Favoriser l'adoption du Cloud en France

Entre compétitivité et souveraineté

Christian SAINT-ÉTIENNE

Hubert VÉDRINE

Aurélien PORTUESE

- INSTITUT - CHOISEUL

- Les Notes Stratégiques -

Les Notes Stratégiques

Adressées aux acteurs économiques, institutionnels et politiques mais aussi à un public averti, les Notes Stratégiques de l'Institut Choiseul ont vocation à analyser et éclairer les principaux débats économiques, sociaux et politiques sous le prisme des ruptures géopolitiques et géoéconomiques à l'œuvre dans le monde contemporain.

Institut Choiseul

Favoriser l'adoption du Cloud en France

Entre compétitivité et souveraineté

Christian SAINT-ÉTIENNE
Universitaire et Consultant en stratégie

Hubert VÉDRINE
Ancien Ministre des Affaires étrangères

Aurélien PORTUESE
Docteur en droit et Avocat au barreau de Paris

Novembre 2021

À propos des auteurs :

Christian Saint-Étienne *est docteur d'Etat en économie et professeur titulaire de la Chaire d'économie industrielle au Conservatoire National des Arts et Métiers. Ancien économiste au Fonds Monétaire International (FMI) et administrateur de l'Organisation de coopération et de développement économique (OCDE), Christian Saint-Etienne a fondé en 1996 un cabinet de conseil spécialisé en analyse stratégique des marchés et en conseil stratégique pour les entreprises patrimoniales (Conseil stratégique européen SA). Il est également l'auteur de nombreux ouvrages dont La Fin de l'Euro (2009), l'Incohérence Française (2012), l'Iconomie pour sortir de la crise (2013) et, le dernier, Le Libéralisme Stratège, paru aux éditions Odile Jacob en septembre 2020.*

Hubert Védrine *est un haut-fonctionnaire et homme politique français. Ancien élève de l'ENA, il a été Ministre des Affaires étrangères (1997-2002) et fut à l'Elysée successivement conseiller diplomatique, porte-parole et, surtout, secrétaire général (1981-1995). Il est le fondateur d'Hubert Védrine Conseil, une société de conseil spécialisée dans les problématiques internationales, économiques et géopolitiques. Il est également Président de l'Institut François Mitterrand. En 2020, il a été désigné par la France pour participer aux réflexions sur l'OTAN en 2030. Il est également l'auteur de nombreux ouvrages dont Face à l'Hyperpuissance (2003), Continuer l'Histoire (2007), La France au défi (2014) et Sauver l'Europe (2016). Il a publié en février 2021 un Dictionnaire amoureux de la géopolitique (Plon, Fayard).*

Aurélien Portuese *est docteur en droit (Paris II) et avocat au barreau de Paris. Spécialisé en économie et en politique de la concurrence dans l'économie numérique, il est directeur de la politique antitrust et de l'innovation à la Fondation pour la technologie et l'innovation (ITIF), le principal groupe de réflexion mondial sur la science et la technologie. Ses recherches portent plus particulièrement sur les implications en matière d'innovation de l'application des règles antitrust aux plateformes numériques. Il enseigne le droit de la concurrence au Global Antitrust Institute de la George Mason University ainsi qu'à l'Université Catholique de Paris.*

Synthèse

Le Cloud computing, ou l'informatique en nuage, est devenu pour les entreprises un outil fondamental dans la course à l'innovation : intelligence artificielle, biotechnologies, voiture du futur, *smart city*, énergie, etc. Le Cloud n'est plus une option, c'est devenu un impératif. Plus qu'une solution de stockage d'information, il représente une capacité quasi infinie de calcul et de traitement des données soutenue par une gamme très large d'applications. Cette technologie permet à toute organisation - des entreprises de toutes tailles aux administrations centrales en passant par les collectivités territoriales - d'avoir accès au meilleur de ce qu'offre le digital et donc d'innover plus facilement.

Sa place dans la vie économique et sociale grandissant, et les fournisseurs avec, le Cloud est devenu ces dernières années un véritable sujet de politiques publiques, soulevant des enjeux macro et micro économiques, juridiques et géopolitiques alors même que le marché est très loin d'avoir atteint tout son potentiel de développement. Parallèlement, son utilisation en France est inférieure à celle constatée dans des économies comparables, entrainant un retard dans la R&D et l'innovation qui sont de plus en plus dépendantes de cette technologie.

Conscient du retard pris par les entreprises françaises tout comme des enjeux soulevés par cette technologie, les pouvoirs publics se sont saisis du sujet en déployant une stratégie nationale pour le Cloud reposant sur trois piliers : (1) « Cloud au centre », pour accélérer l'adoption du Cloud par les entreprises et les administrations ; (2) « Cloud de confiance », un label qui ajoute des contraintes liées à la souveraineté : passer au Cloud oui, mais au Cloud français ; (3) une politique industrielle dédiée pour faire émerger des champions français du Cloud.

Le « Cloud de confiance » illustre parfaitement la multiplicité des enjeux politiques et géopolitiques du Cloud : la maîtrise de la donnée, qui représente un atout certain dans la compétition mondiale, l'avantage dans la course à l'innovation que procure une puissance de calcul supérieure à celle des autres et enfin la question de la sécurité des données face aux cyberattaques, à l'évidence critique.

L'Union européenne et les États-Unis sont en première ligne : projet Gaia X, invalidation du Privacy Shield, transferts transatlantiques de données... autant d'évènements qui rythment les relations de la France et de l'Union européenne avec les États-Unis. Dans ce contexte, la montée en puissance rapide de la Chine soulève des craintes.

Autant d'enjeux qui mal appréhendés pourraient porter préjudice non seulement aux fournisseurs de Cloud, quelles que soient leurs nationalités, mais aussi et surtout aux utilisateurs finaux. Un risque d'autant plus grand que des pratiques anticoncurrentielles pourraient rendre plus lente l'adoption de celui-ci et accentuer le retard de la France.

La technicité des sujets et leur compréhension, parfois erronée, alimentent un climat de méfiance envers la technologie et de défiance entre les États. Cette note s'attache à expliquer la place grandissante qu'occupe le Cloud dans l'économie mondiale, à en expliciter les enjeux politiques et géopolitiques et à analyser les freins rencontrés par son adoption en France pour essayer de les lever.

Chapitre 1 - Christian Saint-Étienne

Le Cloud en France et en Europe : un retard à rattraper et des opportunités de croissance à saisir

Introduction

Le Cloud computing ou « l'informatique en nuage », tel que défini par la CNIL[1], désigne l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. À l'inverse des serveurs dits sur site ou *on-premise*, les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage, le Cloud, composé de nombreux serveurs distants interconnectés.

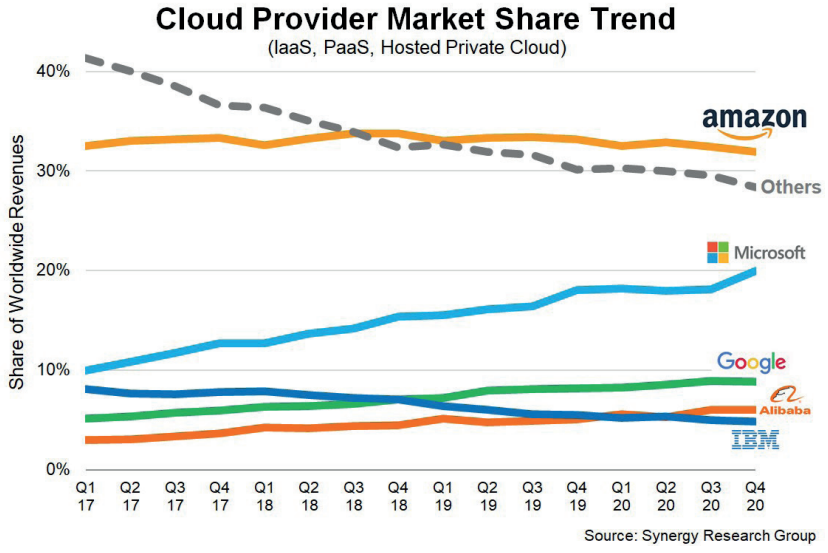
Cette technologie, indispensable pour permettre aux entreprises européennes de se faire une place dans les technologies de demain – intelligence artificielle, voiture du futur, big data, *smart city*, biotechnologies, etc. – reste peu développée et sous-utilisée en Europe. Sujet nébuleux, le Cloud est souvent desservi par une mauvaise appréhension de ses enjeux et une méconnaissance des bénéfices de son utilisation pour les organisations, comme pour les États.

Le Cloud est un environnement où la présence mondiale et la capacité à industrialiser les opérations de traitement à grande échelle sont des avantages compétitifs massifs. Détenus majoritairement par les fournisseurs américains de services Cloud (35% par AWS, 20% par Microsoft Azur, 10% par Google Cloud[2]) à l'échelle mondiale, le marché du Cloud est loin d'avoir atteint toute

1 *https://www.lebigdata.fr/definition-Cloud-computing*

2 *https://www.srgresearch.com/articles/Cloud-market-ends-2020-high-while-microsoft-continues-gain-ground-amazon*

sa profondeur de champ : selon Gartner, seulement 4% des systèmes d'information sont sur le Cloud à l'échelle mondiale, contre 96% sur des équipements d'entreprises. Le basculement vers le Cloud ne fait donc que commencer et le marché est promis à une croissance exponentielle : en France, le marché du Cloud pèse aujourd'hui 15 milliards d'euros et croît de plus de 20% par an.



I. Les avantages du Cloud

A. Rentabilité et efficience

Aujourd'hui, les entreprises et les services publics n'ont plus besoin d'acquérir leur propre centrale électrique, de traitement des eaux ou leurs propres serveurs informatiques. Elles achètent directement leurs ressources auprès de grandes structures gérées par des fournisseurs spécialisés, bénéficiant ainsi d'économies d'échelle. Comme pour l'électricité ou l'eau, cette pratique gagnerait à devenir la norme pour le Cloud computing, plus performant que l'informatique traditionnelle.

