Les politiques publiques européennes en faveur d'un cloud souverain : fondements, modalités de mise en œuvre et évaluation critique

Frédéric Marty

LES POLITIQUES PUBLIQUES EUROPÉENNES EN FAVEUR D'UN CLOUD SOUVERAIN : FONDEMENTS, MODALITÉS DE MISE EN ŒUVRE ET ÉVALUATION CRITIQUE

Documents de travail GREDEG
GREDEG Working Papers Series

Frédéric Marty

GREDEG WP No. 2023-03
https://ideas.repec.org/s/gre/wpaper.html

Les politiques publiques européennes en faveur d'un cloud souverain : fondements, modalités de mise en œuvre et évaluation critique[1]

Frédéric Marty

CNRS – GREDEG – Université Côte d'Azur
CIRANO, Montréal

GREDEG Working Paper No. 2023-03

Résumé : Le recours à l'informatique en nuage est appelé à une très forte croissance en Europe dans les prochaines années et les grands opérateurs numériques (les *hyperscalers*) semblent être les mieux placés pour capter une part déterminante de cette croissance. Les enjeux liés au contrôle sur les données et au développement des applications dépassent les seules dimensions concurrentielles pour déborder sur des problématiques d'économie industrielle mais aussi de souveraineté tant en matière politique que stratégique. Des notions de contrôle, de résilience et de préservation d'une capacité de décision et d'action autonome des acteurs, tant les entreprises que les pouvoirs publics, doivent être interrogées dans cette perspective. Ce document de travail vise à identifier les risques de souveraineté liés au cloud et à présenter les initiatives prises par les Etats Membres et l'Union européenne dans ce domaine.

Mots clés : infonuagique, souveraineté, écosystèmes numériques, politique de concurrence, politique industrielle

Codes JEL : L13, L24, L41, L86

Abstract: Cloud computing is destined for very strong growth in Europe over the next few years and the large digital operators (hyperscalers) seem to be best placed to capture a decisive share of this development. The issues related to control over data and application development go beyond the competitive dimension to include not only industrial economy matters but also issues of sovereignty in both political and strategic terms. Notions of control, resilience, and the preservation of an autonomous capacity for decision-making and action on the part of actors, both companies and public authorities, must be examined from this perspective. This working paper, therefore, aims to identify the sovereignty risks associated with the cloud and to present the initiatives taken by the Member States and the European Union in this area.

Keywords: cloud computing, sovereignty, digital ecosystems, competition policy, industrial policy

JEL codes: L13, L24, L41, L86.

[1] Ce document de travail est issu d'une communication présentée à la faculté de droit et de science politique d'Aix-Marseille Université dans le cadre du colloque annuel organisé par le Master II Distribution Concurrence de l'Institut de Droit des Affaires, *Etat des lieux et perspectives d'une souveraineté numérique européenne*, le 6 mars 2023. Ce texte doit beaucoup aux présentations assurées pendant cette journée par Marie Cartapanis, David Bosco, Marc Mossé et Romain Deslorieux.

L'informatique en nuage (*cloud computing*) fait l'objet d'une attention croissante de la part des pouvoirs publics. Cette attention porte sur le fonctionnement du marché comme en témoigne l'enquête sectorielle lancée le 27janvier 2022 par l'Autorité de la concurrence[2]. Au-delà même de la préservation de la concurrence sur le marché, l'importance cruciale du secteur dans une économie fondée sur les données et les algorithmes en fait un paramètre central de la politique industrielle. Cependant, les services cloud ne soulèvent pas que des enjeux dans le champ des activités économiques mais également dans la sphère politique en ce que l'accès à certaines données personnelles ou sensibles met en jeu des droits fondamentaux et des dimensions essentielles de l'ordre public et que de possibles mises en cause de l'intégrité des systèmes informatiques de l'Etat font courir des risques majeurs en termes de sécurité collective. Prendre en compte les risques liés au recours au cloud, s'assurer les conditions d'une résilience face aux possibles exploitations de vulnérabilité et définir les mesures nécessaires pour les prévenir et y remédier pour préserver une capacité d'action à la fois pour les personnes physiques, les firmes et pour les pouvoirs publics. Il s'agit donc d'un enjeu de contrôle et d'exercice d'un pouvoir de décision, c'est-à-dire un enjeu de souveraineté.

L'infonuagique recouvre des technologies de stockage traitement des données et de développement et de mise en œuvre de solutions logicielles sur une base externalisée et distribuée. L'entreprise prestataire de service met à la disposition de ses clients des équipements et des applications natives dont les entreprises clientes ont l'usufruit (Benzina, 2019). Pour reprendre la définition donnée par l'Autorité de la concurrence : « Le cloud met à la disposition d'entreprises des capacités qui pourraient être difficiles et coûteuses à développer en interne. Ces avantages comprennent l'accès à des ressources informatiques évolutives et élastiques et la possibilité pour les clients d'augmenter ou de réduire facilement l'accès à la puissance informatique ». Le cloud permet d'externaliser l'infrastructure en matière d'investissement et d'entretien et offre aux firmes et aux utilisateurs un certain nombre de services. Le fournisseur de solutions cloud permet à ses clients de virtualiser des infrastructures (serveurs, data centers…) et fournit des outils logiciels permettant de traiter leurs données.

Si cette solution technique réunit des caractéristiques particulièrement attractives en termes de scalabilité, flexibilité et performance, elle n'en soulève pas moins des risques en termes de vulnérabilité et de dépendance. Cette situation n'est pas propre au cloud, elle prévaut à

[2] Se reporter au *Document de consultation publique sur le fonctionnement de la concurrence dans le secteur de l'informatique en nuage (cloud)* publié sur le site de l'Autorité de la concurrence dans le cadre de son enquête sectorielle le 13 juillet 2022.
https://www.autoritedelaconcurrence.fr/sites/default/files/Consultation-publique-cloud.pdf

différents degrés pour l'ensemble des écosystèmes numériques dans lesquels les utilisateurs peuvent être verrouillés au travers de standards et de complémentarités techniques et par le biais de clauses contractuelles (Marty, 2019). Une solution pour répondre à cette situation de dépendance est de permettre aux acteurs de reprendre le pouvoir (pour reprendre les termes de Toledano (2020)) c'est-à-dire de recouvrer leur souveraineté (étymologiquement de bénéficier d'une supériorité sur leur contrepartie). Cette souveraineté s'entend comme une capacité autonome d'appréciation, de décision et d'action.

Déclinée dans le secteur numérique et appliquée aux firmes et aux entités publiques, la souveraineté devient une autonomie stratégique numérique qui permet de prévenir ou de remédier à une situation de dépendance vis-à-vis d'un partenaire commercial ou technologique (Danet et Desforges, 2020). Face aux phénomènes de dépendance vis-à-vis des grandes firmes du numérique, des risques d'interférences liées à l'application extraterritoriales des règles de droit par des états tiers[3] voire de déstabilisation, la souveraineté se définit comme une volonté de reprendre le contrôle sur l'espace numérique quant aux technologies critiques et aux données, de minimiser les risques en termes d'intégrité ou de continuité de service, de préservation d'une capacité d'action autonome (Baur, 2023).

Le terme même de souveraineté numérique peut générer quelques doutes dans une perspective d'économie du droit de la concurrence. La notion de souveraineté appliquée à la sphère numérique en général ou à l'infonuagique en particulier appelle en effet plusieurs réflexions préliminaires.

Premièrement, la souveraineté en question doit-elle s'entendre comme la préservation des conditions d'une autonomie stratégique ou fait-t-elle écho aux conceptions portées par certains états de protection de leur espace numérique vis-à-vis des influences étrangères ? En d'autres termes, s'agit-il de gérer au mieux les interdépendances (voire les situations de dépendances) pour préserver les intérêts stratégiques de nos états et de nos entreprises ou au contraire d'être en mesure d'isoler ceux-ci de nos partenaires extérieurs ? Deuxièmement, cette souveraineté doit-elle s'entendre au niveau de la protection des individus (en matière de droits fondamentaux), de celle du marché ou de celle de la défense nationale ? Troisièmement dans quelle mesure l'argument de la souveraineté fait-il écho à une logique de politique industrielle et s'oppose-t-il dans cette mesure à une intervention sur la base des politiques de concurrence?

[3] La souveraineté de l'Etat peut *a contrario* se définir comme le monopole de la compétence d'exécution des lois répressive sur le territoire (Davis et Gunka, 2021, p.48).

Ce sont ces trois niveaux qu'il s'agit de considérer : le niveau stratégique, le niveau de la protection des données et des processus administratif et celui relatif aux activités de marché, que celles-ci se déclinent en termes de préoccupations de concurrence ou de défense d'une base technologique et industrielle au niveau des Etats-membres ou à celui de l'Union européenne[4]. Comment expliquer les initiatives portées par les Etats membres et par la Commission en faveur d'un cloud souverain ? Quel est l'éventail des outils utilisés ? Que peut-on conclure quant à leur efficacité présente et à leurs effets potentiels ? Pour répondre à ces questions nous nous attachons successivement à la caractérisation du problème, en mettant en exergue sa multi-dimensionnalité et ses traductions en termes de risques économiques et politiques, et à l'évaluation critique des solutions mises en œuvre en termes de politiques publiques tant au niveau des Etats membres que de l'Union européenne.

