Thème : Cloud de confiance – quels enjeux ?

Résumé de notes prises lors de la réunion du « Cercle d'échanges de l'AEFR » du 11 octobre 2023.
A l'invitation de Crédit Mutuel Alliance Fédérale.

Les débats entre les membres de l'AEFR, accueillis au Crédit Mutuel par Nicolas Théry, Directeur général de Crédit Mutuel Alliance Fédérale, ont été introduits par Frantz Rublé, Directeur général adjoint - Crédit Mutuel Alliance Fédérale / Président - Euro-Information, et Michel Paulin, Directeur général - OVHcloud.

Didier Valet, président du Conseil d'Orientation des Cercles d'échanges de l'AEFR, a modéré les échanges. Il a, en avant-propos, souligné l'importance de mieux comprendre et mieux se saisir de cette thématique complexe, mais essentielle, du cloud de confiance.

En préambule, il a été rappelé que la numérisation des services était une tendance profonde, englobant des activités de plus en plus diverses. Le cloud devient un élément essentiel de toute offre commerciale, mais également de tout fonctionnement interne pour une entreprise. Pour les fournisseurs - ou exploitants - de cloud, il est nécessaire d'avoir accès à des services optimisés pour l'ensemble des secteurs d'activité des clients potentiels.

L'utilisation d'un cloud implique que les applications et données utilisées ne sont plus un ordinateur mais dans un ''nuage'' composé d'un nombre important de serveurs distants interconnectés. Cela nécessite une mise en réseau des serveurs (répartis, généralement, dans différentes aires géographiques) dont l'architecture permet l'utilisation des capacités de calcul et des emplacements de mémoire, où que l'on soit, dès lors que le terminal est relié au cloud.

Il existe deux grands types de cloud : le cloud public et le cloud privé. Ce dernier correspondant à la mise en place d'une infrastructure propre à l'organisation, qui fonctionne en circuit fermé. Ce type de cloud présente l'avantage d'offrir un niveau avancé de contrôle mais nécessite un espace non négligeable et une sécurisation avancée des bâtiments. A l'inverse, le cloud public est une infrastructure dont la gestion, du point de vue de l'entreprise, est confiée à un tiers. L'accès se fait alors via l'Internet public.

Le cloud de confiance, un enjeu de liberté

Le premier enjeu soulevé lors de cet échange fut celui de l'infrastructure qui pose celui, de la souveraineté sur les données.

C'est pourquoi, il fut relevé que la gestion de la sous-traitance était cruciale, d'un double point de vue : en confiant toute son infrastructure de stockage et gestion des données à un tiers, on n'en garde pas la maîtrise totale -ce qui selon certains acteurs présents pouvait représenter une erreur ; selon les mêmes acteurs, cela revenait à dépendre de la bonne volonté des prestataires dont la puissance est proportionnée au niveau et à la quantité d'informations (sensibles et communes) qu'ils possèdent et peuvent exploiter.

Certains participants autour de la table ont relevé l'importance d'avoir une régulation solide pour cloisonner de tels risques ; tous ont convenu qu'il s'agit d'un enjeu non seulement économique, mais également politique. Ainsi, fut-il noté que des acteurs étatiques, au premier rang desquels les Etats-Unis, avaient intégré l'utilité et la puissance des données dans leurs stratégies géopolitiques. L'exemple par excellence serait d'échanger ressources physiques contre ressources numériques, pétrole contre datas. Considérant ces éléments, il fut explicitement fait mention de l'importance de rappeler à tous les États membres de l'Union européenne (UE) les enjeux en présence, de sorte que n'existe plus la possibilité d'un accord du type protection industrielle contre cession de données. Les données sont une source de pouvoir essentielle dont l'UE aura besoin au XXIème siècle, il est donc nécessaire de parler d'une voix unie dans un environnement où les Etats-Unis mettent l'accent sur le pouvoir des données tandis que l'UE privilégie la protection.

Afin de contrecarrer la montée en puissance, pour ne pas dire la puissance monopolistique des Etats-Unis en la matière, l'ensemble des participants ont convenu de la nécessité d'un plus grand engagement du secteur public européen. L'illustration idoine a été apportée en mentionnant l'importance de l'investissement des Etats-Unis dans leurs start-up. Dans le quantique, certains membres recommandaient ainsi de soutenir en priorité Quandela, Alice & Bob ou encore C12 face à Google.