Le Cloud permet aux entreprises de toutes les tailles de profiter d'économies d'échelle et donc de créer de nouvelles opportunités commerciales. En moyenne, les clients du Cloud réalisent un retour sur investissement net de US$2,5 pour chaque dollar investi dans les services Cloud (Deloitte 2018)[3], et la Commission européenne estime que l'adoption du Cloud computing entraine une réduction de 20% à 50% des coûts informatiques totaux[4]. Au-delà de l'ouverture des possibilités techniques sur le Cloud pour les développeurs, le Cloud permet également d'accélérer les activités des entreprises et d'améliorer leur modèle économique. D'après l'étude McKinsey (2021)[5], les bénéfices du Cloud pourraient créer jusqu'à 1 000 milliards de dollars de richesses nouvelles pour l'économie mondiale d'ici 2023. La flexibilité offerte par le Cloud permet aux entreprises d'adapter facilement leur service informatique en ajustant instantanément les capacités à leurs besoins, contribuant davantage à réduire leurs coûts informatiques.

B. Une technologie propre

Contrairement aux idées reçues, l'utilisation du Cloud permet aussi de réduire la consommation d'énergie et d'améliorer la durabilité de l'informatique : une enquête menée par Accenture révèle que le Cloud permet de réduire significativement les émissions de carbone des entreprises utilisatrices. Les grandes entreprises réduisent ainsi leur empreinte carbone jusqu'à 30% par utilisateur et les petites entreprises jusqu'à 90%. Un rapport du Carbon Disclosure Project (CDP) a également indiqué que les services externalisés peuvent réduire les émissions annuelles de carbone de 5,7 millions de tonnes[6]. C'est plus que les émissions annuelles de

3 https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-Cloud.pdf

4 https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-Cloud-computing-europe

5 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Clouds-trillion-dollar-prize-is-up-for-grabs

6 https://www.insee.fr/fr/statistiques/2015759

l'ensemble de la population française (11,2 tonnes par an et par habitant).

C. Un rempart de sécurité

Au-delà de l'agilité et de la performance, le Cloud améliore significativement la cybersécurité des systèmes d'informations : les principaux fournisseurs de Cloud sont capables de restaurer les sauvegardes qui peuvent être faites en double ou en triple selon le niveau de service exigé par le client, mais aussi de réduire les surfaces d'attaque sur les données grâce aux couches de protection qu'ils mettent en place sur leurs systèmes. Aucun système n'est infaillible mais une des clés de résilience vient de la capacité et de la vitesse de restauration des systèmes.

La crise sanitaire a démontré l'importance du Cloud computing. En raison de la pandémie, l'année 2020 a été marquée par une migration massive vers le travail à distance et le commerce en ligne en seulement quelques jours dans toutes les régions du monde. Un changement rapide qui n'aurait pas été possible sans le recours au Cloud computing.

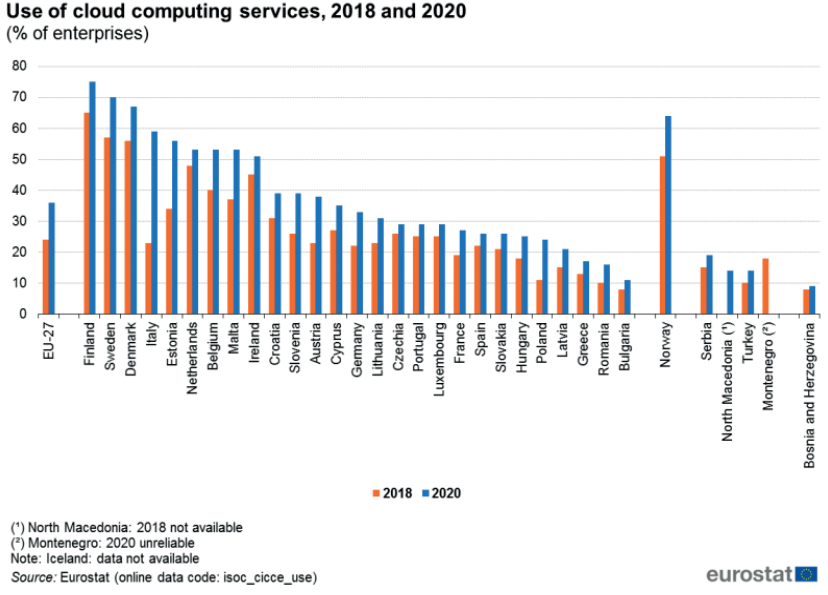
La pandémie a également favorisé la recrudescence de la cybercriminalité. Des tentatives d'hameçonnage routinières à la plus grande attaque DDoS jamais enregistrée, le contexte des cyber-menaces est en constante évolution et croissance. Depuis le début de l'année, les cyberattaques ont augmenté de 36% par rapport à 2020, avec 777 attaques hebdomadaires. Les attaques de type rançongiciel sont quant à elles en hausse de 93%[7].

7 *D'après Check Point Software Technologies*

II. L'utilisation du Cloud en France : un retard à rattraper

A. Pour les entreprises

L'utilisation du Cloud en France demeure sensiblement inférieure à celle que l'on constate dans d'autres économies avancées. Dans l'Union européenne à 27 (UE27), 36% des entreprises utilisaient le Cloud en 2020. Le taux d'utilisation est de 26% en Espagne, 27% en France, 33% en Allemagne, 59% en Italie, 70% en Suède et 75% en Finlande d'après Eurostat[8].



Parmi les 27% d'entreprises françaises qui utilisent le Cloud, les trois usages qui sont supérieurs aux moyennes européennes sont à 76% pour le stockage de dossiers (67% en UE27), à 63% pour stocker ses bases de données (47% en UE27) et à 36% pour des ap-

8 https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Enterprises.E2.80.99_dependence_on_Cloud_computing

plications de gestion de la relation client (CRM) (27% en UE27). Sur ces trois usages, les niveaux d'utilisation par les entreprises allemandes sont inférieurs à la moyenne européenne. En d'autres termes, les 27% d'entreprises françaises qui utilisent le Cloud l'utilisent davantage pour ces trois usages que les 33% d'entreprises allemandes. En termes de dépenses totales, le marché de Cloud computing en France représente environ la moitié de celui du Royaume-Uni. Par habitant, les dépenses totales en France représentent moins d'un quart du niveau de dépenses des États-Unis.

Mais la tendance s'accélère. Au cours des dix dernières années, les entreprises françaises ont accéléré leur migration vers le Cloud : Eurostat estime que la proportion d'entreprises françaises utilisant le Cloud a plus que doublé au cours des six dernières années, passant de 12% en 2015 à 27% en 2020. Le marché français du Cloud devrait croître de 15% par an au cours des prochaines années.

Le Cloud computing devrait avoir un impact plus significatif au cours de la prochaine décennie. La France doit se donner les moyens de rattraper ses pairs, et ce, pour plusieurs raisons :

-> La plupart des technologies, en particulier celles qui sont axées sur les entreprises, ont historiquement pris plusieurs décennies pour atteindre leur pleine maturité. Le Cloud a été lancé depuis quinze ans déjà.

-> Le Cloud computing constitue généralement une condition préalable essentielle pour l'essor d'autres technologies commerciales qui gagnent en importance, telles que les Big Data ou encore l'apprentissage automatique (machine learning).

-> L'expérience de nombreuses entreprises au cours de la crise sanitaire a démontré l'importance du Cloud informatique dans l'accroissement de la résilience et le soutien d'un mode de travail plus agile.

-> Même si les entreprises leaders ont adopté le Cloud en France, il reste encore une marge de manœuvre critique pour une adoption et une transformation numérique plus intensives au sein des

entreprises traditionnelles.

B. Pour le secteur public

Concernant le secteur public, l'adoption du Cloud computing en France a été perçue comme plus lente que dans d'autres pays, freinée notamment par une approche conservatrice en matière d'investissement. Des enquêtes menées auprès de personnalités du secteur ont révélé que le pays était en retard par rapport à l'Italie, l'Espagne, le Royaume-Uni et les pays nordiques[9]. Alors que les États-Unis ont annoncé la stratégie Cloud First en 2011 et le Royaume-Uni en 2013[10], la France n'a annoncé sa propre stratégie centralisée du Cloud qu'en 2018.

Cependant, depuis l'adoption de sa propre stratégie en matière de Cloud, le pays a commencé à rattraper son retard. Des évaluations indépendantes jugent généralement que la France dispose d'un gouvernement numérique moyen à fort : le pays se classe 11ème dans le Digital Government Index de l'OCDE[11] et 19ème dans l'enquête menée par l'ONU sur l'e-Government[12]. Le programme « Services Publics + » pour la numérisation des services publics lancé le 28 janvier 2021 semble porter ses fruits : 85% des démarches sont aujourd'hui disponibles en ligne et France Connect compte désormais plus de 27 millions d'utilisateurs (contre respectivement 63% et 500 000 utilisateurs en 2017), comme l'a rappelé la Ministre de la Tranformation et de la Fonction Publique, Amélie de Montchalin, en conseil des ministres le 25 août dernier.

---

9 https://www.computerweekly.com/news/4503004 88/French-public-sectors-never-ending-struggle-with-the-Cloud

10 https://policyexchange.org.uk/wp-content/uploads/2018/05/The-Smart-State-1.pdf

11 https://www.oecd.org/gov/digital-government-index-4de9f5bb-en.htm

12 https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

III. La stratégie Cloud de la France

Dans le cadre de l'ancienne stratégie Cloud «des trois cercles» lancée par Mounir Mahjoubi en 2018 lors de la Cloud Week, les organisations du secteur public pouvaient accéder à la puissance des services Cloud externes par l'intermédiaire du marché des services de Cloud computing de l'UGAP (Union des groupements d'achats publics), ouverts à tous les fournisseurs de services Cloud. Le marché de l'UGAP devait permettre aux services et organisations publiques de beaucoup plus facilement créer de nouveaux services via la meilleure infrastructure Cloud, ainsi que d'éliminer la plupart des freins à l'adoption du Cloud. Plus tard, le gouvernement avait annoncé un programme ambitieux « 400 jours pour accélérer la transformation numérique de l'État »[13], le 5 mars 2021.

La nouvelle stratégie Cloud pour l'État[14], présentée par Cédric O le 17 mai 2021, s'articule autour de trois enjeux :

Enjeux 1 - La transformation des entreprises et des administrations,

Enjeux 2 - La souveraineté numérique,

Enjeux 3 - La compétitivité économique.

Et repose sur trois piliers :

Pilier 1 - Le label « Cloud de confiance» qui devrait permettre aux entreprises françaises de bénéficier des meilleurs services Cloud grâce à un double niveau de sécurisation juridique et technique.