I – Caractérisation du problème

Il s'agit successivement de définir les différentes définitions qu'il est possible de donner de la souveraineté numérique appliquée au cloud et de mettre en exergue les différents risques qui peuvent procéder de ses imperfections.

A- Définition des termes et mise en évidence de la nature multi-niveaux de la problématique

1- Définitions de la souveraineté appliquée au cloud

Les définitions de la souveraineté peuvent être mises en perspective avec les différentes dimensions qu'elle peut couvrir. Selon que l'on se place dans une perspective stratégique, politique ou économique, les paramètres de la souveraineté peuvent varier mais un sens commun demeure. Il s'agit de la capacité d'action autonome dans le cadre d'interdépendance

[4] La stratégie nationale pour le cloud initiée en France le 17 mai 2021 qui place la souveraineté numérique dans ses objectifs adopte une structure comparable en combinant objectifs de sécurité pour les entreprises et les pouvoirs publics (cloud de confiance), une logique de transformation de l'Etat (politique dite de cloud au centre) et enfin une perspective de politique industrielle.
Se reporter à la circulaire n°6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat.

maîtrisées et non de développement autarcique[5]. Ainsi, dans le domaine numérique, il ne saurait être question de concevoir la souveraineté comme la capacité d'isoler ses réseaux de l'extérieur comme le font depuis une vingtaine d'années les régimes russes (avec le *runet souverain*, voir Limonier (2018)) et chinois. Il s'agit plutôt d'identifier des situations de risque et de définir les mesures à même de garantir la résilience des systèmes afin de permettre une action autonome.

La question de la souveraineté est exprimée dans toute sa clarté dans la *Revue nationale stratégique* publiée le 7 novembre 2022[6]. Le quatrième objectif stratégique porte en effet sur la résilience cyber, conçue comme une condition de la souveraineté. Cette dimension conduit à se pencher sur les systèmes d'informations de l'Etat, sur nos infrastructures critiques mais également sur le rôle systémique de certains acteurs de l'économie numérique.

Parmi les investissements nécessaires relevés par la *Revue nationale stratégique* figure la consolidation d'un socle numérique d'Etat homogène et sécurisé. La *Revue* insiste également sur la nécessité de pouvoir se reposer sur des écosystèmes numériques publics et privés robustes, résilients et performants. Ce support nécessite la sécurisation de certaines chaînes de valeur et la maîtrise de technologies critiques mais également une gestion des interdépendances avec nos alliés. Il s'agit de préserver notre autonomie stratégique en prévenant tout risque d'entrave à la mise en œuvre de nos capacités de défense et de nos systèmes d'armes. Cela ne signifie pas la mise en œuvre de systèmes propres en ce que l'autonomie stratégique n'exclut en rien des coopérations avec nos alliés. Elle se conçoit donc en termes d'interdépendance (Danet et Desforges, 2020). Il s'agit donc d'admettre le recours à des composants et à des systèmes développés par des tiers sur une base de confiance réciproque tout en conservant et en développant nos capacités de maîtrise des technologies les plus critiques.

La deuxième dimension, après celle relevant du domaine de la défense, est liée à l'exercice même de la souveraineté en termes politiques. Il s'agit de protéger les données ou les systèmes informatiques d'accès de l'extérieur à la fois pour protéger des droits fondamentaux ou pour garantir l'intégrité du fonctionnement administratif. La première dimension fait écho à la capacité d'accès aux données d'états tiers que cela soit sur une base territoriale (si les serveurs sont localisés dans les états concernés) ou sur une base extraterritoriale[7] (Bômont, 2018). La souveraineté numérique doit être également reliée à la préservation des conditions et des ressorts de la vie démocratique. Les élections américaines de 2016 ont montré les risques

[5] Pour un parallèle avec la stratégie de dissuasion nucléaire, se reporter à Poirier (1982).
[6] http://www.sgdsn.gouv.fr/uploads/2022/11/revue-nationale-strategique-07112022.pdf
[7] C'est la problématique du Cloud act américain que nous développons infra.

pouvant découler non seulement de l'exploitation indue des données dans la sphère commerciale (voir Cambridge Analytica) mais également ceux résultants d'interférences d'états hostiles. Ce second phénomène a pu être observé depuis à maintes reprises, notamment dans le cadre de campagnes électorales[8].

La souveraineté se définit comme une capacité d'action autonome. Les technologies reliées au cloud se caractérisent par une externalisation complète des systèmes informatiques vers des entreprises d'hébergement, fournissant des services intégrés. Ces services sont essentiels pour la performance des firmes utilisatrices. Ils réunissent les caractéristiques de scalabilité, flexibilité et de performance liés à l'exploitation algorithmique des données. Ils sont des supports essentiels de notre révolution industrielle (industrie 4.0, IA et IoT). Ils sont également appelés à occuper une place croissante dans les systèmes de défense (ex. SCAF et cloud tactique, voir Gros (2019)).

Cependant, de grands opérateurs (américains) occupent une place dominante en Europe et voient celle-ci se renforcer au fil des adoptions des solutions par les entreprises et administrations européennes. Leur place se renforce selon un modèle bien connu en économie numérique de consolidation autour d'écosystèmes en situation d'oligopole mais de plus en plus cloisonnés. La question de la préservation d'une capacité d'action autonome est posée.

2- Les trois niveaux de la question de la souveraineté numérique appliquée au cloud

Il s'agit de considérer successivement les risques relevant du champ des activités économiques et ceux du champ de la souveraineté dans le domaine politique.

La problématique est souvent envisagée sous l'angle concurrentiel ou du moins sous celui des activités économiques. Le terme même de concurrence doit d'ailleurs être entendu dans un sens plus large qu'à l'accoutumée. La problématique n'est pas limitée à la sanction des abus de position dominante. Elle porte également sur de possible défaillances structurelles de la concurrence – au travers d'effets de verrouillage concurrentiel irréversibles. Elle porte également sur des questions de déséquilibres contractuels qu'il serait possible d'envisager dans une perspective d'abus de dépendance économique (liée à des verrouillages techniques et à l'imposition de clauses contractuelles abusives).

[8] Voir le rapport de la RAND (Mazarr et al., 2019) sur la notion d'*information warfare* préparé pour l'Office of the Secretary of Defense (US DoD).

L'intervention peut dépasser la sanction des pratiques anticoncurrentielles pour aller vers des objectifs de maintien de la liberté de la concurrence (en termes de fluidité du marché définie à partir des possibilités d'entrées et de sorties) et de loyauté de celle-ci (en termes de contrôle de l'exercice des pouvoirs économiques privés). Elle peut aller jusqu'à une volonté de rééquilibrage de relations commerciales marquées par une asymétrie de pouvoir de négociation entre les contractants. L'ambition passe dès lors de la garantie de la loyauté ou de la « moralité » des relations de marché à une recherche d'équité en termes de *fairness*. On s'intéresse dès lors moins à la garantie des conditions de la transaction (exercice ou non d'un pouvoir de coercition) qu'à son résultat en termes de justice distributive ou de protection d'un acteur donné. L'intervention publique peut alors être animée par des objectifs relevant de la politique industrielle : elle est finalisée, sélective et donc asymétrique. Cette politique peut tout aussi bien être défensive (protéger les intérêts de notre base industrielle et technologique) qu'offensive (favoriser l'émergence d'offres alternatives ou de champions nationaux).

Le deuxième niveau de préoccupation lié au cloud porte sur l'intégrité des données et sur les possibilités d'atteintes aux droits fondamentaux liés à des ruptures d'intégrité des données. Ces questions peuvent porter sur l'accès à des données personnelles sensibles (en matière de santé par exemple) ou encore sur la capacité à interférer dans les processus administratifs et politiques. Les problématiques reliées aux données personnelles peuvent être saisies à la fois sous l'angle de leur collecte, stockage et traitement à des fins commerciales sans consentement éclairé et sous celui des droits d'accès sur une base extraterritoriale où que les données soient stockées au point de vue physique.

Les problématiques liées à la sécurité des données peuvent être envisagées en termes de vulnérabilité informatique. La question de la confiance dans les caractéristiques techniques des cloud utilisés est alors déterminante[9].

La dernière problématique à considérer dans cet ensemble porte sur la garantie des processus administratifs mais également politiques. Il s'agit ici de s'attacher aux risques de déstabilisations et aux risques de manipulations. Si nous considérons les seconds, le cas de l'utilisation des données issues des réseaux sociaux peut être intéressant à considérer. L'exploitation des données personnelles à des fins de ciblage publicitaire (voire de manipulation comportementale comme le comme le montre la littérature sur les *dark patterns*)

[9] Il ne faut pas oublier qu'il convient de mettre en balance les risques liés à l'utilisation d'un cloud public ou même d'un cloud privé mis à disposition par un hyperscaler avec les risques informatiques induits par la coexistence de très nombreux systèmes IT hétérogènes, souvent obsolètes et mal sécurisés.

est connue dans la sphère des activités économiques. L'affaire Cambridge Analytica a montré que ces techniques pouvaient être aisément répliquées dans la sphère politique, sur le marché électoral.

