_swissprivacy.law

Le secteur du cloud computing au prisme du droit de la concurrence

Michael Montavon, le 27 mai 2024

Le secteur du cloud computing soulève des préoccupations en matière de droit de la concurrence. En 2023, deux études menées par les autorités françaises et anglaises ont mis en évidence certaines pratiques jugées problématiques des fournisseurs de services cloud.

Avis n° 23-A-08 du 29 juin 2023 de l'Autorité française de la concurrence portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »)

Final report du 5 octobre 2023 de l'Autorité anglaise de régulation des télécommunication (Ofcom) sur le cloud services market

Dans deux études publiées en 2023, l'Autorité française de la concurrence et l'Autorité anglaise des télécommunications ont analysé diverses pratiques liées au secteur du cloud au travers des outils classiques du droit de la concurrence que sont l'abus de position dominante, la lutte contre les ententes illicites, le contrôle des concentrations et l'abus de dépendance économique. Bien que les études se concentrent sur les services cloud, des pratiques comparables peuvent se retrouver dans le secteur des logiciels et des licences informatiques.

La contractualisation

Les fournisseurs de services cloud concluent deux principaux types de contrats avec leurs clients :

Dans l'immense majorité des cas, il s'agit de contrats standards, formulés sous forme de conditions générales et directement conclus sur le site web du fournisseur, sans négociation. Ils sont généralement à durée indéterminée et résiliables (presque) à tout moment par le client.

Seuls quelques clients professionnels de plus grande taille parviennent à obtenir des contrats (un peu) plus personnalisés. D'une durée déterminée, ces contrats contiennent certaines

clauses négociées et éventuellement une remise commerciale en contrepartie de l'utilisation d'un certain volume ou d'une certaine valeur de services. Mais ils restent la plupart du temps des contrats génériques, pré-rédigés par les fournisseurs de services eux-mêmes. Il est par conséquent toujours difficile d'obtenir leur modification.

Face à cette situation, certains clients commencent néanmoins à mieux s'organiser. Ils rédigent leurs propres conditions générales d'acquisition à l'attention de leurs futurs partenaires. À titre d'exemple, dans le secteur public, l'organisation Administration numérique suisse (ANS) fournit des conditions générales types ainsi que plusieurs modèles de contrats-types que la Confédération, les cantons et les communes tentent d'imposer à leurs fournisseurs. Des initiatives du même type existent aussi dans le secteur privé. Même si cela ne signifie pas encore que ces documents sont par la suite forcément acceptés tels quels par les fournisseurs, cette pratique oblige au moins à ouvrir la discussion sur les conditions d'acquisition du client.

Le risque de *lock-in*

En économie, la dépendance au fournisseur (également appelée verrouillage propriétaire ou verrouillage du client – *lock-in* en anglais) est un scénario dans lequel un client devient dépendant d'un fournisseur pour des produits et des services, parce qu'il n'est pas capable de changer de fournisseur sans efforts, ni coûts prohibitifs.

Sur le plan technique, le verrouillage peut venir de l'utilisation de technologies propriétaires ou de standards spécifiques à un fournisseur. Par exemple, certains fournisseurs de cloud développent des formats de données et des interfaces de programmation d'applications (API) qui sont uniques à leur environnement. Cela signifie que les données et les applications développées sur une plateforme spécifique peuvent nécessiter une réécriture substantielle pour fonctionner sur une plateforme différente. Cette spécificité engendre des coûts élevés de transition, dissuadant les clients de migrer leurs applications et leurs données vers un nouveau fournisseur de cloud.

Les architectures cloud modernes encouragent l'utilisation de microservices et de fonctions intégrées, qui peuvent créer des dépendances complexes entre les différents services d'un même fournisseur. Par exemple, une entreprise peut utiliser à la fois l'hébergement de données, les fonctions de calcul, et les services d'analytique d'un seul fournisseur. La migration d'une partie de cet écosystème vers un autre fournisseur devient alors non seulement techniquement complexe mais aussi coûteuse, en raison de l'interdépendance des services qui nécessitent d'être migrés ensemble pour maintenir la fonction dans sa globalité.

Sur le plan contractuel, les fournisseurs de cloud peuvent imposer des conditions qui compliquent encore davantage la migration. Les contrats peuvent inclure des durées d'engagement longues avec des pénalités pour résiliation anticipée, des clauses de renouvellement automatique, des frais élevés pour l'exportation des données ou des limitations sur la fréquence de ces exportations. Ils peuvent aussi volontairement omettre de prévoir toute assistance visant à permettre au client de récupérer ses données ou de les migrer sur un autre cloud.