Pilier 2 - La politique « Cloud au centre » pour la transformation numérique de l'Etat

Pilier 3 - Une politique industrielle mise en œuvre dans le prolon-

13 https://www.transformation.gouv.fr/la-ministre/actualite/400-jours-pour-accelerer-la-transformation-numerique-de-letat

14 https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-Cloud/

gement de France Relance avec un soutien direct à des projets à forte valeur ajoutée dans le cadre du 4e Programme d'Investissements d'Avenir (PIA IV).

Si elle donne l'impulsion pour inciter la migration vers le Cloud, la politique « Cloud au centre » du gouvernement est insuffisante. Portée par une vision superficielle et artificielle de la souveraineté, cette politique prive les entreprises françaises du rendement des coûts offerts par les grands fournisseurs de Cloud.

Conclusion : l'heure du rattrapage a sonné

La valeur offerte par le Cloud pour la France est trop forte pour ne pas avancer plus vite, d'autant plus que l'Allemagne encourage les grands fournisseurs internationaux du Cloud à investir dans le pays. Car vouloir tout faire tout seul, avec dix ans de retard et dix fois moins de puissance que ce qui est déjà possible en s'appuyant sur des acteurs existants, serait prendre le risque de ne pas réussir à moderniser notre appareil de production. Les conséquences en seraient catastrophiques, tant pour la réindustrialisation indispensable du pays que pour la compétitivité dans le domaine digital et, plus largement, des services.

Plutôt que de priver les entreprises françaises du choix de certains fournisseurs de Cloud, l'État gagnerait à créer des conditions équitables et justes d'accès au marché, à l'image de l'initiative du Cigref et du CISPE qui ont lancé en avril 2021 « les dix principes d'une licence logicielle équitable pour les clients du Cloud » et proposent, dans le cadre des réglementations européennes en cours d'élaboration de définir des contrôleurs d'accès ou « gatekeepers» et de créer des obligations qui freinent les pratiques de licence déloyales[15].

Dans les économies avancées, il reste beaucoup à faire pour que

15 voir Chapitre 3 – Vers une concurrence libre et non faussée pour le Cloud computing, Aurélien Portuese

le Cloud soit une technologie pleinement mature, mais en France, l'adoption de cette technologie accuse un retard par rapport à ses pairs. Un rattrapage s'impose donc. L'utilisation du Cloud y est notamment limitée par la trop faible numérisation des TPE-PME. Les décideurs politiques et les entreprises doivent mettre en place les outils et les mécanismes nécessaires pour améliorer leur agilité et créer un contexte favorable à l'innovation pour accélérer la croissance en France.

L'État doit donc agir pour accélérer leur numérisation et leur utilisation du Cloud grâce, par exemple, à des aides ciblées. C'est plus que jamais le moment d'agir pour que ces entreprises résistent à la pression économique et gagnent en productivité.

Chapitre 2 - Hubert Védrine

Le Cloud au risque des paradoxes de la géopolitique : il ne faut pas oublier la nécessité du redressement économique !

Introduction

Technique en apparence, le Cloud computing est en réalité un enjeu géopolitique majeur qui mobilise les diplomaties des États-Unis, de l'Union européenne et de ses membres, ainsi que celle de la France en particulier. La donnée est en effet devenue un actif stratégique dont la maîtrise confère un atout certain dans la compétition mondiale. S'ajoute à cet enjeu celui des avantages que donne à une économie et à son appareil productif une puissance de calcul supérieure à celle des autres. Enfin, la question de la cybersécurité, et donc de la sécurité des données, est à l'évidence également critique. C'est pourquoi l'actualité des relations internationales concernant la donnée est dense.

Au niveau de l'Union européenne d'abord, au sein de laquelle différents textes sont en cours d'adoption sur ce sujet et dont la Cour de Justice de l'Union européenne a récemment invalidé le Privacy Shield - accord de transfert de données entre l'Union européenne et les États-Unis - par son arrêt Schrems II.

Au niveau transatlantique ensuite, avec les négociations en cours entre l'Union européenne et les Etats-Unis sur un accord de réciprocité à la suite de l'adoption par ces derniers en 2018 d'une loi sur l'accès des données y compris dans certains cas à l'étranger - le Clarifying Lawful Overseas Use of Data Act ou CLOUD Act qui, contrairement à ce que son acronyme semble indiquer, ne se réfère pas spécifiquement au Cloud computing - et la recherche d'un nouvel accord pour remplacer le Privacy Shield.

Au plan mondial enfin avec l'appel de certains États à la création d'une Organisation Mondiale de la Donnée. N'oublions pas la Chine dont la politique en la matière est, comme en d'autres, offensive, voire agressive.

Dans ce contexte, l'Europe, et la France pour son compte, cherchent à affirmer ou à récupérer leur souveraineté. Selon un vocable à la mode, elles mettent en avant l'importance de leur "autonomie stratégique", dans ce domaine comme dans d'autres. Au fondement de cette démarche se trouve l'idée que la domination du marché concerné par les acteurs américains constituerait un danger pour les entreprises du continent… et de l'Hexagone.

La souveraineté dans le Cloud computing est un enjeu important mais, comme sur d'autres terrains, il est souvent mal défini. Il faut en effet distinguer la capacité des Etats, ou de l'Union, à réguler le stockage, l'usage et le traitement des données, d'une part, et d'autre part l'autonomie stratégique dans la disponibilité des systèmes et le lieu de stockage des données. Ces questions sont essentielles et le cadre à définir important. Le risque ou le paradoxe serait que le futur cadre européen ou français, au lieu de contribuer à l'autonomie réelle de nos économies, freine l'adoption de ces nouvelles technologies et soit à ce titre finalement défavorable à la puissance de nos nations.

Les travaux de Christian Saint-Étienne, dont sa contribution dans la présente note tendent à démontrer que la France est en train d'accumuler un retard notable. Si, comme chacun s'accorde à le dire, le Cloud computing est à la mutation technologique encore en cours ce que l'électricité a été à la révolution industrielle, on voit combien ce retard risque d'être dommageable.

Parmi les fondements des politiques publiques françaises et européennes qui freinent l'adoption du Cloud par les acteurs économiques et les services publics se trouve la conviction que les acteurs européens eux-mêmes seraient en mesure de rattraper le

retard accumulé et d'offrir, à échéance raisonnable, des services comparables à ceux fournis par les grands acteurs américains du secteur.

Cet objectif industriel est lui-même mis à l'agenda sous l'effet de deux facteurs conjugués, quoique très différents. D'une part, des sociétés en France, en Allemagne et dans d'autres pays d'Europe, ont évidemment intérêt à faire de l'émergence d'acteurs européens une priorité politique. D'autre part, plusieurs changements juridiques récents, en Europe et aux Etats-Unis (le CLOUD Act et l'arrêt Schrems II, du nom de l'activiste de la vie privée et des libertés civiles autrichien Maximilien Schrems) ont conduit les autorités du vieux continent à durcir leurs positions sur ces sujets.

Aux dires de nombreux économistes et juristes reconnus dans ces matières, cependant, et notamment des deux autres contributeurs de cette note, ces deux facteurs, économiques et juridiques, ne justifient pas nécessairement la façon dont est conçue la régulation européenne.

Au plan économique, on peut se demander si l'émergence d'acteurs locaux du Cloud computing, service qui a vocation à certains égards à demeurer une commodité, est un objectif plus ou moins important que celui de la digitalisation de l'économie dans son ensemble.

Aux yeux des pouvoirs publics et des décideurs économiques allemands, par exemple, la capacité du secteur automobile à damer le pion à ses compétiteurs mondiaux grâce au digital, notamment en ce qui concerne la voiture autonome ou à l'hydrogène, est une priorité qui l'a emporté jusqu'ici sur le soutien aux acteurs locaux du Cloud. Pour une économie innovante, compétitive et, partant, puissante, l'accès au meilleur du digital est une condition sine qua non et le meilleur du digital aujourd'hui, c'est le Cloud, et le Cloud le plus puissant, c'est le Cloud américain. C'est bien ce que Peter Altmeier, le Ministre allemand de l'économie, a exprimé en voyant

dans l'ouverture de deux giga data centers de Google Cloud près de Francfort et de Berlin un "signe fort pour l'attractivité" de son pays.

Les prises de position et les initiatives des pouvoirs publics se multiplient aujourd'hui, au point qu'il risque de sembler impossible à brève échéance pour une entreprise française ou un service public de faire appel à un fournisseur de Cloud américain ou chinois. Loin de favoriser comme il est souhaité l'émergence d'acteurs technologiques européens, cette position pourrait conduire au contraire à faire paraître superflue la montée en capacité technologique de l'industrie, des services, des entreprises et du secteur public en France.

C'est un risque et ce serait d'autant plus regrettable que :

1. Des solutions technologiques et juridiques existent pour permettre aux entités françaises et européennes d'avoir recours aux services des opérateurs non-européens avec le meilleur niveau de sécurité, comme le permet par exemple la politique allemande en la matière.

2. Les menaces en matière de cybersécurité ne cessent d'augmenter, représentant un danger bien plus sérieux et rendant d'autant plus nécessaire le recours aux technologies les plus avancées.

Autrement dit, il est à la fois possible et indispensable de permettre aux organismes publics et privés français d'avoir accès au meilleur de la technologie, sans risquer de fuites de données. La souveraineté formelle est à l'évidence un enjeu essentiel, pour autant qu'elle n'obère pas la puissance réelle, or c'est ce qui risque de se passer. La régulation actuelle du Cloud en cours d'élaboration dans l'Union européenne freine considérablement le développement et l'adoption de cette technologie. La France aurait peut-être, au contraire, intérêt à porter une vision différente, plus réaliste, pour mieux articuler souveraineté, puissance et compéti-

tivité. C'est la thèse développée ici.

I. Les relations UE-Etats-Unis à l'épreuve de la réglementation du Cloud computing

A. Une réglementation européenne bouleversée

La réglementation européenne en matière de données personnelles a été considérablement bouleversée ces derniers mois suite, entre autres, à la décision d'invalidation du Privacy Shield par la Cour de Justice de l'Union européenne et aux positions prises à la suite de cette décision par le Comité européen de la protection des données (CEPD).

Le Privacy Shield garantissait la libre circulation des données entre l'Union européenne et les entreprises américaines ayant adhéré au Privacy Shield. Le 16 juillet 2020, la Cour de Justice de l'Union européenne a invalidé le Privacy Shield dans son arrêt « Schrems II », rendant impossible la poursuite des transferts de données personnelles de l'UE vers les Etats-Unis réalisés sur cette base.