La possibilité d'attaques sur les systèmes informatiques et sur les infrastructures collectives conduit à interroger le cloud sous l'angle de la sécurité vis-à-vis des actions malveillantes que celles-ci émanent de groupes criminels (rançongiciel ou *ransomware*) ou d'états hostiles (Taillat, 2016). Les attaques hybrides qui se sont multipliées depuis 2014 sur le flanc est européen témoignent de ces stratégies de déstabilisation mises en œuvre pour rester sous le niveau de qualification d'actes de guerre mais dont les effets déstabilisateurs sont significatifs. De la même façon, la stratégie mise en œuvre par l'armée russe vis-à-vis des infrastructures ukrainiennes montre que certains états pourraient exploiter toute faille de sécurité dans nos systèmes d'information ou dans nos systèmes de pilotage des infrastructures de réseaux.

La protection des infrastructures critiques peut être non seulement compromise par des cyberattaques mais également par des vulnérabilités liées à l'utilisation de composants ou de logiciels en provenance d'Etats potentiellement hostiles. Cette problématique touche non seulement les infrastructures civiles (songeons par exemple aux réseaux de 5G) mais également les systèmes d'armes[10].

La question liée à la vulnérabilité des systèmes d'information et de décision utilisant l'infonuagique revêt donc également une dimension stratégique. Les vulnérabilités qui en découlent peuvent compromettre notre souveraineté, c'est-à-dire notre autonomie stratégique.

Les interrogations liées au cloud souverain s'inscrivent donc dans un continuum allant de la politique économique jusqu'à la défense de nos intérêts stratégiques elle-même. Cependant cette souveraineté ne doit aucun cas être saisie dans une acceptation autarcique. Il s'agit de prendre en compte les phénomènes d'interdépendance, de mesurer les risques induits et de mettre en œuvres des mesures à mêmes d'en minimiser les conséquences. En ce sens, la souveraineté peut être rapprocher de la notion de résilience.

B – Quels risques s'agit-il de traiter ?

[10] Songeons au cas, en dehors même de celui des composants électroniques, d'un des alliages utilisés dans le F35 dont la découverte avait donné lieu à une suspension des livraisons en septembre 2022 de crainte qu'il n'introduise des failles dans la protection électronique de l'appareil.
https://www.reuters.com/business/aerospace-defense/f-35-jet-deliveries-can-resume-following-waiver-chinese-origin-alloy-pentagon-2022-10-08/

1) *Dans le domaine de la défense et des risques rattaché aux domaines politiques et des droits fondamentaux*

Dans le domaine de la défense, les risques que nous avons présentés *supra* relèvent de l'intégrité des systèmes et de la maîtrise des technologies les plus critiques. Le problème pour les données personnelles est relié aux conditions de collecte et de traitement des données. Il peut tenir à des questions reliées à des capacités de ciblage et d'exploitations malveillantes des données acquises par des voies légales (songeons à certains réseaux sociaux) ou par des stratégies délinquantes (piratage de systèmes informatiques publics).

Considérons la première dimension : celle des données hébergées sur des clouds opérés par des opérateurs étrangers même s'ils sont localisés en Europe. Des états peuvent avoir une capacité d'accès aux données d'états tiers que cela soit sur une base territoriale (si les serveurs sont localisés dans les états concernés) ou sur une base extraterritoriale (Bômont, 2018). C'est la problématique du Cloud act américain. Le Cloud Act - *Clarifying Lawful Overseas Use of Data Act*[11] – permet aux autorités américaines de requérir des firmes américaines l'accès aux données détenues même si celles-ci sont stockées à l'étranger[12]. Celui-ci, voté en 2018, s'inscrit dans la continuité du Patriot Act du 25 octobre 2001 (Mastor, 2008), il permet aux autorités américaines d'accéder aux données des particuliers et des entreprises à l'étranger sans passer par les voies habituelles de la coopération judiciaire (Davis et Gunka, 2021).

L'une des dimensions essentielles porte sur le transfert des données et sur l'accès à ces données depuis des territoires étrangers. La question est celle de la capacité de surveillance algorithmique extraterritoriale[13]. Il convient de s'interroger sur la nature des exigences de politiques publiques qui pourraient répondre à ce souci de protection des données. Des

[11] https://www.justice.gov/criminal-oia/cloud-act-resources

[12] Dans le cadre de procédures pénales ou administratives, les autorités américaines peuvent accéder à des données même si elles sont stockées en dehors des Etats-Unis dès lors que l'opérateur concerné (communication service provider) est soumis à la juridiction américaine (en vertu du standard de *personal juridiction*, il suffit que la personne ait un lien avec les Etats-Unis) et ce même sans passer par les voies normales de la coopération inter-étatique basée sur des traités d'assistance judiciaire internationale. La question centrale est celle de la capacité d'accès depuis les Etats-Unis. Le Cloud act a été promulgué à la suite d'un long contentieux avec Microsoft quant à l'interprétation du Stored Communication Act de 1986, contentieux qui fut porté devant la Cour Suprême (United States v Microsoft Corp, 584 U.S.__ 2018).

[13] Il va de soi que des applications d'origines non américaines apportent bien moins de garanties en termes de recueil des données. On songera ici à certaines applications de micro-messagerie ou de réseaux sociaux. Les mesures prises ces dernières semaines contre le réseau social TikTok témoignent des risques qui sont communs aux différentes démocraties occidentales quant aux capacités de collecte de données sensibles. Voir pour le cas de la Commission européenne, la décision prise le 23 février 2023 : https://www.reuters.com/article/ue-tiktok-idFRKBN2UX0XZ

exigences en termes de localisation des données existent de longue date en Chine et en Russie par exemple. Cependant, la localisation en elle-même importe moins qu'il peut y paraître. Le contrôle de l'accès et la sécurisation des données est bien plus déterminante. Cependant, des questions liées à la disponibilité des données, à leur intégrité et à leur confidentialité doivent être posées et ce d'autant plus dans une approche basée sur les risques qu'il s'agit de données sensibles.

La question est alors celle des risques induits par l'utilisation de cloud publics voire de cloud privés mis en place par les différents *hyperscalers*[14]. Doit-on pour minimiser lesdits risques opter pour des cloud propres à l'administration, mettre en œuvre des stratégies hybrides ou développer des stratégies multiclouds ?

2) Dans le domaine des activités de marché

Il convient de distinguer les risques de nature concurrentielle *stricto sensu* des risques liés à l'asymétrie des acteurs et donc aux phénomènes de dépendance économique.

L'infonuagique constitue une extension radicale, dans son ampleur et dans les solutions techniques utilisées, des modèles d'infogérance développés depuis les années 1980 en matière d'externalisation des services informatiques. Ce nouveau modèle mis en place depuis la première décennie de notre siècle. Il a évolué vers une plateformisation avec trois niveaux distincts d'intégration : pour les données (PaaS[15]), pour les applications (SaaS[16]) et enfin plus

[14] Nous reprenons ici les termes utilisés par l'Autorité de la concurrence dans son document de consultation diffusé dans le cadre de son enquête sectorielle sur le secteur du cloud. L'Autorité définit ces derniers comme des acteurs déjà installés sur d'autres marchés numériques et qui ont développé une activité cloud en bénéficiant de leurs capacités techniques et de leurs fortes capacités d'investissements (avec des horizons de retours financiers particulièrement longs). Ces entreprises de la donnée et de développement logiciel bénéficient d'économie d'échelle et d'envergure particulièrement significatives. Elles doivent être distinguées d'autres opérateurs tels que des firmes spécialisées dans l'hébergement Internet (comme OVH). Ces derniers proposent également des offres de type IaaS et PaaS. La description de l'écosystème cloud par l'Autorité met également en exergue le rôle des entreprises de services du numériques comme Atos ou Capgemini. Celles-ci apportent des prestations techniques auprès des utilisateurs et des services de conseil. Comme nous le verrons infra, ces entreprises s'engagent dans des montages partenariaux avec les hyperscalers pour assurer des services garantissant la conformité des services avec les exigences relatives à la conformité des services cloud avec les objectifs de sécurité et de résilience portés par les textes français et européens.

[15] L'utilisateur n'a pas la main sur le système d'exploitation opérant les infrastructures de l'opérateur cloud mais conserve la main sur les applications utilisées.

[16] L'utilisateur des services met en œuvre les applications mises à disposition par le fournisseur de services et peut y accéder par une interface web.

stratégique encore pour les infrastructures elles-mêmes (IaaS[17]). L'avantage déterminant du cloud est qu'il réunit des qualités de scalabilité, de flexibilité et de performance que les firmes ne pourraient développer pour leur compte propre.