La tarification

De manière générale, la structure tarifaire des services cloud est souvent considérée comme opaque, voire artificielle. Les fournisseurs de services cloud utilisent des modèles de tarification basés sur une multitude de variable, qui sont difficiles à appréhender. Au-delà de cet aspect, certaines pratiques spécifiques intéressent plus particulièrement les autorités de la concurrence.

Les rabais combinés (« *committed spend discounts* ») sont offerts par des fournisseurs de cloud d'une certaine importance en échange d'un engagement de dépense minimum de la part du client et/ou l'achat de plusieurs services combinés. Bien que cela puisse réduire les coûts pour les clients, ces rabais incitent également à rester avec un seul fournisseur pour tous leurs besoins en cloud, même lorsque d'autres fournisseurs pourraient offrir des services de meilleure qualité ou plus adaptés aux besoins spécifiques du client.

Les « crédits cloud » sont utilisés comme une forme d'incitation par laquelle des fournisseurs de cloud offrent à leurs clients des services gratuits à titre d'essai dans un délai défini, généralement de 6 à 12 mois. Même s'ils offrent des opportunités de développement intéressantes pour les start-ups et les nouvelles entreprises notamment, ils peuvent encourager les entreprises à s'engager davantage dans des architectures et des services spécifiques, rendant difficile toute migration future vers des solutions concurrentes.

Les frais de sortie (« e*gress fees* ») sont imposés par des fournisseurs de cloud pour le transfert de données hors de leur environnement. Ils peuvent engendrer des coûts supplémentaires significatifs pour les clients qui doivent déplacer des données entre différents fournisseurs ou qui souhaitent simplement ré-internaliser leurs données ou changer de fournisseur. Ces frais sont particulièrement critiqués. Tant l'étude française que l'étude anglaise indiquent que les coûts facturés sont sans rapport avec les coûts incrémentaux de la fourniture du service.

Finalement, certains fournisseurs de services cloud peuvent profiter d'une situation de *lock-in* pour agir sur leurs tarifs. Une fois qu'un client est profondément intégré dans l'environnement d'un fournisseur de cloud, changer de fournisseur devient non seulement techniquement complexe mais aussi coûteux pour le client. Le fournisseur peut alors choisir de capitaliser sur cette dépendance en augmentant drastiquement et sensiblement ses tarifs. Dans son rapport « Magic Quadrant 2021 » concernant les offres d'infrastructures de cloud public, Gartner indiquait à ce propos que des clients d'Amazon Web Services avaient subi des pressions à l'occasion du renouvellement de leurs contrats. En pratique, il n'est, en effet, pas rare que des fournisseurs décident à ce moment d'augmenter leurs tarifs précédents, parfois même en allant jusqu'à les multiplier.

Les clauses d'exclusions ou de limitation de responsabilité

Il est fréquent dans le secteur des services cloud que les fournisseurs imposent des clauses qui excluent ou qui limitent toute responsabilité du fournisseur et de ses sous-traitants. En droit suisse, de telles clauses sont généralement valables. Seuls les dommages causés par dol, faute grave ou négligence grave du fournisseur ne peuvent pas être exclus (art. 100 al. 1 CO). Rien n'empêche non plus le fournisseur de s'exonérer de toute responsabilité pour ses propres sous-traitants (art. 101 al. 2 CO). La situation est néanmoins différente dès lors qu'on se situe dans le domaine de la protection des données. En sa qualité de sous-traitant du responsable du traitement, le fournisseur de services cloud demeure responsable des traitements qu'il confie à son tour à des tiers et ne peut donc pas s'exonérer des responsabilités prévues par la loi (cf. le texte très clair de l'OPDo par rapport au fait qu'il s'adresse tant au responsable du traitement qu'à son sous-traitant).

Même si aucune partie n'aime voir la responsabilité de son co-contractant exclue ou limitée, de telles clauses ne sont pas forcément le signe d'un contrat léonin. Dans le secteur du cloud, la limitation de responsabilité est une question de scalabilité. Un logiciel à CHF 50'000.- peut être utilisé pour concevoir un système de plusieurs centaines de millions de francs ou pour gérer un portefeuille d'actifs de plusieurs milliards. En cas de dysfonctionnement, le même logiciel peut ruiner son usager. Le fournisseur ne pourrait cependant pas faire des affaires si chaque vente impliquait un risque réel de responsabilité équivalent à plusieurs centaines de millions, voire de milliards, de francs.

