N°210



au regard de ces révélations, la terminologie « cloud de confiance » pouvait réellement s'appliquer aux futurs services de « S3NS ».

Contacté par L'Informaticien, Cyprien Falque, directeur général de S3NS, employé de Thales, tempère les craintes : *« Nous nous entretenons depuis plusieurs années avec Google afin de développer une solution qui fournisse l'équivalent des services de Google Cloud, mais protégée contre les lois extraterritoriales. »* Et le directeur général de rappeler que dans ce cadre, le modèle de S3NS repose sur un ensemble de mesures logiques, techniques et opérationnelles, qui garantissent que les données seront stockées dans des data centers de S3NS, contrôlées par S3NS et basées en France. Cyprien Falque est catégorique : *« S3NS ne peut pas tomber sous l'égide des autorités américaines. Google n'aura aucun contrôle ni accès sur les données et S3NS n'aura aucun ancrage physique aux États-Unis »* Et si Google deviendra bien un actionnaire minoritaire, il ne disposera d'aucun droit de vote et jouera, pour l'essentiel, un rôle d'observateur, nous assure-t-on.

Citoyens américains, circulez il n'y a rien à voir

Le cabinet d'avocats va même jusqu'à déconseiller d'employer des ressortissants américains *« ayant accès aux données pertinentes »*. Car ces derniers peuvent être obligés de les transmettre en vertu du Cloud Act. Dans le cas de S3NS, l'intégralité des employés sera de Thalès et issue de pays membres de l'Union européenne, promet Cyprien Falque. *« Seuls des opérateurs de S3NS seront autorisés à accéder aux trois data centers de S3NS, tous basés en France »*. Et si un employé de Google devait y accéder pour X raison, ce dernier serait toujours accompagné.

Une organisation qui sera sensiblement identique chez Bleu, future société française, détenue par des actionnaires exclusivement français (Capgemini et Orange), dirigé par des Français et avec un siège social sur l'Hexagone. *« Cette société aura son propre personnel qui travaille sur le sol français et ne donnera pas accès à ses plateformes à des entités américaines »*, indique une source qui souhaite rester anonyme. Bleu est construit de telle manière que Microsoft n'a aucun accès aux données. *« Tout ce qui est conçu l'est en lien très étroit avec l'ANSSI qui est très vigilante afin que ces solutions soient totalement immunes au Cloud Act et protégées contre des fuites de données. Et quand bien même Microsoft voudrait fournir des données, il ne pourrait pas »*, précise notre source.

SecNumCloud à la rescousse

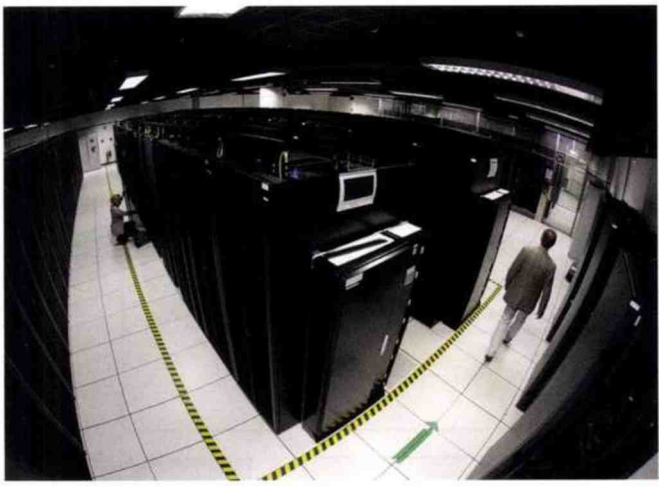
Reste que d'un point de vue opérationnel, les acteurs américains joueront bel et bien un rôle. Mais minime, nous assure-t-on. Les mises à jour de Google, elles, seront reçues via un réseau entrant parfaitement autonome, qui repose sur du matériel certifié par l'ANSSI et validé par S3NS, nous indique-t-on. Au moindre doute, le code source pourra être audité par le Français. Gestion des identités, certificat racine... Là encore, tout sera géré par S3NS, sans intervention de Google. Et en cas d'incident ? *« Les opérateurs seront exclusivement de S3NS. Un opérateur de Google n'aura jamais la main sur les opérations. »*

Quant aux conclusions de l'étude attestant qu'une entité de l'UE qui n'est pas située aux États-Unis, mais qui offre des services ou des produits à des clients aux États-Unis, peut être soumise au Cloud Act, S3NS confirme que son offre couvrira les besoins français, même si un adressage géographique plus large n'est pas exclu. Idem pour l'offre Bleu qui ne travaillera qu'avec des clients français, qu'elle accompagnera possiblement dans d'autres pays de l'Union européenne, nous confirme-t-on.

Au cas où les États-Unis exigeraient une divulgation de certaines données, l'Union européenne est en mesure de s'y opposer en l'absence d'accord sur l'encadrement du transfert des données vers les États-Unis, suite à l'invalidation par la justice européenne du Privacy Shield, en 2020.

Pour renforcer leurs lignes, S3NS et Bleu travaillent étroitement avec l'ANSSI, afin que leurs services soient conformes au label SecNumbCloud censé apporter *« des garanties fortes en matière de protection vis-à-vis des législations non-européennes »*, peut-on lire sur une page dédiée. Le Graal. Mais pour être certifiés, encore faut-il que les deux services répondent à tous les critères et soient opérationnels afin d'être évalués lors de tests physiques de l'infrastructure. Reste à savoir ensuite si la réalité des liens qui unissent les deux entités françaises à leurs partenaires américains suffiront à les priver de certification, et finalement de leur raison d'être. Réponse en 2024. ☐

Victor Miget



Plus que des enveloppes juridiques encapsulant des technologies américaines, ces clouds sont aussi des infrastructures, des serveurs, des hardwares, basés en France, opérés en France, et de propriété française. Dans ces deux cas, toutes les infrastructures seront déconnectées complètement des infrastructures de Microsoft et de Google. C'est en tout cas ce que confirment nos sources.