Une première définition du cloud souverain peut se limiter au développement d'une infonuagique propre à l'administration. Outre un gain en performance, il est surtout anticipé un gain significatif en matière de sécurité informatique. Cela substitue un système centralisé à maints systèmes spécifiques, hétérogènes, peu sécurisés et mal maintenus. Il convient donc de distinguer les données et les systèmes de l'Etat de ceux mis en œuvre par les acteurs de marché. Pour les premiers l'intégrité et la résilience importent bien plus que la performance économique. L'enjeu principal est celui de la cybersécurité. En effet, les effets externes immédiats d'une cyberattaque sur de tels systèmes sont sans commune mesure avec ceux qui pourraient résulter de stratégies d'espionnage industriel.

La logique de sécurisation des cloud et des systèmes informatiques doit également prévaloir dans le cas des infrastructures critiques. Les tensions sur le flanc est européen qui ont scandé la période 2014-2022 ont bien montré les possibles attaques informatiques contre les grands réseaux. Les réseaux peuvent être une cible de cyberattaques en cas de conflits tout comme l'ensemble des systèmes d'information publics (Nocetti, 2018).

Si l'on excepte les cloud réservés aux administrations publiques, la solution d'un cloud construit sur une base régionale ou étatique présente maints défauts lesquels tiennent aux effets pervers de la balkanisation de l'Internet ou encore aux pertes de compétitivités liées à la renonciation aux effets d'échelle, d'envergure et d'accroissement de performance liés au traitement de données plus massives, plus diversifiées et plus fréquemment renouvelées. Ces caractéristiques sont essentielles dans le contexte d'un recours massif à l'intelligence artificielle (Iansiti et Lakhani, 2020). La capacité à entraîner les algorithmes utilisant des techniques d'apprentissage machine dépend des caractéristiques des cloud. *In fine* utiliser un cloud autarcique se paierait par un déclassement industriel irréversible. Non seulement une telle stratégie serait certainement vouée à l'échec du fait de la limitation de nos moyens techniques et financiers mais elle nous exposerait à disposer d'algorithmes moins performants que ceux de nos compétiteurs.

[17] La capacité est mise à disposition par l'opérateur cloud et le consommateur peut y déployer et y exécuter les applications de son choix, y compris le système d'exploitation.

L'une des solutions réside dans le développement de stratégies de cloud hybrides. Elle peut se concevoir, si nous reprenons les catégories habituelles de l'économie numérique, dans une logique de multi-hébergement, qui est la seule à même de prévenir les risques de dépendance économique et technologique.

Ce multi-hébergement peut prendre différentes formes. Il s'agit peut tout d'abord s'agir de stratégie de cloud hybride conduisant à combiner cloud public (hébergement complet chez les hyperscalers[18]) et cloud privé (une infrastructure mise à disposition par ces derniers à titre exclusif mais bénéficiant de leurs solutions logicielle[19]). Il peut ensuite s'agir de mettre en œuvre des stratégies multiclouds passant par la répartition de différentes tâches sur différents clouds. L'Autorité de la concurrence distingue trois types de stratégies multicloud dans son document de consultation de juillet 2022. Dans une première l'entreprise utilise des services distincts pour des tâches distinctes. Les problèmes d'interopérabilité sont alors limités. Dans une deuxième stratégie, l'entreprise utilisatrice de services cloud utilisent plusieurs prestataires pour différentes étapes de la même tâche (hébergement des données, développement des algorithmes etc…). Cette option – qui apparaît comme peu utilisée – suppose une forte interopérabilité des services. Dans une troisième stratégie, une entreprise utilisatrice répartit une même tâche entre plusieurs prestataires. Cette stratégie de multi-hébergement réduit significativement les risques de dépendance économique et technique pour l'entreprise utilisatrice mais l'expose à des difficultés en termes d'interopérabilité des services, à des risques additionnels quant à la continuité d'exploitation et à la vulnérabilité des systèmes informatiques et enfin à des coûts de transaction additionnels. La réduction des risques de dépendance peut enfin passer par le recours à des solutions de *edge computing*[20] permettant de traiter les données à la source (i.e. en périphérie du cloud) pour ne les transférer qu'*ex post* vers un entrepôt de données hébergé sur un cloud.

Si l'on sort du champ strictement concurrentiel, les différentes politiques publiques successivement mises en œuvre en Europe (d'abord au niveau des Etats membres puis à celui de l'Union) permettent d'illustrer les différentes de la souveraineté numérique appliquée au cloud mais également leurs limites. Il convient de noter que les notions mêmes d'internet souverain ou de cloud souverains posent des questions techniques en ce que les flux de données

[18] Pour reprendre la définition proposée par l'Autorité de la concurrence, dans le cas du cloud public l'infrastructure est détenue, gérée et exploitée par un opérateur de services cloud sur ses propres serveurs et dans ses data centers.
[19] Dans ce cas, l'infrastructure mise à disposition par l'hyperscaler l'est pour un seul client. Les serveurs peuvent être localisés chez l'hyperscaler ou chez le client, ou même dans une combinaison des deux.
[20] Informatique en périphérie : les données sont traitées près de leur source en périphérie du réseau. Pour une discussion générale, voir Varghese et al., (2021).

sont indépendants des questions de juridictions. L'ensemble des dispositifs techniques qu'il est possible de mettre en œuvre ont indubitablement un coût en termes financiers ou en termes de performance[21].

1- Risques concurrentiels

La question de la dépendance des firmes européennes vis-à-vis des grands acteurs, en l'occurrence américains[22], se pose avec d'autant plus d'acuité que le recours aux services cloud est significativement plus faible en Europe qu'aux Etats-Unis. En l'espèce, 94% des entreprises et administrations américaines ont recours à ces services alors que le taux ne dépasse pas 41% en Europe et 29% en France[23]. Les taux d'adoption vont aller croissant et ce de façon très significative mais les entreprises en cause, les hyperscalers, s'approprient une part très largement majoritaire de la croissance[24]. En 2021, près de 75% du marché français était contrôlé par trois opérateurs américains : Amazon, Microsoft et Google (respectivement 46%, 17% et 8%). Cette dépendance ne pose pas des problèmes de nature géostratégique mais plutôt de nature économique dans le champ concurrentiel.

L'accent mis sur les questions concurrentielles peut dans une certaine mesure entrer en conflit avec les dimensions stratégiques de la souveraineté numérique. En effet, tant pour les questions de protection des données personnelles que pour celles relatives aux pratiques de marché, certains textes européens traitent plus durement les firmes américaines que des firmes non occidentales dans la mesure où celles-ci ne peuvent être tenues – pour l'heure – comme des contrôleuses d'accès. Cependant celle-ci posent des questions de sécurité bien plus graves en ce qu'elles ne concernent pas seulement des dimensions économiques mais des questions militaires. Les initiatives européennes ne doivent pas être conçues comme porteuses de mesures discriminatoires ou visant à ériger des barrières à l'entrée (voir Burwell et Propp, 2020). Cependant, les initiatives réglementaires pèsent également sur les opérateurs européens et ce particulièrement quand elles ne sont pas asymétriques. Les coûts de conformité sont

[21] Les données sont a priori stockées sur des bases techniques qui ne répondent pas à des logiques de délimitations étatiques. Il est en outre possible que pour des raisons de robustesse et de limitation de la latence la gestion optimale d'un cloud suppose de dupliquer les données et de les localiser dans plusieurs data centers lesquels n'ont pas vocation à être situés dans le même état.

[22] Au niveau mondial néanmoins, Alibaba Cloud est le troisième acteur avec 9,5% de parts de marché, derrière AWS (39%), Microsoft (21%) mais devant Google (données septembre 2022). Les opérateurs chinois sont bien moins implantés en Europe que les firmes américaines, à la fois dans le cloud et dans les autres activités numériques.

[23] Données Eurostat, décembre 2021 : *Cloud computing, statistics on the use by enterprises*

[24] Ces derniers s'approprient 80% des nouveaux utilisateurs (Luzeaux, 2022).

comparativement plus importants pour des acteurs de taille modeste que pour de grands groupes intégrés[25].

Les risques liés aux comportements des opérateurs dominants sont communs à l'ensemble des écosystèmes numériques et n'appellent pas à ce titre de développement particulier ni de nouvelles théories du dommage concurrentiel. Les pratiques en question relèvent de la catégorie des abus de position dominante, à savoir les abus d'éviction et les abus d'exploitation. Ces pratiques unilatérales sont cependant particulièrement aisées à mettre en œuvre dans le cloud, notamment dans le segment IaaS, du fait de sa nature de *quasi* facilité essentielle.

L'essentialité doit en effet se concevoir ici non pas en termes d'indispensabilité mais plutôt en termes de réplicabilité (Marty et Mouton, 2022). Comme le note l'Autorité de la concurrence dans son document de consultation les hyperscalers ont pu développer leurs infrastructures avant même la commercialisation des services. Les investissements consentis par ces derniers jouent (imparfaitement) le rôle de barrière à l'entrée en ce que le développement de capacités propres induirait pour les entreprises des coûts d'investissement prohibitifs, des risques majeurs (en regard des compétences à développer en interne) et des délais significatifs. En outre, la performance des services prestés par les hyperscalers est liée à leurs économies d'échelle et d'envergure et à leurs capacités d'apprentissage. Un cloud propriétaire ne peut rivaliser sur ces points. Il ne peut pas plus le faire au regard de préoccupations de résilience et de sécurité. L'essentialité du service ne signifie pas pour autant celle du prestataire. Il est sur le principe possible de choisir entre des cloud concurrents mais les capacités de transition de l'un à l'autre peuvent être entravées par de nombreux facteurs que nous présentons *infra*.