C'est pourquoi la responsabilité des fournisseurs de services cloud est presque toujours limitée aux dommages directs et plafonnée à un montant global (*cap*). Bien que cette méthode soit globalement acceptée, le montant du cap doit néanmoins être validé par chaque partie

en tenant compte de la prestation fournie, des tarifs fixés et des dommages potentiels en cas de mauvaise exécution. Les contrats cloud peuvent, certes, ne pas être soumis à une obligation de résultat. Mais une clause d'exclusion de responsabilité qui va jusqu'à libérer une partie de faire précisément ce qu'elle s'engage à faire, y compris en termes de diligence, est problématique et ne devrait pas être acceptée sans autre.

Les *hyperscalers*

Le marché du cloud est largement dominé par un petit nombre d'acteurs majeurs, à l'image d'Amazon, Microsoft, et Google. Leur capacité à offrir des écosystèmes intégrés de services, couplée à leur puissance financière et à leur base de clients existante, leur confère des avantages concurrentiels significatifs. Ces acteurs peuvent ainsi exercer une influence considérable sur les structures de marché en ayant recours à des pratiques de ventes liées, en englobant des services non-désirés dans des offres groupées ou en offrant des avantages tarifaires que des concurrents de taille moindre ne pourraient jamais proposer.

En raison des infrastructures (IaaS) et des plateformes (PaaS) dont ils disposent, les *hyperscalers* collaborent souvent dans le cadre de partenariats stratégiques avec des « Independant Software Vendrors » (ISVs). Ces derniers bénéficient alors de l'infrastructure massive et de la portée des *hyperscalers* pour offrir leurs propres logiciels (SaaS). Ces collaborations peuvent entraîner des innovations et des services améliorés pour les clients. Cependant, elles peuvent aussi créer des risques, si elles débouchent sur des pratiques exclusives ou des ententes sur les prix, les territoires de vente ou les clients cibles, ou si les *hyperscalers* favorisent certaines ISVs par rapport à d'autres.

Les outils du droit de la concurrence

Pilier de la régulation économique, le droit de la concurrence compte plusieurs instruments permettant d'intervenir contre les pratiques anti-concurrentielles. La loi sur les cartels (LCart ; RS 251) a pour but d'empêcher les conséquences nuisibles d'ordre économique ou social imputables aux cartels et aux autres restrictions à la concurrence. Elle repose sur trois piliers :

En premier lieu, la LCart interdit les accords entre entreprises occupant des échelons du marché identiques ou différents, dans la mesure où ils visent ou entraînent une restriction à la concurrence (art. 4 al. 1 et 5 LCart). Cela peut notamment concerner les alliances stratégiques et les partenariats renforcés, entre fournisseurs de services cloud ou les accords d'interopérabilité spécifiques entre certains acteurs du cloud et du SaaS. Paradoxalement,

des solutions de standardisation, qui favorisent à première vue l'interopérabilité et donc le changement de fournisseur, peuvent, dans certains cas, devenir problématiques en empêchant l'émergence de solutions alternatives et en paralysant l'innovation par le biais de pratiques de verrouillage technique.

En deuxième lieu, la loi sanctionne les entreprises qui abusent d'une position dominante, parce qu'elles sont à même, en matière d'offre ou de demande, de se comporter de manière essentiellement indépendante par rapport aux autres participants du marché (art. 4 al. 2 et 7 LCart). En été 2023, la Commission européenne a ouvert sur ce fondement une enquête formelle afin de déterminer si Microsoft avait profité d'une position dominante avec son produit de communication et de collaboration Teams. La Commission cherche à déterminer a) si, en ne donnant pas aux consommateurs le choix d'inclure ou non l'accès à Teams lorsqu'ils acquièrent Office ou Microsoft 365, Microsoft accorde ou non à ce produit un avantage en matière de distribution et b) si Microsoft limite l'interopérabilité entre son produit et les offres des concurrents en matière d'outils collaboratifs. Dans une autre affaire datant de 2007, le Tribunal de l'Union européenne a confirmé la décision de la Commission européenne selon laquelle le refus de Microsoft de divulguer des informations en matière d'interopérabilité constituait un abus de position dominante (Arrêt du Tribunal de première instance du 17 septembre 2007 – Microsoft/Commission, Affaire T-201/04). Windows équipant à cette époque 90% des ordinateurs individuels dans le monde, la Commission estimait que Microsoft devait donner à ses concurrents un accès à un certain nombre de données techniques relatives à Windows afin de leur permettre de développer des logiciels compatibles.

Un cran en dessous de l'abus de position dominante, l'abus de dépendance économique représente une autre voie d'intervention, lorsqu'une entreprise bénéficie d'un pouvoir de marché relatif. Elle sanctionne l'exploitation abusive par une entreprise de la situation de dépendance dans laquelle se trouvent ses partenaires commerciaux, faute de possibilité suffisante et raisonnable de se tourner vers d'autres entreprises (art. 4 al. 2bis et 7 LCart). Contrairement à l'abus de position dominante, la situation de dépendance économique ne s'apprécie pas par rapport à la position d'une entreprise sur un marché donné, mais au regard des spécificités de la relation commerciale qu'elle entretient avec ses partenaires. Ce mécanisme peut, par exemple, se révéler pertinent pour appréhender des cas où des fournisseurs de services cloud imposent des conditions contractuelles ou tarifaires particulièrement agressives à des clients se trouvant en situation de *lock-in*.