La stratégie optimale pourrait être de développer un champion européen afin de rééquilibrer la balance avec les Etats-Unis. Toutefois, certains acteurs soulignaient qu'un soutien national était une nécessité première et que le soutien de l'UE arriverait dans un deuxième temps. Ces mêmes acteurs notaient que le report de l'effort financier à l'unique échelon européen constituait une tentation à laquelle il ne fallait pas céder.
Est alors fait mention d'une des principales difficultés : celle de lutter avec une entité multiscalaire ayant un fort ancrage historique dans le champ informatique. Ainsi, il a été dit que 78% des dépenses de logiciels en France sont liées à des entreprises américaines. Une mise en perspective a d'ailleurs été interrogée : celle de l'estimation du PIB passant par Microsoft ou les grandes entreprises américaines de logiciel. Si aucun chiffre précis n'a été apporté, il faut être conscient du pouvoir que cela confère à ces entreprises.

D'un point de vue commercial, la politique de ces multiscalaires a également été jugée très agressive et anti-concurrentielle. En effet, ils pratiquent très généralement une offre proposant un ''bouquet'' de logiciels, dont le langage est illisible par des logiciels tiers créant un écosystème très fermé. Certains de ces groupes sont accusés de pratiques anticoncurrentielles au niveau européen. Et si la Commission peut se montrer en appui pour le respect de la libre concurrence, des participants estiment que certains États membres sont trop en retrait.
Il a été également notifié que l'entraide entre les différents acteurs européens, et a minima nationaux, était bien trop faible.

Fut également relevé le sujet de l'ergonomie des espaces de travail, qui complique la concurrence avec les multiscalaires américains. En effet, la problématique de la praticité des outils informatiques mis à disposition des collaborateurs est importante dans le choix des logiciels. La force de certains multiscalaires américains est de proposer aux entreprises de mettre à disposition des outils aussi performants que ceux que leurs collaborateurs utilisent dans un contexte non-professionnel, auxquels ils sont, de surcroît, habitués. L'optimisation du poste de travail doit être pensée lors de la sélection d'un opérateur de cloud, ou de la mise en œuvre d'un cloud privé, qui doit être lié à l'utilisation de logiciels informatiques.

Il fut également relevé que les prix des Graphics Processing Unit (GPU) n'ont cessé d'augmenter et représentent un très fort coût d'entrée, inaccessible pour la plupart des PME, qui pourtant doivent avoir accès à un cloud de confiance. Certains acteurs énonçaient ainsi que le recours à un tiers pour avoir accès à un cloud pouvait donc être nécessaire et qu'il était irréaliste de penser que chaque entreprise aurait la capacité de mettre en place l'infrastructure nécessaire au cloud privé. La lecture bipartite cloud privé vs cloud public est inopérante ; l'enjeu est autour de la question de la confiance dans le cloud et son opérateur.

Autour de la table, une grande partie des participants s'accordent à dire que le cloud de confiance repose sur un contrat. En l'occurrence, cela peut être une mise à disposition d'une technologie Microsoft sans sacrifier la souveraineté des données. Mais, le contrat est surtout celui de proposer un choix : faire usage d'un cloud public ou privé mais surtout, et avant tout, de pouvoir revenir sur ce choix. Le cloud de confiance est, en somme, un cloud basé sur une relation certes contractuelle, mais surtout une relation de confiance où l'utilisateur acquiert la certitude qu'il pourra dénoncer le contrat dans un temps futur et rester seul propriétaire de ses données sans qu'elles soient conservées ou utilisées de quelques manières que ce soit par un tiers. Le cloud de confiance est une question de liberté, avant même d'être une question de souveraineté.