L'offre proposée par le prestataire est non réplicable en interne (il n'y a pas de réversibilité du choix dans des conditions techniques et financières raisonnables) et la décision de changer de prestataire est non seulement extrêmement coûteuse mais de plus risquée pour la continuité de l'exploitation (la transférabilité est donc extrêmement difficile). La littérature économique

[25] Un certain nombre de nuances est à apporter quant à l'attitude de nos partenaires américains. Premièrement, certains textes européens exercent une influence sur les législations passées par des états fédérés. Il en est ainsi quant au RGPD dont l'influence sur les textes californiens est notable (voir le California Consumer Privacy Act – CCPA, adopté en 2018) mais également des règles de concurrence elles-mêmes, notamment au travers de la notion d'abus de position dominante pourtant propre au droit européen (voir par exemple, sur des questions reliées aux impacts concurrentiels des stratégies d'auto-préférence, l'American Innovation and Choice Online Act proposé par la sénatrice Klobuchar). Deuxièmement, l'attitude de l'administration américaine est différente d'un ministère à l'autre, ce qui est somme toute normal dans un système administratif. Les préoccupations vis-à-vis des Big Techs sont partagées par le DoJ et la FTC à la fois dans les domaines concurrentiels et politiques. La prise en compte des risques cyber est bien évidemment centrale dans les évaluations du DoD. Cependant, la focale est très différente pour le Departement of Commerce ce qui est naturel dans la mesure où sa mission porte sur la défense des activités des firmes américaines (Velliet, 2023).

montre que si les gains liés à l'adoption de solutions clouds sont très significatifs pour les firmes (qui n'ont pas les moyens financiers et technique de déployer une infrastructure performante et sécure qui soit immédiatement dimensionnée à leurs pointes d'utilisation en termes de capacité), il n'en demeure pas moins que l'inertie en faveur du service utilisé réduit très significativement leurs gains de bien-être. Jin et al. (2022) ont par exemple montré que si les gains d'efficacité liés à l'utilisation des services clouds dépassent de 216% les coûts associés, 62% de ce bénéfice échappe aux firmes utilisatrices du fait de leur dépendance vis-à-vis du service existant.

Cette position de force donne la capacité et éventuellement les incitations à la commission d'abus (Hubert et Marty, 2019).

Dans le domaine des abus d'éviction, les problématiques habituelles sur les refus d'accès à une infrastructure (quasi) essentielle ou les refus de contracter constituent une première modalité de pratiques d'éviction[26]. Les refus peuvent prendre la forme de refus absolu ou de refus relatif de contracter (i.e. selon des conditions dégradées ou discriminatoires). Ces pratiques pourraient par exemple être mises en œuvre au détriment de partenaires commerciaux pratiquant le multi-hébergement (en l'espèce des stratégies multiclouds) pour les inciter à opter pour un mono-hébergement. Elles pourraient également dans le cas d'une intégration verticale être utilisées à l'encontre d'une firme ayant une activité concurrente sur un marché aval dans une logique de compression des marges ou de dégradation de la qualité du service presté.

Au-delà des stratégies de forclusion, des stratégies d'extension verticale de la position dominante peuvent être mises en œuvre au travers de ventes liées ou groupées. Les ventes liées depuis des activités d'IaaS sont potentiellement aisées à mettre en œuvre.

Enfin, les stratégies d'éviction par rapport aux clients du service amont qui peuvent également être des concurrents en aval peuvent reposer sur une instrumentalisation de l'accès privilégié aux données que détient l'opérateur cloud. Il peut s'engager dans des stratégies de micro-prédation vis-à-vis des clients les plus attractifs ou encore cloner leurs offres de services (Marty, 2019).

Les abus d'éviction peuvent également être accompagnés d'abus d'exploitation par lesquels les opérateurs cloud peuvent imposer des conditions tarifaires déséquilibrées ou imposer des

[26] Se reporter à notre communication, « Les enjeux économiques et concurrentiels liés au cloud : une infrastructure essentielle ? », Conférence de l'AMCo, M2 Droit de la concurrence et des contrats, Université Paris Saclay, janvier 2023.

conditions de transaction qu'il aurait été impossible d'obtenir en l'absence d'une position dominante.

Les stratégies de prix abusifs peuvent également être utilisées pour imposer un mono-hébergement aux partenaires commerciaux. C'est par exemple le cas des *egress fees* qu'a présenté l'Autorité de la concurrence dans son document de consultation préparatoire à son enquête sectorielle sur le cloud. Imposer des coûts élevés sur les flux sortants peut à la fois renforcer la dépendance du partenaire commercial en faisant obstacle aux stratégies multiclouds mais elle accroît les barrières à la sortie (*switching costs*) et entrave donc la transférabilité des données et des services associés d'un cloud à l'autre.

Le document de consultation de l'Autorité de la concurrence publié en juillet 2022 dans le cadre de son enquête sectorielle illustre les dynamiques possibles de verrouillage des utilisateurs dans un écosystème numérique[27] lesquelles sont exacerbées pour les services de cloud. Un opérateur dominant dans un écosystème a tout intérêt de subventionner l'entrée des utilisateurs dans ce dernier. Dans le domaine du cloud cela passe notamment par des mécanismes de jetons de type *credit cloud.* Ce type de dispositif peut fonctionner comme des primes de fidélité (en accordant des ristournes sur la base des volumes) ou comme des incitatifs à l'adoption[28]. Il s'agit dans tous les cas de figure d'abaisser les barrières à l'entrée pour accroître le niveau d'activité sur le cloud. Cependant, ces incitatifs peuvent contribuer à créer une dépendance dans la mesure où les stratégies multicloud sont difficiles à mettre en œuvre techniquement, que la redondance est coûteuse pour les firmes et que les opérateurs peuvent faire peser des conditions bien moins favorables pour les flux sortants. Comme le relève l'Autorité de la concurrence, un opérateur cloud peut mettre en œuvre une tarification asymétrique entre les flux entrants (*ingress fees*) et les flux sortants (*egress fees*). Les seconds frais, s'ils sont très élevés, peuvent dissuader les entreprises utilisatrices de changer d'opérateur cloud, de réinternaliser les services en question (si tant est que cela soit possible) ou encore de mettre en œuvre des stratégies multicloud).

2- Des risques allant au-delà des limites des règles de concurrence

[27] Pour une présentation générale de ces dernières se reporter à Marty et Pillot (2021).
[28] Dans de nombreux écosystèmes numériques, notamment dans les *blockchains*, la distribution préalable *d'utility tokens* ou la mise à disposition à un prix privilégié, vise à répondre aux difficultés liées au *cold start*. Les écosystèmes numériques se caractérisent par des effets de réseaux et des rendements croissants, sans parler des effets d'apprentissage, qui font que leur performance dépend du nombre d'utilisateurs. Au démarrage il peut être rationnel de « subventionner » les premiers adopteurs du service (Chen, 2021).

Si les catégories du droit de la concurrence permettent de saisir un certain nombre de pratiques problématiques, l'application des règles de concurrence peut s'avérer moins aisée que souhaitable. Premièrement, comme souvent sur les marchés numériques, le marché pertinent n'est pas aisé à définir. Deuxièmement, nous sommes face à un oligopole et donc la position dominante individuelle n'est pas facilement caractérisable. Le problème vient de l'étanchéité des silos qui caractérisent cet oligopole. La question est celle des positions dominantes relatives et également celle des positions significatives sur plusieurs marchés (pour reprendre les termes de l'amendement de janvier 2021 à la loi allemande sur les restrictions de concurrence à l'origine de l'article 19(1a)[29]). Les problématiques économiques sont alors reliées à des phénomènes de dépendance économique, de conditions de concurrence déloyales (absence de concurrence à égalité des armes), de discriminations, de conditions contractuelles déséquilibrées.

Les problèmes sont donc les mêmes que sur de nombreux marchés numériques. Les complémenteurs ont besoin des services de l'opérateur de plateforme mais ce dernier pour s'approprier une part croissante de la rente créée ou encore se substituer à ses partenaires commerciaux pour accroître ses marges et consolider sa position de marché (Marty, 2019). Ces questions sont d'autant plus déterminantes pour les politiques européennes que les complémenteurs sont des acteurs stratégiques pour notre révolution industrielle (IA, IoT, Industrie 4.0, 5 et 6G…).

Si le recours aux services des hyperscalers induit des vulnérabilités de long terme pour nos firmes (et pour nos administrations), le problème est qu'il n'y a peut-être pas de solution alternative équivalente en termes de coûts, flexibilité, performance, scalabilité et même sécurité. Le recours à leurs services est une composante essentielle à la compétitivité sur les marchés aval et contribue à minimiser les risques cyber décrits *supra*.

Des clouds souverains pourraient-ils être des solutions équivalentes ? La question ne relève pas du champ de la concurrence mais de celui de la politique industrielle.