À la suite de l'arrêt Schrems II, le CEPD a publié des recommandations afin d'aider les exportateurs de données européennes à évaluer le niveau de protection octroyé aux données personnelles par les pays hors UE, et à identifier le cas échéant les mesures supplémentaires appropriées. Mais ces recommandations sur les mesures qui peuvent compléter les outils de transfert proposés par le Règlement général sur la protection des données (RGPD), dont les « clauses contractuelles types » (CCT), pour assurer le respect du niveau de protection des données personnelles requis par le droit de l'UE ne sont pas toujours simples à mettre en œuvre.

B. Des a priori contestables sur le CLOUD Act

L'autre élément de complexité résulte du CLOUD Act adopté par les États Unis en 2018 et qui vise notamment les entreprises sous

contrôle américain opérant des services Cloud et hébergeant des données à ce titre. Le CLOUD Act rend possible l'accès des autorités américaines aux preuves électroniques détenues par ces entreprises dans les enquêtes pénales pour les crimes les plus graves, y compris lorsque les données se trouvent en dehors du territoire américain.

Or l'article 48 du RGPD prévoit qu'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant le transfert de données personnelles en dehors de l'UE ne peut être reconnue ou rendue exécutoire qu'à la condition qu'elle soit fondée sur un accord international en vigueur entre le pays tiers demandeur et l'UE ou un État membre, ce qui n'est pas le cas à ce jour du CLOUD Act.

L'a priori des acteurs européens du Cloud affirmant que le CLOUD Act permettrait à n'importe quel représentant des pouvoirs publics américains d'avoir accès à n'importe quelle donnée stockée par un opérateur américain, quelle que soit la localisation de stockage de ces données, y compris dans l'UE, est donc contestable.

D'une part, les dispositifs concernés ne sont applicables qu'en cas de suspicion de *serious crime*, autrement dit quand la criminalité, le blanchiment, les trafics ou le terrorisme sont en cause. Ce point est très important car il permet de souligner que le CLOUD Act ne vise que les situations les plus graves. D'autre part, la procédure nécessite un mandat délivré par un juge indépendant.

Du côté des sociétés concernées, en outre, les données sensibles sont la plupart du temps chiffrées, la clé de chiffrement étant stockée sur un serveur différent. Si elles devaient saisir des données sous couvert de lutte contre le crime, hypothèse d'école, les autorités judiciaires américaines se retrouveraient donc avec des données indéchiffrables.

C. La nécessité de trouver un nouvel accord-cadre entre l'Union européenne et les Etats-Unis

À ce jour, les discussions entre européens et américains n'ont pas permis d'aboutir à un nouvel accord-cadre pour remplacer le Privacy Shield et les transferts internationaux lorsqu'ils sont encore possibles sont désormais soumis à ces conditions plus contraignantes.

Un nouvel accord cadre permettrait probablement d'alléger ces contraintes, mais le chemin est encore long et ce malgré la réouverture du dialogue transatlantique sur le sujet depuis l'arrivée de l'administration Biden. Il existe de fortes divergences quant à la portée et à l'architecture d'un accord-cadre pour remplacer le Privacy Shield.

Par ailleurs, en ce qui concerne l'accord de réciprocité dans le cadre du CLOUD Act, le gouvernement américain est favorable à la conclusion d'un accord-cadre avec l'Union européenne, complété par des accords bilatéraux avec les États membres afin de satisfaire aux exigences du CLOUD Act. Alors que l'Union européenne souhaite parvenir à un accord global autonome à l'échelle de l'Union et s'oppose à des solutions qui pourraient entraîner une fragmentation et un traitement inégal entre les États membres.

II. Protectionnisme de fait et menaces sur la compétitivité

Il semble en fait que certains pays de l'Union européenne, dont la France en particulier, aient vu dans cette évolution du contexte règlementaire – exacerbé par le contexte anxiogène de la crise sanitaire – une opportunité pour pousser le développement de leurs propres acteurs du Cloud, influencés en cela par le lobbying très actif des acteurs nationaux. Pour protéger les intérêts de certains acteurs, loin de faire émerger des champions européens, on risque donc d'obérer la compétitivité des entreprises françaises et européennes. Ces risques contre-intuitifs sont amplement illustrés par

la contribution de Christian Saint-Etienne à cette note.

A. Les stratégies Cloud de la France

Bien qu'elle paraisse évidente, cette ambition politique de souveraineté numérique dans le Cloud s'est pour l'instant soldée par deux échecs complets – Numergy et Cloudwatt – par l'abandon d'une politique – les trois cercles du Cloud – et par une certification qui a du mal à s'imposer – SecNumCloud.

Comment expliquer cela ? Pour faire entrer la France dans l'économie du Cloud et concurrencer les américains, le gouvernement a soutenu le projet « Andromède » pour la création d'un Cloud souverain. Ce projet avait pour ambition de proposer une alternative pour les administrations et les entreprises françaises utilisant le Cloud américain, soumis au Patriot Act, loi de surveillance américaine. Mais il s'est pourtant soldé par deux échecs : Numergy puis Cloudwatt, tous deux créés en 2012, puis placés en procédure de sauvegarde quelques années à peine après leur création en raison de leur chiffre d'affaires respectif, très inférieur à ceux attendus, engloutissant au passage plusieurs dizaines de millions d'euros d'argent public et privé.

Tirant les leçons de cet échec, le gouvernement français a réajusté sa stratégie : au lieu de créer son propre Cloud souverain, il souhaite désormais réguler les acteurs du marché en découpant les offres de Cloud en trois cercles. Ainsi, le secrétaire d'Etat au numérique de l'époque, Mounir Mahjoubi présentait le 3 juillet 2018 la première stratégie de la France en matière de Cloud pour accompagner la transformation numérique de l'Etat. Cette première doctrine, cantonnée au secteur public et à l'administration, a défini les « trois cercles » du Cloud :

1. le Cloud interne pour les données sensibles hébergées « sur site » ;

2. le Cloud dédié pour les données sensibles hébergées dans le

Cloud public et supervisée par l'ANSSI (et conditionnée plus tard à l'obtention d'une certification : SecNumCloud) ;

3. le Cloud externe pour les données peu sensibles. Le troisième cercle a donné lieu à la création du marché public de l'UGAP pour les fournisseurs de services Cloud.

Mais la mise en place de cette stratégie n'a pas rencontré le succès escompté . Le marché public de l'UGAP n'a pour l'instant pas permis l'accélération de la transformation numérique de l'Etat et la certification SecNumCloud n'a été accordée qu'à trois offres de Cloud.

Le 17 mai 2021, le gouvernement a donc abandonné cette stratégie en trois cercles au profit d'une politique plus large, aux accents encore plus prononcés de souveraineté et de protectionnisme, englobant cette fois les acteurs privés. Sous couvert des leçons tirées de la crise sanitaire, le gouvernement a présenté une stratégie autour de trois axes :

1. le label « Cloud de confiance » pour se protéger contre les règlementations extraterritoriales, conditionné au visa de sécurité de la certification SecNumCloud ;

2. la politique du « Cloud au centre » pour moderniser l'action publique grâce aux technologies du Cloud ;

3. et le déploiement d'une politique industrielle soutenue par France Relance au service de la reconquête de la souveraineté française pour accompagner la construction de nouveaux services Cloud français.

Le tout s'appuyant, à l'échelle européenne, sur le projet Gaia X, lancé par la France et l'Allemagne en 2020 pour la création d'une offre de Cloud européenne et souveraine. Projet qui, si il s'accélère et devrait aboutir à une première architecture avant la fin de l'année 2021, illustre la divergence de vision entre les deux riverains du Rhin (ce n'est pas le seul domaine).

B. Différence d'approche entre l'Allemagne et la France

D'un côté la France prône un souverainisme qui ne souhaite pas que les entreprises américaines du Cloud apportent leur aide au projet (transfert de technologies, partage de savoir-faire, financement des start-ups, etc) ; de l'autre côté, l'Allemagne préconise une approche holistique tirant le meilleur de chaque acteur de l'industrie du Cloud.

Une divergence de vision que l'on retrouve sur le terrain de la régulation. Quand l'autorité allemande des systèmes d'information, le Bundesamt für Sicherheit in der Informationstechnik (BSI, homologue de l'ANSSI) a certifié près de 200 opérateurs en lien avec le Cloud computing via la certification allemande C5, en France, trois fournisseurs seulement sont qualifiés pour la certification délivrée par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), le SecNumCloud.

Quand l'ancien Ministre allemand de l'économie, Peter Altmaier, se félicitait, comme on l'a vu, de l'élargissement du site de stockage de données numériques de Google à Hanau et des ambitions du géant numérique dans la région de Francfort (1 milliard d'euros d'investissement d'ici 2030), le Ministre français de l'économie avait qualifié les GAFAM d'« adversaires » de la France.

La tendance à multiplier les obstacles à l'activité des opérateurs de Cloud non-européens en France est donc discutable, tant au plan du droit que de l'économie et même des intérêts français. Le débat « franco-français » autour du Cloud donne une vision biaisée de la souveraineté et peut orienter les entreprises vers une impasse. Si une compréhension maximaliste de la souveraineté se justifie pour les données sensibles du secteur public, aucun acteur du secteur privé, sauf rares exceptions, ne devrait être concerné.

Là encore, les positions françaises et allemandes divergent. Dans le cadre de l'élaboration du Data Governance Act de la Commis-

sion européenne, texte visant à créer un cadre législatif facilitant le partage des données – l'Allemagne, par pragmatisme, appelle à un niveau de protection proportionnel au niveau de sensibilité de la donnée, rappelant au passage que toutes les données ne sont pas sensibles, alors que la France souhaite que toutes les données personnelles soient caractérisées de « sensibles ».

C. Un protectionnisme au prix de la compétitivité

La ligne choisie par la France risque donc de se révéler contre-productive et pourrait avoir des incidences sur des secteurs clés. C'est le cas du secteur bancaire qui prend un retard considérable sur ses concurrents européens en matière digitale au moment du développement des fintech. De même, faire face au défi constitué par l'essor de ces mêmes GAFAM dans le e-commerce se révèlera impossible pour nos distributeurs tant qu'ils n'adopteront pas le meilleur du Cloud computing. En d'autres termes, un protectionnisme en faveur des acteurs locaux du Cloud peut s'avérer contre-productif, sauf s'ils étaient presque prêts à prendre la relève, et ne saurait tenir lieu de politique industrielle et encore moins digitale.