L'importance de la réglementation

Les participants ont également insisté sur l'importance du Cloud Act, texte législatif américain dont l'acronyme signifie 'Clarifying Lawful Overseas Use of Data Act'. Avec pour objectif premier de lutter contre les crimes graves, notamment le terrorisme, la maltraitance des enfants et la cybercriminalité, le Cloud Act permet aux autorités américaines d'ordonner, au cours d'une enquête, aux fournisseurs de services en cloud de collecter, conserver et mettre à leur disposition des données en leur possession. Et il ne s'applique pas uniquement aux fournisseurs de services en cloud, mais s'étend également à certains fournisseurs de logiciels (suite Microsoft par exemple). Sur ce point précis, nombreux furent les participants à présenter la suite informatique comme un cheval de Troie, au même titre qu'Internet Explorer, il y a quelques années. - En outre, le Cloud Act introduit la notion d'extra-territorialité puisqu'il s'applique aux entreprises américaines, mais également à toute entreprise étrangère située en dehors du territoire américain fournissant suffisamment de services à la population américaine ou à des entreprises américaines. L'an dernier plus de 2.000 demandes ont été adressées par le gouvernement américain. C'est pourquoi, certaines entreprises apprécient de pouvoir s'installer dans l'UE, afin d'échapper au Cloud Act. Un élément que l'UE devrait mettre plus en valeur.

L'importance de la réglementation européenne repose également sur la mise en place d'une réglementation forte, capable d'empêcher la création de monopole. La réglementation en matière de lutte contre les pratiques anticoncurrentielles devrait être renforcée ainsi que la supervision, coordonnée à l'échelle européenne, de ce secteur ; notamment de sorte qu'il soit plus aisé de détecter les abus de position dominante, nécessitant parfois une surveillance accrue de certains acteurs.

Pour certains acteurs présents, le Digital Markets Act (DMA) est un d'échec ; ils conseillent de rouvrir le dossier estimant qu'au sein du DMA, le cloud est absent. Plus de $100 millions ont été déployées pour des actions de lobbying spécifique à ce dossier, notamment afin d'exclure le cloud de la législation. En outre, il ne peut être satisfaisant que des acteurs tel qu'Amazon, par exemple, échappent à la réglementation. Si l'UE semble avoir montré un certain dynamisme et a pu apparaître en faiseur de normes en matière de Règlement Général sur la Protection des Données (RGPD) et de Digital Operational Reislience Act (DORA), certains participants ont regretté que ce ne soit pas le cas concernant DMA/Digital Service Act (DSA), ces textes devraient être réouvert

pour les rendre plus solides et opérants.

Une législation devrait rendre obligatoire une assurance contre les fuites de données. Aujourd'hui, aucun fournisseur ne garantit les données et leurs fuites, ce qui est problématique car l'on estime, en moyenne, à 4% du chiffre d'affaires d'une banque de l'UE, le coût de ces fuites. Il a été recommandé par certains participants de prendre la certification Hébergeurs de Données de Santé (HDS) comme base pour constituer toute réglementation à venir.

Pistes et perspectives

Une première évolution concerne la qualification des données. Certains intervenants estiment que la bipolarisation données sensibles-données courantes est inopérante. Les données de santé et les données d'identité personnelles soient très sensibles, mais toutes celles d'observation comportementales sont aussi importantes, si ce n'est plus d'un point de vue commercial. Savoir qui regarde quoi, combien de temps et quel contenu engage du clic, est, pour le secteur industriel et commercial, bien plus important que de connaître l'adresse d'un individu.
D'autres participants ont tenu à apporter des éléments de complément, estimant qu'il était nécessaire d'avoir une conception très segmentée des données afin de faciliter le traitement de ces données en silos juridiques distincts. Toutefois, une approche segmentée n'implique pas une hiérarchie entre les données. Les deux visions sont compatibles.

Dans la complexe articulation entre structure et usage, l'architecture sera ce qui permettra de protéger les données, là où l'usage devra être encadré par l'éthique.

Les citoyens doivent être sensibilisés à ces questions. Car, s'il est souvent simple de mobiliser lorsque que la situation concerne du BtoC, cela devient plus complexe dans un dynamique de BtoB. Pourtant la question des données relève bien de l'autonomie stratégique de l'UE, de ses États membres, et in fine des citoyens.
Afin de mobiliser les citoyens les plus compétents et connaisseurs et permettre à la France et à l'UE de gagner cette bataille, il a été souligné qu'il fallait augmenter la part de femmes formées aux technologies de l'information, améliorer le financement des centres de recherche, des sociétés technologiques et des universités, favoriser l'innovation, renforcer les liens public/privé en développant la commande publique et la réglementation. Il faut aussi développer une conscience commune des enjeux en formant des coalitions entre la recherche, les acheteurs et l'offre publique.