II – Quelles solutions et quelles évaluations ?

29 https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html

Il s'agit de s'attacher successivement à la présentation des différentes initiatives suivies par les Etats membres et la Commission et à l'analyse de leurs possibles impacts.

A - Les initiatives des pouvoirs publics

1) Les politiques menées par les Etats-membres

Les initiatives initiales viennent des Etats-membres avant que le relais ne soit pris par la Commission. Nous présentons succinctement les stratégies française et allemande afin de montrer de quelle façon elles évoluent entre les différents niveaux de la problématique du cloud souverain et quant à leur dimension de politique industrielle.

Dans le cas français, la question du cloud souverain a été posée dès 2009 et figurait dans le programme investissements d'avenir[30]. La première intention du gouvernement a été de faire émerger un champion national dans une logique de partenariat public-privé (Bômont et Cattaruzza, 2020). Ce premier projet, baptisé Andromède, réunissait Thalès, Dassault Systèmes et Orange. Le départ de Dassault Systèmes en décembre 2011 se traduisit par la formation d'un second consortium avec SFR en février 2012 avant qu'il ne se retire définitivement en avril 2012. Au final, deux consortia public-privé furent formés : Cloudwatt (Orange et Thalès) et Numergy (SFR et Bull). Progressivement les deux opérateurs télécom rachetèrent les parts de l'Etat et de leurs partenaires industriels. Les évaluations de cette expérience de création d'une offre ex-nihilo (Bômont et Cattaruzza, 2020) insistèrent sur une entrée à un moment où la demande pour une 'offre souveraine' était encore trop faible, à une concurrence déjà installée qu'il s'agisse des hyperscalers ou d'opérateurs nationaux (tel OVH) et à des services qui demeuraient essentiellement des services d'hébergement. Le projet de cloud souverain fut relancé en 2013 comme l'un des 34 plans de la Nouvelle France Industrielle[31]. Le projet validé en juin 2014 était porté par OVH et Atos. Il ne s'agissait plus de construire ex nihilo un champion national mais de soutenir la stratégie d'opérateurs déjà présents sur le marché. Cette

[30] La loi de finances rectificative de 2010 prévoyait un budget de 1,75 milliard d'euros pour le « développement des usages et contenus innovants, dont notamment le développement de l'informatique en nuage ».
Pour le Plan Investissement d'avenir, voir : https://www.gouvernement.fr/le-programme-d-investissements-d-avenir

[31] https://www.economie.gouv.fr/files/files/PDF/dp-indus-futur-2016.pdf

approche est soutenue par une stratégie de labellisation via l'ANSSI (Agence nationale de la sécurité des systèmes d'information) avec le label *secure cloud* lancé en février 2015[32].

Ainsi, une approche centrée sur la stratégie industrielle succéda progressivement une approche plus centrée sur les enjeux de sécurité. Le cloud occupe par exemple une place importante dans la *Revue stratégique de cyberdéfense* publiée en février 2018[33] mais également dans la stratégie globale de l'administration. Celle-ci a été définie par une circulaire du Premier Ministre du 8 novembre 2018 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat[34]. La question de l'utilisation des services clouds par l'administration porte donc essentiellement sur des questions de sécurité des données dans une optique de B2G (*Business to Government*).

La solution prônée est celle d'un cloud hybride combinant des solutions de cloud public et de cloud privé. Le cloud privé permet d'héberger les données sur des serveurs sécurisés et isolés des autres clients. Comme le notent Bômont et Cattaruzza (2020), l'architecture globale repose sur la superposition de trois niveaux aux caractéristiques de sécurité distinctes. Le premier correspond à un cloud privé directement opéré et hébergé par les services de l'Etat. Le deuxième à un cloud privé hébergé chez un opérateur qui propose donc ses services sur une infrastructure dédiée. Le troisième enfin à un cloud générique permettant d'utiliser toutes les potentialités de l'infonuagique. Le cloud souverain a progressivement évolué d'une politique industrielle volontariste visant à créer *ex nihilo* un champion national vers une approche plus centrée vers la sécurité des données. Le cloud de confiance actuel vise plutôt à utiliser des solutions techniques développées par les opérateurs privés mais en garantissant un niveau satisfaisant de sécurité. A partir de 2018, la question ne fut plus celle d'une politique industrielle visant à construire ou consolider une offre nationale mais celle de garantir un niveau adéquat de sécurité pour les entreprises et pour l'administration. L'approche française converge vers celle suivie en Allemagne.

La première initiative allemande au milieu de la décennie 2010 répondit à une stratégie de mise à disposition d'une offre souveraine visant notamment à prévenir l'accès aux données par des états étrangers. Il s'est agi de l'initiative Microsoft Cloud Deutschland. Elle visait à disposer des capacités techniques développées par MS pour gérer des data centers de droit allemand et localisés en Allemagne[35] avec Deutsche Telekom intervenant comme mandataire. L'abandon

[32] https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/
[33] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
[34] https://www.legifrance.gouv.fr/circulaire/id/44120
[35] Les serveurs n'étaient pas intégrés au système de Cloud globalde Microsoft.

de cette stratégie par Microsoft en 2018[36], se traduisit par le lancement d'une nouvelle initiative, le Bundescloud, visant à garantir des solutions sécurisées pour l'administration selon un modèle de cloud privé[37]. La dernière initiative correspond au projet GAIA-X commun avec la France et étendu à l'échelle de l'Union.

2) Les politiques de l'Union européenne

Les appels en faveur d'une souveraineté numérique européenne résidaient initialement à des souhaits de faire émerger des champions industriels à même de rivaliser avec les firmes américaines et chinoises[38]. Cependant, comme pour les cas français et allemands décrits supra, une évolution s'est progressivement dessinée entre une ambition de favoriser l'essor d'alternatives aux offres des hyperscalers et volonté de construire les conditions d'une autonomie vis-à-vis de ces derniers. Il s'agit dans ce cadre de prévenir une situation de dépendance. Nous allons à cette fin présenter les outils qui relèvent de la régulation des marchés avant de nous attacher aux outils qui peuvent relever d'une définition traditionnelle de la politique industrielle.

2a) Les stratégies relevant du droit de la concurrence et de la régulation des marchés

La politique de la concurrence est la première des politiques industrielles (Marty, 2012) en ce qu'elle garantit le cadre d'une concurrence par les mérites en prévenant toute intervention sélective en faveur d'une entreprise donnée qui pourrait compromettre une concurrence à égalité des armes. Elle fournit également les incitations idoines aux entreprises en termes d'efficacité mais également en termes de différenciation des services. Elle est, à ce titre, la plus à même d'inciter les firmes à proposer des offres spécifiques en termes de sécurité des solutions cloud. Les incitations concurrentielles ne se limitent pas aux volets classiques des politiques de la concurrence (sanction des pratiques anticoncurrentielles, contrôle des concentrations et

[36] Il est nécessaire de relier cette évolution au cloud act américain dans la mesure où sa logique d'accès ne permet pas de formuler un refus sur la base d'une localisation géographique donnée. Pour Baur (2023, p.19) cette expérience témoigne de la difficulté de concilier les bénéfices du recours aux services d'un hyperscaler avec les garanties de non-accès de tiers aux données, en d'autres termes de concilier innovation et contrôle, deux termes qu'essaie de concilier le projet GAIA-X.

[37] L'infrastructure cloud de l'administration est alors séparée. Il s'agit de concilier la partition du cloud avec les avantages traditionnels du cloud centralisé (économie de coût, flexibilité, scalabilité…).

[38] Voir par exemple le discours du Président Macron prononcé en Sorbonne le 26 septembre 2017, cité par Codagnone et Weigl (2023).

l'encadrement des aides publiques), elles s'exercent également au travers des règles régissant la commande publique (attribution concurrentielle des contrats, absence de discriminations…) et par celles relatives au commerce extérieur. Les règles de concurrence n'interdisent en rien les coopérations interentreprises mais les conditionnent à la démonstration de gains d'efficacité contrebalançant leurs effets restrictifs (le contrôle des concentrations repose in fine sur la même logique). Elles ne prohibent pas plus les interventions de l'Etat dans les activités économiques. Le principe de neutralité du Traité quant au régime de propriété des entreprises fait qu'un acteur public peut investir dans des activités économiques tant que celles-ci respectent le critère de l'investisseur privé en économie de marché. Si l'intervention ne respecte pas ces critères, elle revient à une aide publique, laquelle peut néanmoins être considérée comme compatible avec le Traité dès lors qu'elle est nécessaire pour corriger une défaillance de marché, qu'elle constitue un instrument adéquat pour l'atteinte de ce résultat et qu'elle est proportionnée.

Sur le domaine du cloud lui-même, les pratiques qu'il serait éventuellement possible de reprocher aux hyperscalers tomberaient naturellement sous le coup des dispositions relatives aux abus de position dominante. Elles ne s'écarteraient donc pas d'autres pratiques connues dans les écosystèmes numériques. Les règles de concurrence pourraient à ce titre suffire à discipliner les acteurs du marché. Cependant, l'exemple même du numérique montre que les règles de concurrence ont pu être vues comme insuffisantes pour traiter de l'ensemble des pratiques potentiellement anticoncurrentielles et notamment d'en dissuader la commission ou de remédier à leurs effets qui peuvent s'avérer irréversibles. Les critiques portent alors sur la durée excessive des procédures, l'absence de remèdes effectifs, le risque trop élevé de faux négatifs (du fait des règles applicables en termes de standard et de charge de la preuve…).