Dans l'état actuel des choses, si de fortes restrictions à l'activité des acteurs américains devaient être envisagées, elles handicaperaient 80% des entreprises du CAC 40 et au moins 75% des start-up, toutes clientes de fournisseurs américains. Sans parler du secteur des médias et du divertissement où la quasi-totalité des acteurs comme TF1, Canal+ , M6, le Figaro, les Echos et tant d'autres utilisent des fournisseurs de Cloud américains.

Il faut donc mieux concilier la souveraineté, objectif globalement incontestable avec sa déclinaison domaine par domaine, et la politique industrielle. L'objectif respectable d'une souveraineté numérique française ou européenne se heurte dans sa dimension industrielle à un constat dur à accepter : nous avons 10 ans et 100 milliards d'euros d'investissements de retard dans le Cloud com-

puting. Il faut évidemment tout faire pour rattraper ce retard… mais sans se couper du meilleur de la technologie et de l'innovation.

III. Deux menaces plus qu'émergentes

A. La montée en puissance de la Chine dans le domaine du Cloud

Quand l'Union européenne investit 2 milliards d'euros dans l'intelligence artificielle, les Etats-Unis en investissent 11 milliards… et la Chine 59 milliards. Cela se passe de commentaire.

En Chine, les dépenses en infrastructures et services Cloud ont atteint un niveau record de 4,3 milliards de dollars au deuxième semestre 2020. Elle détient sur ce plan la deuxième position sur le marché mondial et réalise 12,4% des investissements mondiaux dans le secteur du Cloud. Portés par ses géants du numériques, les BATX (Baidu, Alibaba, Tencent et Xiaomi), le secteur du Cloud computing chinois affiche un taux de croissance supérieur à 50% et bénéficie, à l'image des GAFAM aux Etats-Unis dans les années 2000, d'un soutien public massif : Pékin a annoncé investir 1,4 milliard de dollars dans les plateformes numériques d'ici 2022[1].

La Chine vient d'ailleurs d'adopter son propre RGPD. Cette loi – Personal Information Protection Law (PIPL)[2] - entrera en vigueur le 1er novembre 2021 et sera à portée extraterritoriale. Si elle offre des garanties comparables à celle du RGPD, elle spécifie explicitement que l'Etat chinois et les entreprises d'Etat sont exemptés de son application en ce qui les concerne. Autrement dit, les autorités pourront continuer à recueillir une grande quantité de données en soutien de leur politique industrielle...ou sécuritaire, y compris au plan politique. La PIPL offre également

1 *https://itsocial.fr/enjeux-it/enjeux-cloud-computing/cloud-public-prive-hybride/le-cloud-chinois-en-forte-croissance/*

2 *https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html*

au régime chinois de nouvelles armes légales pour imposer des restrictions aux entreprises technologiques locales.

Autrement dit, pour paraphraser François Mitterrand sur les euro-missiles, les activistes de la protection des données personnelles sont à l'Ouest… mais les menaces sont à l'Est. La Présidence Française de l'Union européenne, (PFUE) au premier semestre 2022, pourrait être l'occasion de parler d'égal à égal avec la nouvelle administration américaine et de trouver un accord pour faire rempart face à la Chine.

B. L'enjeu crucial de la cyber sécurité au niveau mondial

Outre la Chine, il est une autre menace qui pourrait handicaper davantage la France et l'Europe dans leur transition numérique : les cyberattaques.

Les menaces de cyberattaques sont de plus en plus nombreuses et sophistiquées et sont beaucoup plus destructrices quand elles attaquent des serveurs et services informatiques sur site. Le Cloud apparait donc comme l'ultime rempart contre cette menace, ou tout du moins, comme la solution la plus robuste face à celle-ci.

En effet, le Cloud s'est montré plus robuste face aux cybermenaces et ce pour plusieurs raisons. Tout d'abord, le Cloud permet d'automatiser et de réduire les risques grâce à des services intégrés. L'automatisation des tâches de sécurité permet de réduire la possibilité d'erreurs humaines de configuration, entre autres, et de bénéficier d'une infrastructure sécurisée. Les plus grands opérateurs de Cloud utilisent tous des techniques de prévention, de détection, de réponse et de correction des menaces et des attaques cyber.

En 2020, l'ANSSI et son homologue allemand, le BSI, alertaient le gouvernement et les entreprises sur l'augmentation des cyberattaques dont le nombre a été multiplié par 4 en un an seulement. En 2021 en France, c'est 9 entreprises sur 10 qui ont été touchées par des tentatives d'attaques ou des attaques, pour un coût moyen

de 1,3 million d'euros. Les principales victimes de ces attaques sont les PME et ETI, les collectivités locales et les hôpitaux. En 2020, 20% des victimes de rançongiciels portées à la connaissance de l'ANSSI étaient des collectivités locales[3] et on dénombre 192 attaques contre les hôpitaux, dont ceux de Villefranche-sur-Saône et d'Arles. Autrement dit, les entités qui disposent des moyens informatiques les plus limités et qui ne sont pas sur le Cloud. Guillaume Poupard, le directeur général de l'ANSSI l'a d'ailleurs réaffirmé lors des dernières assises de la sécurité informatique en octobre 2020 : « *Le Cloud répond à un vrai besoin en matière de sécurité informatique. On accompagne les entreprises qui veulent aller vers le Cloud, comme le sens de l'histoire les y encourage, notamment pour les PME et les petites structures qui ne deviendront jamais expertes en cybersécurité* ».

Et pour preuve, la cybersécurité s'est aujourd'hui imposée dans la stratégie globale des entreprises au sein des conseils d'administration et des conseils exécutifs, ou au sein des directions pour les entreprises de plus petite taille, ainsi qu'au sein de l'administration : le gouvernement a présenté le 18 février 2021 sa stratégie de cybersécurité[4].

Cette stratégie vise à renforcer le secteur de la cybersécurité en France en augmentant le chiffre d'affaires de la filière, en créant des emplois et en faisant émerger trois licornes françaises de la cybersécurité. Sans surprise, le premier parti pris de la stratégie est de développer des solutions souveraines et innovantes de cybersécurité.

Pourtant, qu'ils visent des Etats (comme l'Estonie attaquée par

3 https://www.ssi.gouv.fr/actualite/lanssi-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/

4 https://www.entreprises.gouv.fr/fr/strategies-d-acceleration/strategie-d-acceleration-cybersecurite#:~:text=Le%20Gouvernement%20a%20pour%20ambition,d'acc%C3%A9l%C3%A9ration%20%C2%AB%20Cybers%C3%A9curit%C3%A9%20%C2%BB.

la Russie en 2007), des collectivités locales ou des entreprises, les cybercriminels ne connaissent pas de frontière, ni de nationalité. On peut alors aisément imaginer le désastre si les entreprises et administrations françaises étaient privées des meilleurs services de Cloud, et donc des meilleurs services de sécurité.

Si la cybersécurité est indéniablement un enjeu majeur de notre époque, il ne doit pas être confondu avec des mesures globalement protectionnistes qui ne pourront que nuire aux objectifs poursuivis à savoir protéger les entreprises françaises et les administrations des cyberattaques.

À ce propos, on peut interpréter les politiques en matière de cybersécurité mises en place en France et proposées par différents acteurs, de deux façons :

1. La cybersécurité comme clé de voûte de la souveraineté numérique : à savoir que c'est en permettant aux entreprises de se doter des meilleurs services de sécurité, et donc de Cloud, que l'on permettra aux entreprises de garder le contrôle de leurs données et de ne pas être à la merci des cybercriminels.

2. La cybersécurité comme fer de lance de la souveraineté numérique : à savoir que la nationalité des fournisseurs de services primerait sur la qualité de service en raison des risques de perte de contrôle de données par les mesures extraterritoriales du CLOUD Act. Mais comme évoqué précédemment, ce risque est sans doute surestimé.

IV. Pour un « ordre mondial de la donnée » compatible avec les intérêts français et européens

Une position réaliste et d'équilibre en matière de données au niveau mondial devrait donc se fixer quatre objectifs :

Objectif 1 - Permettre la liberté de circulation des données : c'est d'ailleurs un objectif du RGPD décrit dans son intitulé même : « Règlement relatif à la protection des personnes physiques à l'égard

du traitement des données à caractère personnel et à la libre circulation de ces données ».

Objectif 2 - Permettre aux entreprises françaises et européennes d'avoir accès aux meilleures technologies disponibles.

Objectif 3 - Protéger les citoyens des entreprises et activités criminelles.

Objectif 4 - Protéger les données des entreprises pour des raisons économiques et celles des citoyens au nom des libertés et du respect de la vie privée.

La politique du gouvernement français et, dans une moindre mesure, celle des institutions européennes, semblent presque uniquement inspirées par le quatrième de ces objectifs, au détriment possible de l'innovation, de la puissance économique du continent et même de la protection contre le crime.

Afin d'inverser cette tendance, nous formulons trois recommandations pour le Gouvernement français et la Commission Européenne. L'objectif doit être de passer de mesures unilatérales - et à ce stade non-réciproques – à une gestion multilatérale de ces enjeux.

A. Accélérer la conclusion des négociations transatlantiques

L'ambition devrait être de travailler de concert avec nos partenaires à l'élaboration d'un corpus réglementaire pour l'économie numérique. Nous avons l'opportunité de mettre au point un programme technologique conjoint UE - États-Unis. Un consensus se dessine, des deux côtés de l'Atlantique. L'administration Biden sera en capacité d'apporter des garanties supplémentaires et il y a de fortes chances pour qu'elle manifeste très prochainement une meilleure prise en compte de la vision européenne sur la protection des données, comme l'imagine Wojciech Wiewiórowski, Contrôleur européen de la protection des données.

Un alignement des États-Unis sur les normes RGPD ou, a minima, la conclusion d'un accord-cadre pour remplacer le Privacy Shield serait très propice pour atteindre les objectifs numériques de l'Union européenne : conjuguer l'influence normative indéniable et utile de l'Union à la préservation de nos capacités d'innovation et à d'investissement.

Enfin, la signature d'un accord de réciprocité entre l'UE et les États-Unis dans le cadre du CLOUD Act, permettrait de compléter les bases d'un cadre juridique apaisé et favorable à l'utilisation des services des fournisseurs de Cloud américains dans l'UE.