En troisième lieu, la LCart prévoit que les concentrations impliquant de grandes entreprises soient soumises à l'examen de la Commission de la concurrence (COMCO) afin d'établir si

elles vont créer ou renforcer une position dominante capable de supprimer une concurrence efficace (art. 4 al. 3 et 10 LCart). Les scenarios exposés ci-dessus peuvent, en effet, être renforcés par une politique d'acquisitions agressive de la part d'entreprises déjà présentes sur le secteur du cloud afin de renforcer leur position sur le marché.

Perspectives

Il est loin le temps où il était encore possible d'acheter une licence perpétuelle sur un logiciel standardisé. Aujourd'hui, la plupart des éditeurs de logiciels privilégient des modèles d'abonnement modulables, grâce auxquels ils conservent intégralement la main sur les produits qu'ils vendent et sur les revenus qu'ils en retirent. Cette situation crée toutefois un environnement où la loyauté des clients est moins le résultat d'une satisfaction ou d'une préférence volontaire que d'une contrainte économique et technique.

Le droit de la concurrence, on l'a vu, prévoit certains outils capables de réguler des pratiques jugées anti-concurrentielles. Mais il est rarement utilisé, car c'est un droit difficile à manier et qui permet uniquement d'appréhender une situation *a posteriori*. Conscient des lacunes de cette approche, le législateur européen travaille à mettre en place des solutions *ex ante* via des textes modernes et ambitieux.

Le règlement du 14 septembre 2022 sur les marchés numériques (Digital Markets Act ; DMA) vise à lutter contre les pratiques anticoncurrentielles des géants du Net et à corriger les déséquilibres de leur domination sur le marché numérique européen. Il cible les plateformes numériques considérées comme « gatekeepers », celles qui ont une influence dominante sur le marché. Le DMA impose à ces entreprises différentes obligations pour éviter les comportements anticoncurrentiels, notamment le fait de ne pas imposer ou favoriser leurs propres solutions, de rendre interopérables certaines fonctionnalités de base de leurs services, de partager certaines de leurs données de performance marketing ou publicitaire, ou encore de permettre la désinstallation des logiciels préinstallés.

Le règlement du 25 novembre 2022 sur les données (Data Act ; DA) a pour objectif d'assurer une meilleure répartition entre les acteurs de l'économie de la donnée. Il complète notamment le champ d'action du DMA en imposant des exigences de nature contractuelle, commerciale et technique aux fournisseurs de services cloud afin de permettre le passage d'un service à l'autre. Le DA prévoit notamment un renforcement de la portabilité des données, des applications et des autres actifs numériques, la suppression progressive des frais de transferts de données et de migration ainsi que la mise en place de moyens techniques favorisant ces changements. Concrètement, à compter du 11 janvier 2024 et jusqu'au 12 janvier

2027, les fournisseurs peuvent uniquement imposer des frais de changement de fournisseur équivalant aux coûts effectifs du processus de changement. À compter du 12 janvier 2027, ils ne pourront plus imposer aucun frais de changement de fournisseur.

Finalement, le règlement sur la résilience opérationnelle numérique du secteur financier (cf. https://swissprivacy.law/285/) adresse aussi cette problématique pour les entités financières. Il encourage, en particulier, l'adoption d'une stratégie multi-cloud afin d'éviter les situations de *lock-in*. Il oblige aussi à insérer dans les contrats passés entre une entité financière et un fournisseur de services cloud des dispositions garantissant de récupérer les données confiées dans un format facilement accessible et assurant, pour certaines catégories de services, une période de transition adéquate en cas de changement de fournisseur.

Difficile de prédire quel sera l'impact de ces textes en Suisse. S'il n'est pas totalement exclu que les fournisseurs de services cloud actifs au niveau européen décident d'appliquer ces mêmes règles à la Suisse, rien ne les y oblige pour autant. Quant aux fournisseurs de services cloud suisses, leur soumission volontaire à ces mêmes règles ne va pas de soi non plus. Dès lors, le législateur suisse serait bien inspiré d'envisager l'adoption de règles équivalentes.

Proposition de citation : Michael Montavon, Le secteur du cloud computing au prisme du droit de la concurrence , 27 mai 2024 *in* www.swissprivacy.law/301