S'ajoutent comme nous l'avons vu *supra* pour le cas spécifique du cloud des difficultés additionnelles portant sur la définition des marchés pertinents et sur la structure oligopolistique du marché. Cette structure oligopolistique peut faire obstacle à la mise en œuvre de remèdes (s'ils sont désirables) correspondant, certes imparfaitement, à ceux qui pourraient procéder d'une activation de la théorie des facilités essentielles, laquelle suppose une garantie d'un accès dans des conditions techniques et tarifaires raisonnables, équitables et non discriminatoires.

La loi sur les marchés numériques (DMA[39]) vise à pallier ces difficultés[40]. Elle a un impact potentiel sur le secteur du cloud (si les oligopoleurs en cause sont qualifiés de contrôleurs d'accès) au moins sur trois points. Le premier point porte sur l'interdiction faite aux entreprises en cause d'utiliser les données collectées par l'activité des firmes utilisatrices de leurs services pour développer des produits concurrents[41]. Le deuxième point tient à des obligations en termes d'interopérabilité[42]. Le troisième point consiste en des obligations en matière de portabilité des données[43]. Ainsi trois dimensions sont à prendre en considération : la limitation de l'avantage

[39] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[40] L'article 2 du DMA intègre les services d'informatique en nuage dans les services de plateformes essentiels sur lesquels porte la législation (aux côtés des services d'intermédiation en ligne, des moteurs de recherche, des réseaux sociaux, des systèmes d'exploitation…).

[41] Voir le considérant 48 du DMA : « En ce qui concerne les services d'informatique en nuage, l'obligation de ne pas utiliser les données des entreprises utilisatrices devrait s'étendre aux données fournies ou générées par les entreprises utilisatrices dans le cadre de leur utilisation du service d'informatique en nuage du contrôleur d'accès, ou par l'intermédiaire de sa boutique d'applications logicielles qui permet aux utilisateurs finaux des services d'informatique en nuage d'accéder aux applications logicielles ».

[42] Le considérant 57 du DMA insiste sur la finalité des exigences d'interopérabilité en termes de prévention de phénomènes de verrouillages concurrentiels si un opérateur de cloud propose des services aval qu'il peut lier ou imposer au détriment des services tiers : « i les doubles rôles sont exercés d'une manière qui empêche d'autres fournisseurs de services ou de matériel informatique d'avoir accès dans les mêmes conditions aux mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées par le contrôleur d'accès dans le cadre de la fourniture de ses propres services ou matériel informatique complémentaires ou d'appui, la capacité d'innovation de ces autres fournisseurs et le choix des utilisateurs finaux pourraient s'en trouver grandement compromis. Les contrôleurs d'accès devraient donc être tenus d'assurer, gratuitement, une interopérabilité effective avec les mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de ses propres services et matériel informatique complémentaires et d'appui, ainsi que l'accès, aux fins de l'interopérabilité, à ces caractéristiques. Un tel accès peut également être exigé par des applications logicielles liées aux services concernés fournis conjointement au service de plateforme essentiel ou à l'appui de celui-ci afin de développer et offrir effectivement des fonctionnalités interopérables avec celles proposées par les contrôleurs d'accès. Ces obligations ont pour objet de permettre à des tiers concurrents de s'interconnecter, au moyen d'interfaces ou de solutions similaires, aux caractéristiques concernées de manière aussi effective que pour les propres services ou matériel informatique du contrôleur d'accès ».

[43] Le considérant 59 du DMA astreint le contrôleur d'accès à des obligations particulières en termes de portabilité : « Les contrôleurs d'accès bénéficient d'un accès à de grandes quantités de données qu'ils collectent lorsqu'ils fournissent des services de plateforme essentiels, ainsi que d'autres services numériques. Afin d'empêcher les contrôleurs d'accès de nuire à la contestabilité des services de plateforme essentiels, ou au potentiel d'innovation d'un secteur numérique dynamique, en limitant le changement de plateforme ou le multihébergement, il convient d'accorder aux utilisateurs finaux, ainsi qu'aux tiers autorisés par un utilisateur final, un accès effectif et immédiat aux données qu'ils ont fournies ou qui ont été générées par leur activité sur les services de plateforme essentiels concernés du contrôleur d'accès. Les données devraient être reçues dans un format permettant qu'elles soient immédiatement et effectivement consultées et utilisées par l'utilisateur final ou le tiers concerné autorisé par l'utilisateur final à qui elles sont transmises. Les contrôleurs d'accès devraient également veiller, au moyen de mesures techniques appropriées et de haute qualité, telles que des interfaces de programmation, à ce que les utilisateurs finaux ou les tiers autorisés par les utilisateurs finaux puissent librement transférer les données en continu et en temps réel. Cela devrait également s'appliquer à toutes les autres données, à différents niveaux d'agrégation, nécessaires pour permettre effectivement cette portabilité. Pour éviter toute ambiguïté, l'obligation faite au contrôleur d'accès d'assurer la portabilité effective des données en vertu du présent règlement complète le droit à la portabilité des données prévu par le règlement (UE) 2016/679. Faciliter le changement de plateforme ou le multihébergement devrait ensuite permettre d'élargir le choix offert aux utilisateurs finaux et encourage les contrôleurs d'accès et les entreprises utilisatrices à innover ». Ces exigences en termes de portabilité sont donc directement reliées à la question de la possibilité dans notre domaine de mettre en œuvre des stratégies multiclouds.

lié à un accès asymétrique aux données, le renforcement des capacités de multi-hébergement et la limitation des barrières à la sortie pour contrecarrer l'étanchéité croissante des silos verticaux constitués par chacun des écosystèmes.

La logique du DMA repose donc sur la préservation de deux éléments essentiels dans l'économie numérique : la contestabilité des positions (préserver une possibilité de concurrence inter-écosystèmes) et la loyauté de la concurrence (garantie d'une concurrence à égalité des armes intra-écosystème). Il se distingue des règles de concurrence en ce qu'il n'implique pas une analyse contradictoire des effets des pratiques mises en œuvre par un opérateur dominant sur un marché donné, il fait peser des obligations et des interdictions 'per se' aux entreprises qualifiées de contrôleur d'accès.

Le DMA n'est pas le seul texte de nature « réglementaire », c'est-à-dire directement applicable, à la différence d'une directive qui doit être transposé dans les droits internes de chaque état membre, élaboré par la Commission qui peut trouver des éléments applicables aux problématiques cités supra sur le cloud. La question du traitement des données est centrale dans le RGPD[44] et celle des déséquilibres contractuels déterminante dans le Règlement P2B[45].

Cependant le fonctionnement des services cloud va être significativement affecté par le Data act dont la cinquième version a été rendue publique en février 2023[46]. Celui-ci devrait imposer des exigences bien plus significatives en termes de portabilité des données. Le projet de Data act est intéressant pour notre propos à plusieurs égards. Premièrement, il porte explicitement un projet de souveraineté numérique dans les domaines du cloud et des services de traitement des données en périphérie du cloud.

Comme mentionné *supra*, les problématiques ne sont pas spécifiques aux services d'infonuagiques mais doivent être replacées dans le cadre des questions plus générales liées aux écosystèmes numériques et à l'importance de la donnée dans le fonctionnement de ces derniers. Le contrôle sur les données revêt une importance spécifique pour la conquête et la préservation de positions dominantes au sein des écosystèmes numériques et pour la capacité de pouvoir faire jouer la concurrence entre ces derniers. Ce caractère déterminant de la donnée est à remettre en perspective avec le développement des logiciels prédictifs basés sur

[44] Règlement 2016/679 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, 27 avril 2016
[45] Règlement 2019/1150 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, 20 juin 2019
[46] Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

l'intelligence artificielle et l'explosion en cours des flux de données au fil du développement de l'internet des objets.

Il s'agit donc comme cela est mentionné dans l'exposé des motifs du projet de Data act d' « équilibrer le flux et l'utilisation des données tout en préservant un haut degré de protection de la vie privée, de sécurité et d'éthique[47] ». Au-delà des normes liées aux données sensibles, il s'agit de renforcer le pouvoir des entreprises sur leurs données (i.e. leur souveraineté liée aux données) en viabilisant les stratégies multiclouds en complétant significativement les obligations posées par le DMA en termes de portabilité des données et d'interopérabilité des services cloud.

Le Data act reprend en effet les garanties du DMA quant à la question d'utilisation des données de façon contraire aux intérêts de la firme dépendante tout en élargissant considérablement le périmètre : « De surcroît, le détenteur de données ne devrait utiliser aucune donnée générée par l'utilisation du produit ou du service lié afin d'obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation d'une quelconque autre manière que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale de l'utilisateur sur les marchés où celui-ci est actif » (§25). Cette disposition s'appliquerait particulièrement dans le cas où l'opérateur de services cloud peut être un concurrent des entreprises utilisatrices de ses services (§29). Il s'agit du cas couvert par la notion de rôle dual des plateformes, en d'autres termes d'intégration verticale. Disposer d'un avantage informationnel sur ses concurrents facilite les stratégies d'éviction par des stratégies d'auto-préférence[48].

