



## 16ème législature

|  |  |  |
|--|--|--|
| <b>Question N° : 71</b>  | De <b>M. Philippe Latombe</b> ( Démocrate (MoDem et Indépendants) - Vendée ) | <b>Question écrite</b>   |
| <b>Ministère interrogé</b> > Transition numérique et télécommunications  |  | <b>Ministère attributaire</b> > Transition numérique et télécommunications |
| <b>Rubrique</b> >numérique   | <b>Tête d'analyse</b> >Offre Google Cloud-Thales                             | <b>Analyse</b> > Offre Google Cloud-Thales.                                |
| Question publiée au JO le : <b>12/07/2022</b><br>Réponse publiée au JO le : <b>20/06/2023</b> page : <b>5637</b> |  |  |

### Texte de la question

M. Philippe Latombe appelle l'attention de M. le ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications sur l'offre Google Cloud-Thales, S3NS. Le site internet officiel de l'offre S3NS présente celle-ci comme « Le Cloud de confiance pour la France ». L'utilisation faite ici de l'expression « Le Cloud de confiance » pose le risque d'induire les acheteurs en erreur sur le caractère exclusif de cette offre eu égard au « label Cloud de confiance » annoncé par le Gouvernement dans le cadre de sa stratégie nationale pour le cloud, annoncée le 17 mai 2021. Pour tenter de faire obstacle à cette objection, S3NS joue sur la ponctuation. Sur la page des offres, il est écrit que les données seront hébergées « en France dans les *datacenters* Google » concernant l'offre transitoire, puis « dans les *datacenters* S3NS » concernant l'offre « Cloud de Confiance ». Or à ce jour, Google ne dispose pas de ses propres *datacenters* en France, mais loue des espaces dans des *datacenters* de tiers américains, ce qui pose la question de la réelle transparence de Google quant à l'architecture technique projetée. Par ailleurs, cette offre S3NS, dite « cloud de confiance », ne sera pas opérationnelle avant le second semestre de 2024, soit trois ans après l'annonce de la doctrine « Cloud au centre » du Gouvernement. Or Thales et Google annoncent prématurément sa disponibilité future pour, de leur propre aveu, encourager les clients à signer d'ores et déjà un contrat de services d'hébergement basé sur Google Cloud, sans les garanties de sécurité et les garanties juridiques de la qualification SecNumCloud. Les clients des hébergeurs français déjà qualifiés SecNumCloud sont donc sollicités par Google sur la base d'une hypothétique offre future, très incertaine à ce stade, malgré les affirmations qui leur sont répétées. Enfin, alors qu'il a été annoncé que S3NS serait une entreprise commune entre Thales et Google, la société créée est toujours à ce jour une SASU dont Thales est l'unique associé. S'agit-il d'un délai administratif, ou existe-t-il un montage juridique qui permettrait à cette SASU (de 10 K€ de capital) de faire remonter les fonds vers une autre entité commune cachée aux yeux du public ? La question mérite d'être posée. D'un point de vue juridique, est-on sûr qu'une entité commune Thales-Google permettra d'échapper aux lois extraterritoriales et en particulier au *Cloud Act* ? Il y a en effet le risque d'une sous-évaluation de la réalité du partage des parts sociales entre Google et Thales. Or si Google a le contrôle de fait de S3NS, celui-ci sera soumis au *Cloud Act*. Enfin, quelles garanties sont données par Thales sur sa réelle capacité à auditer le code source qui sera fourni par Google ? Il a été évoqué trois jours de décalage entre l'offre publique officielle de Google Cloud et celle de S3NS, pour permettre à Thales d'effectuer les contrôles de sécurité. Or ce délai sera très insuffisant si Google envoie d'un seul coup l'équivalent de plusieurs mois de travail de centaines d'ingénieurs. Quelle protection contre les *backdoors* pour éviter que les services américains ne bénéficient d'un accès détourné aux données hébergées ? Il souhaite savoir, au regard de la doctrine « cloud au centre » annoncée il y a maintenant plus d'un an, comment le Gouvernement envisage d'aborder ce dossier et les questions légitimes qu'il pose en matière de protection des données.



## Texte de la réponse

Le gouvernement s'est engagé dès la précédente mandature dans une politique ambitieuse reposant à la fois sur l'instauration d'un cadre réglementaire protecteur, au travers de la création du label « cloud de confiance » conditionné à l'obtention de la qualification SecNumCloud, et sur le soutien au développement de l'offre française et européenne, au travers de la stratégie d'accélération Cloud de France 2030, avec l'objectif d'atteindre une maîtrise technologique du cloud et d'ainsi contenir la dépendance des entreprises et administrations françaises à des technologies extra-européennes. Les offres partenariales en construction, dont le nombre a vocation à s'accroître dans les prochaines années, s'inscrivent dans cette démarche, et doivent offrir les garanties nécessaires à la protection de données particulièrement sensibles des administrations et des entreprises. Afin d'obtenir la qualification SecNumCloud, délivrée par l'ANSSI, et comme toute autre offre candidate à la qualification, le projet partenarial S3NS devra se conformer à l'ensemble des exigences prévues par le référentiel SecNumCloud révisé, qui inclut des critères techniques, capitalistiques et juridiques, garantissant à la fois un haut niveau de protection cyber et l'immunité des données sensibles aux législations à portée extraterritoriale. L'ANSSI suit de près la construction de l'offre S3NS et attend la candidature officielle afin d'enclencher une expertise pour la qualification SecNumCloud. En ce qui concerne la capitalisation de Google et le contrôle de S3NS, le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement : individuellement détenus à plus de 24% ; et collectivement détenus à plus de 39% ; par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non membre de l'Union européenne. Si le capital détenu par ces entités tierces se présente sous la forme d'actions admises aux négociations sur un marché réglementé, ces susdites entités tierces sont celles déclarées conformément au I de l'article L.233-7 du code de commerce. Ces entités tierces susmentionnées ne peuvent pas individuellement ou collectivement : en vertu d'un contrat ou de clauses statutaires, disposer d'un droit de veto ; en vertu d'un contrat ou de clauses statutaires, désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire. Par ailleurs, la qualification SecNumCloud doit permettre aux utilisateurs de facilement identifier les offres qui répondent à leurs besoins en matière de protection des données sensibles. Ainsi, afin de préserver la lisibilité et la transparence de l'offre cloud de confiance en construction, le gouvernement accompagne étroitement les administrations publiques dans le cadre de la mise en œuvre de la doctrine « cloud au centre », en particulier au travers de l'action de la Direction interministérielle du numérique, qui conseille les ministères dans le cadre de leurs projets de transformation numérique.