B. Impliquer Interpol pour ce qui est de la cybercriminalité

Les dispositifs qui posent problème dans le CLOUD Act, à savoir le transfert de données aux autorités américaines, ne sont applicables qu'en cas de suspicion de « *serious crime* », autrement dit quand la criminalité, le blanchiment, les trafics ou le terrorisme sont en cause.

Ce point est très important car il permet de souligner que le CLOUD Act n'est que l'actualisation des traités multilatéraux d'assistance juridique afin de les adapter à l'instantanéité et à la dématérialisation à l'heure digitale.

Ces enjeux sont d'ores et déjà traités multilatéralement à travers Interpol qui est compétente pour demander, voire exiger, des informations à tous les services de polices et de renseignements afin d'interpeller les criminels faisant l'objet d'un mandat d'arrêt international.

À ce titre, Interpol serait donc légitime pour être l'autorité compétente pour demander le transfert des données, aux entreprises ou aux administrations concernées, en cas de *serious crime*. Autrement dit, si le crime est suffisamment grave pour nécessiter le

transfert de données à une autorité judiciaire, alors Interpol serait l'autorité la plus à-même de gérer cette compétence.

Pour cela, les mesures extraterritoriales doivent devenir réciproques, voire universelles, et être supervisées par une instance internationale.

C. Continuer à coopérer au sein de l'OTAN sur les cyber menaces terroristes

Reconnu depuis 2016 comme milieu d'opérations de l'OTAN[5], le cyberespace est l'un des domaines de coopération possible entre l'Alliance et l'Union européenne. La lutte contre les menaces hybrides fait l'objet d'une certaine coordination entre les deux organisations, même si leurs responsabilités ne sont pas du tout du même ordre. L'OTAN s'est dotée d'un plan d'action de cyberdéfense et soutient notamment que le droit international s'applique au cyberespace. Elle souhaite pour cela pouvoir coopérer avec les industries. Ce plan d'action s'applique aujourd'hui aux trois tâches fondamentales de l'OTAN : la défense collective, la gestion de crise et la sécurité coopérative. Evidemment, les intérêts de l'industrie européenne doivent aussi être pris en compte. Il ne s'agit pas de donner un rôle accru à la bureaucratie de l'OTAN, mais de coopérer au sein de cette organisation.

Si les États-Unis et l'Union européenne parviennent à coopérer dans le cyberespace au sein de l'OTAN, ils le peuvent certainement à l'extérieur, à condition que les bases de cette coopération soient claires.

Certains membres de l'Alliance se sont d'ores-et-déjà saisis du sujet en signant le 22 octobre dernier un traité pour créer un fonds d'investissement d'un milliard d'euros pour l'innovation dans la cyberdéfense[6]. A ce jour, ni la France ni les Etats-Unis n'ont exprimé leur intention de prendre part à cette initiative.

5 *https://www.nato.int/cps/fr/natohq/topics_78170.htm*

6 *https://www.nato.int/cps/fr/natohq/news_187607.htm*

Conclusion : Saisir l'opportunité de la PFUE pour réorienter l'attention vers l'Est

La France semble avoir le choix entre deux lignes :

1. Tenter d'imposer une position protectionniste sur la souveraineté numérique, au risque d'affaiblir son appareil productif ;

2. Viser à surmonter les contradictions qui ont été discutées en demandant officiellement aux Etats-Unis de s'aligner sur la norme RGPD et de réformer leur législation sur la surveillance.

La nuance et la proportion sont encore une fois de rigueur. Pour reprendre la conclusion du rapport d'Agora Fic[7] « Faire de la Cybersécurité la clé de voûte de la souveraineté numérique européenne » : « *si la puissance ne peut pas être uniquement numérique, il ne peut y avoir de puissance sans numérique* ».

La PFUE sera un bref moment, un trimestre en réalité. L'action devra être poursuivie au-delà pendant toute la durée de la Commission Von der Leyen, jusqu'en 2024.

Enfin, l'impact du Cloud sur la consommation d'énergie et donc sur le climat, et autres indicateurs écologiques, devrait être systématiquement pris en compte.

---

7 https://uploads-ssl.webflow.com/594919aebod3dboe7a726347/6138d69a7ecd-491da9389d4d_WP_FR.pdf

Chapitre 3 - Aurélien Portuese

Pour une concurrence libre et non faussée pour le Cloud computing

Introduction

Le retard de la France en ce qui concerne l'adoption du Cloud, pour faire référence à la contribution de Christian Saint-Etienne dans le présent cahier, prive beaucoup d'entreprises françaises du meilleur de la digitalisation et les handicape dans la compétition mondiale. Certes, les pouvoirs publics ont pour objectif d'accélérer l'adoption du Cloud, l'actualité la plus récente en la matière étant l'annonce de la politique dite "Cloud au centre". Le second chapitre de cette publication a montré comment une compréhension erronée de la souveraineté risquait au contraire d'aggraver le retard français dans le Cloud. Les pages qui suivent visent quant à elles à analyser l'impact du droit de la concurrence et des comportements des différents acteurs sur ce même enjeu crucial qu'est le recours au Cloud computing par les entreprises et d'envisager les pistes de réforme sur ce plan, au niveau national comme européen.

Selon des publications récentes du Club Informatique des Grandes Entreprises Françaises (« Cigref ») et le Cloud Infrastructure Services Providers in Europe (« CISPE »)[1], il se pourrait en effet que les fournisseurs de produits adjacents aux services de Cloud computing, y compris les fournisseurs de logiciels offrant également lesdits services, tirent parti de leur position forte, parfois dominante, dans les logiciels afin de fausser la concurrence dans le domaine du Cloud. Cela serait évidemment préjudiciable aux utilisateurs, qui verraient alors leur choix réduit dans ce domaine critique.

1 *https://www.fairsoftware.Cloud/fr/communiques-de-presse/*

En tant que telle, la position forte ou dominante de certains acteurs du logiciel ou d'autres services disposant également d'une offre de Cloud computing peut soulever des problèmes de restrictions verticales d'accès au marché. Ce serait encore plus le cas si ces fournisseurs de logiciels cherchaient effectivement à limiter la concurrence au détriment des utilisateurs du Cloud. Le Cigref et le CISPE ont procédé à un examen détaillé des pratiques commerciales déployées par les fournisseurs de logiciels offrant également des services de Cloud computing et ont souhaité attirer l'attention des pouvoirs publics et de l'ensemble de leur écosystème sur cette situation.

Avec une meilleure compréhension de la souveraineté, c'est l'autre véritable enjeu du secteur : assurer une compétition juste et équitable entre les acteurs pour une meilleure compétitivité.

Un enjeu d'autant plus crucial que le Cloud n'est plus une option, c'est devenu un impératif pour toutes les organisations. Il est très important de réaliser que le Cloud computing n'est pas d'abord une solution de stockage d'information. L'appellation courante de ''data center" est à cet égard trompeuse. Elle pourrait donner à penser que le rôle premier du Cloud computing est de permettre aux entreprises et autres organisations de stocker leurs données ailleurs que dans leurs propres équipements dans leurs locaux.

Une partie de l'histoire du Cloud computing a commencé ainsi et certains acteurs domestiques, encore de taille moyenne, proposent des services parfois presque limités au seul stockage virtuel. Outre le fait que certaines pratiques essentielles en matière de redondance ou de sauvegarde sont parfois insuffisantes chez lesdits acteurs (comme un récent sinistre chez l'un d'entre eux l'a malheureusement illustré), c'est là une vision totalement datée et limitée du Cloud computing.

L'inventeur du Cloud computing a en effet conçu celui-ci d'abord comme un ensemble de services innovants dans tous les domaines. Aujourd'hui, qu'il s'agisse de l'intelligence artificielle, du e-commerce, de la réalité virtuelle, de la cybersécurité ou de l'internet des objets, bref de toutes les technologies digitales les plus avancées, l'apport du Cloud est irremplaçable, bien au-delà de la conservation et de la mise à disposition virtuelle des données. Le Cloud, c'est une capacité infinie de calcul et de traitement des données, et selon un modèle de *pay as you go*, ce qui n'est pas moins important. Avec le Cloud, toute organisation, même la plus petite, a authentiquement accès au meilleur du digital, aux solutions les plus innovantes, sans investissement lourd. Notons-le au passage : à ce titre, le Cloud computing contribue à faire disparaître de nombreuses barrières à l'entrée et constitue un puissant accélérateur de compétition vertueuse et de juste concurrence.

C'est précisément pourquoi il serait catastrophique que le potentiel d'innovation du Cloud soit rendu moins accessible par des pratiques commerciales et des approches réglementaires inhibant son adoption.

Défini par la législation européenne comme « service d'informatique en nuage » à savoir « service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées »[1] , le Cloud computing offre de nombreuses opportunités pour autant que l'innovation offerte par cette technologie soit au service d'une concurrence libre et non faussée.

L'objet de la présente étude est donc, d'une part, de montrer en quoi la concurrence peut être accrue pour les utilisateurs du Cloud computing en évitant certaines pratiques contestables, au bénéfice des utilisateurs (I) et, d'autre part, la nécessité pour les régulateurs

1 Article 4, point 19 de la Directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32016L1148

d'adopter une approche moins étroite et plus dynamique dans le domaine (II).

I. Favoriser la concurrence en minimisant les pratiques nocives

Comme Christian Saint-Etienne l'a rappelé, la technologie Cloud est insuffisamment utilisée en France en comparaison avec d'autres pays. Par exemple, en 2020 seules 27% des entreprises françaises utilisent le Cloud, contre 70% en Suède[2]. Aussi, les entreprises américaines dépensent quatre fois plus que les entreprises françaises dans la technologie du Cloud[3]. Le retard technologique est patent et le rattrapage est impératif car l'innovation digitale représente un réel levier de croissance économique dont la France ne saurait se passer.

Néanmoins, au-delà des différences de taux de pénétration de la technologie Cloud entre pays, l'adoption de cette technologie se voit trop souvent limitée par des pratiques anticoncurrentielles des éditeurs de logiciels, de bureautique notamment.

Les éditeurs de logiciels conçoivent, développent et commercialisent des logiciels et sont des intermédiaires incontournables et déterminants entre les fournisseurs d'infrastructure Cloud et le client final. En effet, certains acteurs qui détiennent les plus grandes parts de marchés des solutions logicielles sont également des fournisseurs de services de Cloud computing.

Certains d'entre eux recourent à des clauses contractuelles, conditionnant le prix d'achat qui peuvent s'apparenter à des pratiques commerciales déloyales entre entreprises au sens des articles L.442-1 à L.442-11 du code de commerce[4]. Ces articles interdisent les pratiques restrictives de concurrence telles que le dé-

2 *« Voir Chapitre 1 – Le Cloud en France et en Europe : un retard à rattraper et des opportunités de croissance à saisir, Christian Saint-Etienne*

3 *Christian Saint-Etienne, op.cit*

4 *https://www.fairsoftware.Cloud/about/*

séquilibre significatif dans les droits et obligations des parties, ou encore le fait de rompre une relation commerciale établie en l'absence d'un préavis écrit suffisant.

Or, la présence de clauses contractuelles pouvant restreindre la concurrence entre éditeurs de logiciels et procurer un déséquilibre significatif entre éditeurs de logiciels et clients finaux est de nature à constituer un obstacle dirimant à l'adoption rapide et généralisée de la technologie Cloud. Autrement dit, la réalité d'une concurrence libre et non faussée permettant la diffusion de la technologie Cloud est inversement proportionnée à la limitation des clauses potentiellement restrictives de concurrence imposées par les éditeurs de logiciels.

La régulation doit néanmoins être agile et souple : une rigidité excessive de la régulation inhiberait une technologie naissante et contraindrait excessivement des acteurs en quête de relations commerciales justes et équitables. Ainsi, le marché doit parvenir à réaliser cet équilibre nécessaire entre, d'une part, la juste rémunération des éditeurs de logiciels, et d'autre part, la concurrence libre entre éditeurs de logiciels pour les utilisateurs finaux de la technologie Cloud.

Cette démarche volontaire et coconstruite est portée par le Cigref et le CISPE[5]. Auteurs d'une charte comprenant 10 principes fondamentaux pour des conditions équitables d'octroi de licences de logiciels aux entreprises utilisant la technologie Cloud, le Cigref et le CISPE ont élaboré des principes qui permettraient de réduire les pratiques potentiellement restrictives de concurrence.

A. Les 10 principes pour réduire les pratiques anticoncurrentielles de licences de logiciels et de Cloud

Ces principes reposent sur quatre grands enjeux qui seront décisifs pour la diffusion et l'adoption de la technologie Cloud par les

5 *https://www.fairsoftware.Cloud/fr/communiques-de-presse/*

entreprises françaises et européennes. Ces enjeux sont : l'optimisation des coûts, la transparence, l'interopérabilité, et la bienveillance. Ces quatre enjeux se déclinent en dix principes :

1. Conditions claires et intelligibles : les clauses contractuelles proposées aux entreprises clientes doivent être aussi claires que possible afin d'éviter de dissuader les entreprises d'adopter la technologie Cloud en raison d'incompréhensions, de risques juridiques excessifs et de la peur d'être soumis à des clauses contractuelles dont elles n'auraient pas préalablement eu connaissance. Ce principe fondamental s'inspire de l'article L.211-1 du code de la consommation qui stipule que « *les clauses des contrats proposés par les professionnels aux consommateurs doivent être présentées et rédigées de façon claire et compréhensible. Elles s'interprètent en cas de doute dans le sens le plus favorable au consommateur* ». En l'espèce, les entreprises clientes sont consommatrices des logiciels proposés sur le Cloud et sont donc légitimes de se voir proposer, surtout dans les contrats d'adhésion, des clauses contractuelles claires et intelligibles. À défaut, la réticence des entreprises françaises et européennes à migrer vers la technologie Cloud ne sera que plus grande.

2. Portabilité des logiciels préalablement acquis : la migration vers la technologie Cloud suppose aussi d'encourager l'utilisation de logiciels acquis préalablement à l'utilisation du Cloud. En l'absence d'une telle portabilité, les entreprises clientes doivent acheter de nouveaux logiciels ou *add-ons* coûteux sans réel lien avec le service offert. Ces coûts superficiellement imposés sont assimilables à la pratique restrictive de concurrence identifiée au 1° de l'article L.442-1 du code de commerce, à savoir « d'obtenir ou de tenter d'obtenir de l'autre partie un avantage ne correspondant à aucune contrepartie ou manifestement disproportionné au regard de la valeur de la contrepartie consentie ». Par conséquent, afin de minimiser le risque d'un avantage obtenu de façon manifestement disproportionnée, les éditeurs de logiciels devraient encourager la portabilité de logiciels préalablement acquis sans coût additionnel, ou à tout le

moins, avec un coût raisonnable et justifiable.

3. Libre utilisation des logiciels : les éditeurs de logiciels doivent garantir l'utilisation libre et sans restriction sur le Cloud de logiciels fonctionnant sur site. À défaut de cette liberté d'utilisation, les entreprises clientes continueront de se voir imposer de nombreuses restrictions quant à leur capacité à utiliser tout le potentiel offert par la technologie Cloud puisque les éditeurs de logiciels continueront de restreindre indûment l'accessibilité de la technologie Cloud pour les logiciels fonctionnant sur site.

4. Libre optimisation des coûts par le matériel informatique : la tendance des éditeurs de logiciels à favoriser tel matériel informatique plutôt qu'un autre pour l'utilisation de la technologie Cloud engendre des surcoûts pour les entreprises qui se trouvent face à l'alternative regrettable suivante : changer de matériel informatique ou utiliser les logiciels avec des fonctionnalités restreintes. Les éditeurs de logiciels doivent s'engager à minimiser autant que faire se peut la réduction des fonctionnalités offertes par leurs logiciels en raison du matériel informatique utilisé par l'entreprise cliente. Ces pratiques restrictives de concurrence peuvent être assimilée à des ventes liées (« tie-ins ») contestables et peu justifiables.

5. Interdiction de représailles pour le choix du Cloud : la concurrence au sein des fournisseurs de la technologie Cloud est non seulement souhaitable, mais elle est impérative si d'aucuns souhaitent que cette technologie bénéficie au plus grand nombre. Or, la capacité de certains éditeurs de logiciels de favoriser leurs propres technologie Cloud en pénalisant les clients qui utiliseraient un fournisseur concurrent entrave le processus d'une concurrence libre et non faussée.

6. Favoriser l'interopérabilité : les éditeurs de logiciels doivent encourager l'interopérabilité par des standard ouverts afin de réduire les risques de verrouillage de leurs clients dans un éco-

système. En effet, la synchronisation et la compatibilité entre protocoles permettraient aux clients de migrer plus facilement entre les solutions Cloud, générant ainsi une concurrence accrue au sein et entre les écosystèmes du Cloud.

7. Favoriser des conditions tarifaires justes et transparentes : les conditions tarifaires offertes par les éditeurs de logiciels peuvent varier selon les clients mais devraient répondre à une ligne tarifaire transparente applicable à tous les clients et modulables selon les services personnalisés offerts aux clients. Des conditions tarifaires justes et équitables seront atteintes dès lors que celles-ci seront transparentes. À défaut, le risque de conditions tarifaires discriminatoires et appliquées arbitrairement dissuadera les entreprises à adopter pleinement la technologie Cloud.

8. Garantir l'utilisation sereine des logiciels : les entreprises clientes doivent bénéficier d'une relative sécurité quant aux fonctionnalités offertes par les logiciels qu'elles utilisent. La modification brutale, non-prévisible et injustifiée desdites fonctionnalités est de nature à créer un dommage certain et immédiat pour les entreprises clientes, réduisant ainsi l'attractivité et la prévisibilité de l'utilisation de la technologie Cloud. Or, de tels changements imprévisibles et brutaux sont de nature à être qualifiés au sens de l'article L.442-1. II du code de commerce qui sanctionne la rupture brutale, « même partiellement », d'une relation commerciale établie.

9. Répondre aux attentes légitimes des clients : lorsque les entreprises clientes utilisent les logiciels, elles sont en droit d'attendre une utilisation normale de ces logiciels, c'est-à-dire une utilisation qui correspond aux attentes légitimes des services offerts par ce logiciel. Aussi, les entreprises clientes devraient pouvoir avoir recours à un service client leur permettant d'assurer la plus grande compatibilité de leurs logiciels avec toute technologie Cloud. L'absence de tels services est de nature à dissuader l'utilisation de la technologie Cloud et de verrouiller les entre-

prises dans un seul écosystème.

10. Autoriser la revente raisonnable de licences de logiciels : dès lors qu'il est légalement possible pour les entreprises clientes de revendre des licences de logiciels, les éditeurs devraient accompagner leurs clients dans cette revente avec une assistance qui pourra s'apparenter à un service marchand.

Ces principes participent au renforcement de la concurrence et ainsi l'adoption des innovations offertes par le Cloud en restaurant une relation plus équilibrée entre les éditeurs de logiciels et les entreprises clientes. L'adoption de ces principes renforcerait la relation de confiance entre éditeurs et clients.

En effet, la capacité accrue des entreprises clientes de changer d'éditeurs de logiciels et de Cloud sans représaille sera de nature à accroître la concurrence qui, à son tour, débouchera sur une innovation accrue concernant les services offerts et sur une baisse des tarifs proposés.

B. Application et conséquences de ces principes sur le marché du Cloud et des logiciels

Ces principes reposent sur une démarche volontaire et constituent un guide de bonne conduite qui pourrait déboucher sur un label. L'éditeur de logiciel s'engageant à respecter ces principes pourrait se voir attribuer un label européen voire international afin d'informer les entreprises clientes de la volonté de cet éditeur d'éviter de tirer indûment partie d'une relation commerciale déséquilibrée.

Plutôt que des labels nationaux reposant sur une vision surannée de la souveraineté (numérique) et sur des démarches tendant à un protectionnisme digital dommageable pour tous[6], comme l'a évoqué Hubert Védrine dans la seconde partie de ce cahier, un label international fondé sur les 10 principes du Cigref et du CISPE

6 Voir ci-dessous, 2.

encouragerait la diffusion de bonnes pratiques et informerait de façon opportune les entreprises clientes des éditeurs engagés dans une démarche de concurrence libre et non faussée au sein de marché de la technologie du Cloud. Démarche positive et gratifiante plutôt que négative et répressive, l'idée d'un label consacrant ces 10 principes aboutirait sans nul doute à un accroissement à la fois de la concurrence et de l'innovation digitale par le sain développement d'un écosystème Cloud en Europe.

Cependant, un label issu de ces 10 principes ne saurait être suffisant pour garantir et consolider la concurrence libre et non faussée dans la technologie Cloud. Il est possible de compléter cette démarche par une prise en compte de ces considérations à la fois par la régulation européenne du Digital Markets Act (DMA) ainsi que par la mise en place de règles de bonnes conduites par le International Competition Network (« ICN »).

II. Favoriser la concurrence en optimisant la régulation

Les principes édités par le Cigref et l'association CISPE, en tant que principes de bonnes pratiques, pourraient être prolongés dans un cadre européen et international. Cela permettrait de renforcer le niveau de concurrence au sein de la technologie Cloud, notamment au sein du DMA.

Le DMA est une proposition de règlement de la Commission européenne visant à instaurer un nouveau modèle de régulation du comportement concurrentiel des grandes plateformes numériques sur le marché unique européen. L'adoption de ce texte pourrait aboutir sous la PFUE et vise à prendre en compte les spécificités de l'économie numérique : le texte cible les entreprises considérées comme « gatekeepers », c'est-à-dire en capacité de contrôler l'accès au marché et prévoit l'imposition de restrictions nouvelles à ces derniers.

Tout d'abord, bien que nécessitant certains ajustements dévelop-

pés plus loin[7], le DMA pourrait être modifié lors du processus législatif actuel afin de permettre une meilleure prise en compte des préoccupations de concurrence susmentionnées (A). Ensuite, des lignes directrices internationales s'inspirant du Cigref et du CISPE pourraient permettre l'adoption globale de ces principes (B).

Avant d'aborder ces deux prolongements nécessaires, il convient de préciser que les stratégies nationales du Cloud visant à accélérer son adoption – et, de préférence, de solutions européennes – profiteraient, dans leur mise en œuvre et dans l'atteinte de leurs objectifs, d'une concurrence juste et équitable entre tous les acteurs du Cloud computing, quelle que soit leur nationalité. En effet, inclure dans l'encouragement à la migration vers la technologie Cloud des préoccupations telles que la nationalité de l'actionnariat comme le ferait le label français « Cloud de confiance » revient à freiner l'adoption par les entreprises françaises des meilleures performances de la technologie Cloud, indépendamment de considérations nationales ou européennes[8], au détriment des enjeux de cybersécurité.

Ce label laisse penser que le Cloud avec un actionnariat non-européen serait de moindre confiance, alors que les performances technologiques devraient également être prises en compte dans l'analyse de ce niveau de confiance. Cette voie prise par le gouvernement français n'est malheureusement pas de nature à rattraper le retard mais plutôt à accroître la méfiance des entreprises françaises envers les leaders mondiaux de la technologie Cloud à un moment pourtant crucial dans la concurrence internationale pour l'innovation digitale.

---

7 https://itif.org/publications/2021/05/24/digital-markets-act-european-precautionary-antitrust; http://www.epicenternetwork.eu/wp-content/uploads/2021/06/Digital-Markets-Act-precaution-over-innovation-final.pdf; https://itif.org/events/2021/05/25/digital-markets-act-europe-precaution-or-innovation ; https://itif.org/publications/2021/06/10/eu-must-make-digital-peace-not-war-united-states

8 https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-Cloud.pdf

Plutôt que d'adopter de tels réflexes protectionnistes voire nationalistes, une action visant à projeter les principes du Cigref et du CISPE, positifs et incitatifs, vers des forums transnationaux générera davantage d'effets positifs.

A. Réformer le DMA et y intégrer les éditeurs de logiciels

Le règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique, le DMA, est de nature à réduire la concurrence, limiter plutôt qu'encourager l'innovation, et ne répond pas aux défis quant à la compétitivité numérique de l'Europe[9]. Le DMA représente la préférence de la précaution sur l'innovation en cela que la régulation interviendra dès lors que des innovations disruptives bousculeront le statu quo[10].

Par exemple, l'introduction d'un nouveau produit ou service par les grandes plateformes pourra être bloqué ou sanctionné dès lors que ce produit ou service entre en concurrence avec ceux déjà proposés par des entreprises. Ainsi, si Google introduit une application gratuite pour les consommateurs, l'entreprise qui vendait une application comparable pourra invoquer une concurrence déloyale de la part de Google et faire retirer, ou à tout le moins faire promouvoir sans frais, sa propre application dans les smartphones de Google. Soit l'application proposée par Google est découragée et alors l'innovation s'en trouve réduite, soit le consommateur paye une application qu'il pourrait avoir gratuitement et le bien-être du consommateur se réduit d'autant au nom d'une concurrence équitable.

Aussi, si Apple veut promouvoir ses Airtags pour que les consommateurs localisent facilement leurs smartphones, les producteurs

9 *https://itif.org/publications/2021/05/24/digital-markets-act-european-precautionary-antitrust*

10 *http://www.epicenternetwork.eu/wp-content/uploads/2021/06/Digital-Markets-Act-precaution-over-innovation-final.pdf*

de produits similaires pourront considérer qu'Apple a non seulement copié mais également discrimine leurs produits de façon anti-compétitive. Afin d'éviter de telles critiques qui seront demain des sanctions réglementaires, les entreprises pouvant innover s'auto-limiteront en faveur d'une approche plus précautionneuse telle qu'instillée par le DMA. En cela, le projet de texte doit être profondément retravaillé, notamment en ce qui concerne la désignation excessivement étroite et arbitraire des contrôleurs d'accès (ou « *gatekeepers* »).

Or, les principes édictés par le Cigref et le CISPE illustrent l'étroitesse et le caractère inopportun de la désignation des contrôleurs d'accès tels que proposée par le DMA. En effet, si le DMA comprend dans son champ d'application les « services d'informatique en nuage » (Cloud)[11], il définit les contrôleurs d'accès de façon si étroite que certains éditeurs de logiciels ne sont pas inclus dans la définition.

Afin d'éviter les effets de seuils générés par les critères quantitatifs dans la désignation des contrôleurs d'accès par le DMA, et afin d'éviter l'exclusion injuste de certains acteurs ayant les caractéristiques de contrôleurs d'accès mais exempts des obligations du DMA, il conviendrait d'amender le projet de texte afin d'intégrer certains éditeurs de logiciels dans la définition des contrôleurs d'accès. Une désignation plus large de la notion de contrôleur d'accès non seulement permettrait de façon spécifique à ce que l'esprit des principes Cigref et des travaux du CISPE soient intégrés dans le DMA, mais permettrait également de façon plus générale d'accroître la juste concurrence en minimisant les effets de seuils indésirables où certaines entreprises sont sujettes à des obligations règlementaires importantes tandis que leurs rivales sont exemptes de ces mêmes obligations.

En cela, les éditeurs de logiciels doivent entrer dans le champ d'application du DMA établi à l'article 2.2 du projet de texte. Aussi,

11 Article 2.2) g) du Digital Markets Act.

les critères quantitatifs de l'article 3.2 du DMA sont inappropriés et devraient être abandonnés au profit, si la désignation doit être adoptée, exclusivement de critères qualitatifs de son article 3.1. La concurrence libre et non faussée commence aussi par un environnement règlementaire commun entre entreprises rivales.

B. Établir des lignes directrices internationales via l'ICN

Afin de renforcer l'impact des principes élaborés par Cigref et le CISPE, et parce que ces principes contribuent à un renforcement de la concurrence au sein de la technologie du Cloud, le forum international chargé d'édicter les bonnes pratiques en matière de concurrence – à savoir l'International Competition Network (ICN) – devrait être sensibilisé aux problèmes de concurrence identifiés par ces principes. Ainsi, l'action des autorités nationales de concurrence sera de nature à saisir l'ICN afin d'édicter des principes internationaux reconnus de tous.

À l'instar des principes directeurs concernant les études de marché[12], ou à l'instar de bonnes pratiques suggérées dans le secteur des télécommunications[13], il serait pertinent que les autorités nationales de concurrence défendent l'idée de porter ces principes au niveau international par l'adoption de principes par l'ICN. Les tribunaux et le marché seront dès lors plus à même de réagir dans un sens qui renforce la concurrence libre et non faussée au sein de la technologie du Cloud.

Conclusion : Concilier innovation technologique et condition équitable d'accès au marché

Gage de plus grande efficacité et sécurité, la technologie du Cloud remplace les supports traditionnels et accroît la productivité et la compétitivité des entreprises faisant le choix de cette technologie

12 https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AWG_GuidingPrinciplesMarketStudies.pdf

13 https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/TelecomRoleforCompetition2006.pdf

aujourd'hui incontournable.

En revanche, les obstacles à l'adoption de la technologie du Cloud sont nombreux, au premier rang desquels les risques d'une concurrence entravée par des clauses contractuelles et des pratiques contestables. Ainsi, nous avons identifié les solutions possibles pour maximiser le potentiel d'innovation offert par la technologie du Cloud tout en préservant la condition d'une concurrence libre et non faussée : l'adoption généralisée des principes du Cigref et du CISPE, permettra de concilier l'innovation technologique du Cloud avec la concurrence nécessaire des éditeurs de logiciels.

Table des matières

Institut Choiseul

L'Institut Choiseul est un think tank indépendant dédié à l'analyse des questions stratégiques internationales et de la gouvernance économique mondiale.

Basé à Paris, son ambition est de créer des espaces indépendants de dialogue au carrefour du monde politique et institutionnel, de la sphère économique et de celle des idées pour fertiliser les débats sur les problématiques contemporaines.

En organisant des évènements de prestige et des rencontres informelles entre les principaux dirigeants à Paris, à Bruxelles, à Moscou ou en Afrique, en diffusant ses publications auprès des décideurs et des leaders d'opinion influents, l'Institut Choiseul nourrit continuellement les décisions des acteurs économiques et politiques.

Identificateur de talents à travers notamment le *Choiseul 100*, le *Choiseul 100 Africa*, le *Choiseul 100 Russia* ou encore le *Choiseul Ville de demain*, l'Institut Choiseul contribue aussi activement à l'émergence d'une jeune génération de dirigeants reconnus au niveau international.

Institut Choiseul - 12, rue Auber - 75009 Paris
Tél : 33 (0) 1 53 34 09 93 - contact@choiseul.info

www.choiseul.info
www.choiseul-france.com

Twitter : @instchoiseul

LinkedIn : Institut Choiseul