Les propositions en termes de portabilité et d'interopérabilité visent à la fois à faciliter le recours aux services de traitement des données à la périphérie (§69), c'est-à-dire au edge computing[49], et la mobilité d'un cloud à l'autre (§70). Il s'agit dès lors de développer des obligations réglementaires palliant les limites de l'autorégulation et l'absence de standard technique.

Le Data act peut aller bien plus loin que les obligations inscrites dans le DMA. Son §72 propose notamment d'imposer aux opérateurs de faciliter le passage d'un service de cloud à un autre en

[47] Orientations politiques pour la Commission 2019-2024, Ursula von der Leyen, 16 juillet 2019.
[48] Voir les engagements proposés par Amazon et rendus obligatoires par la Commission en décembre 2022. Sur les stratégies d'auto-préférence, voir Bougette et al. (2022).
[49] « La capacité des clients de services de traitement de données, y compris de services en nuage et de services à la périphérie, de passer d'un service de traitement de données à un autre, tout en maintenant une fonctionnalité minimale du service, est une condition essentielle pour un marché plus concurrentiel, avec des barrières à l'entrée moins élevées pour les nouveaux fournisseurs de services » (§69).

permettant de transmettre les actifs numériques dont les données à un format permettant une équivalence fonctionnelle. Le droit de transfert doit également porter sur les métadonnées générées par l'utilisation du service.

L'objectif tel que défini au §76 du projet est de permettre « un environnement en nuage multifournisseur continu ».

Ces différentes initiatives réglementaires visent à construire un cadre permettant de concilier les objectifs de sécurité à la collecte et au traitement des données et la préservation des conditions d'une concurrence loyale dans le domaine numérique avec les gains d'efficience qui sont liés au développement des écosystèmes numériques. Quand on se penche sur le cas spécifique du cloud, la logique est celle d'un manque de confiance par rapport aux possibilités d'autorégulation des acteurs ou de régulation par les incitations concurrentielles.

La question du pouvoir de régulation privée des 'plateformes' et la difficulté de faire jouer la concurrence entre les différents écosystèmes du fait des phénomènes de verrouillage sont centrales (Marty, 2020). Il s'agit donc comme nous l'avons vu supra de prévenir les effets de forclusion et des possibilités de dépendance économique et technologique qui en découlent. Dans le domaine non économique le niveau de sécurité garanti pour les données et les applications peut être insuffisant ; dans le domaine économique, la possibilité d'abus et donc de dommages concurrentiels (potentiellement irréversibles) n'est pas prévenue par les risques de voir les utilisateurs des différents services se reporter vers une offre alternative en cas de dissatisfaction. A ce titre, la question des barrières à la sortie est déterminante (dans ses volets de réversibilité et transférabilité). L'interopérabilité des cloud et la portabilité des données sont donc des variables essentielles pour la mise en œuvre de stratégies multiclouds, de politiques de cloud hybrides ou encore de mise en concurrence des différents cloud. La standardisation technique pourrait jouer ce rôle ; il est pris indirectement en charge par certaines des provisions contenues dans le projet de Data Act.

Il est à noter que les efforts de la Commission en matière de règlementation a un effet qui peut potentiellement se diffuser à d'autres espaces géographiques, et ce pour plusieurs raisons. Premièrement, les règles européennes revêtent également un caractère d'extraterritorialité. Les entreprises doivent les appliquer pour accéder au marché intérieur. Deuxièmement, ces mêmes entreprises ont tout intérêt à orienter leur stratégie de conformité vers la norme la plus exigeante. Troisièmement, un effet d'exemplarité est à l'œuvre par rapport aux réglementations que

peuvent être amenés à concevoir d'autres espaces géographiques (Cervi, 2022). Nous retrouvons ici la notion d'effet bruxellois (Bradford, 2020).

2b) Les stratégies relevant de la politique industrielle

Au-delà des interventions réglementaires et de l'utilisation des politiques de concurrence, l'action de l'UE peut passer par des politiques industrielles communes. Cette stratégie peut passer par des voies hybrides comme celle du paquet législatif sur les semi-conducteurs[50]. La question est (relativement) distincte de celle de l'infonuagique mais la stratégie repose sur les mêmes fondements : « renforcer la compétitivité et la résilience de l'Europe dans les applications et les technologies des semi-conducteurs ». L'hybridité de la politique tient au fait que le paquet législatif est accompagné d'un programme d'investissements publics et privés. La politique revêt également une dimension 'stratégique' commune à celle décrite supra pour le cloud. Selon les termes mêmes de la Commission : il s'agit de « mettre en place des partenariats internationaux en matière de semi-conducteurs avec des pays partageant les mêmes valeurs ». Au-delà des aspects strictement économiques, sont donc présents les deux dimensions citées supra de la problématique du cloud ; la sécurité par rapport à des intrusions malveillantes qu'elles soient le fait de groupes criminels ou d'états hostiles et la minimisation des vulnérabilités par rapport à la déstabilisation des chaînes d'approvisionnements ou à des actes de guerre hybride émanant desdits états. La solution n'est pas ici à rechercher dans une stratégie autarcique (logique de substitution aux importations ou dans notre cas politique du cloud dans un seul pays[51]) mais dans la gestion des interdépendances avec nos alliés partageant nos valeurs démocratiques et nos intérêts géopolitiques.

La stratégie de la Commission en matière de semi-conducteurs s'inscrit dans le cadre du basculement de notre économie vers une nouvelle ère industrielle dont nous avons déjà dessiné les contours (IA, IoT, informatique quantique…)[52]. Celle menée dans le cloud s'inscrit dans la même logique comme le montre le projet GAIA-X que nous avons abordé supra dans le cadre de la présentation des initiatives franco-allemandes. Ce projet insère la dimension cloud dans

[50] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_fr#investissements-%C3%A0-lappui-du-paquet-l%C3%A9gislatif-sur-les-semi-conducteurs

[51] Une logique de *cloud dans un seul pays* impose de renoncer à des gains d'efficience. L'avantage d'un cloud tient à son homogénéité technique et à la dispersion optimale des données. Pour autant celles-ci sont toujours localisées à proximité de leurs lieux d'utilisation pour limiter les temps de latence.

[52] Il suffit de se reporter au discours d'installation de la présidente de la Commission, Ursula von der Leyen en novembre 2019 ; la stratégie numérique de l'Union passe par la maîtrise de technologies clés et la garantie d'une autonomie pour chacune d'entre-elles.

une perspective plus large, GAIA étant l'acronyme de General Artificial Intelligence Architecture. L'accent est à la fois mis sur le rattrapage mais également sur la définition de normes d'interopérabilité et de standards techniques communs. Cependant, non seulement chaque partenaire européen avait une définition propre des objectifs qu'il était nécessaire de donner à Gaïa mais ceux-ci évoluèrent significativement avec le temps. De la politique industrielle traditionnelle visant à la construction d'une alternative européenne[53], le projet a évolué vers la protection des intérêts des firmes utilisatrices des services. Les entreprises utilisatrices doivent pour bénéficier de services respectant les règles et valeurs de l'UE, dans un cadre non discriminatoire, évitant les phénomènes de capture dans les silos des différents hyperscalers et garantissant les conditions d'une souveraineté numérique (Baur, 2023).

B – Discussion de l'efficacité des politiques publiques engagées

1) Les politiques publiques au regard des trois niveaux de problématiques reliées au cloud souverain

Il ressort des cas présentés supra que les initiatives de la Commission et des Etats-membres, au-delà des différences de formes, visent à faciliter pour les entreprises la mise en œuvre de stratégies multiclouds et pour les administrations la mise en œuvre de stratégie de cloud hybrides. Cependant malgré les points communs à ces différentes optiques (sécurité, portabilité des données, interopérabilité), il convient d'insister sur les spécificités des politiques au regard des trois niveaux d'interrogation : défense, droits fondamentaux et activités de marché.

En matière de défense, la question principale est celle de la résilience et de la minimisation de la vulnérabilité des systèmes. Cette vulnérabilité doit se concevoir au regard des risques de cyberattaques et des risques liés aux composants et aux technologies utilisés. Les équipements utilisés peuvent être liés à des technologies duales et les approvisionnements peuvent exposer à des risques additionnels s'ils reposent sur des partenaires commerciaux peu sûrs en termes de garantie d'approvisionnement ou d'intégrité des composants livrés. La sécurité ne doit en outre pas seulement être envisagée au regard des systèmes publics en eux-mêmes mais également en fonction de leurs interactions avec le comportement des agents et des équipements

[53] Comme le soulignent Codagnone et Weigl (2023, p.2), GAIA X était même présentée en 2019 par le ministère allemand des affaires économiques et de l'énergie comme « a fully self-sufficient cloud computing infrastructure to ensure European Data sovereignty »

informatiques personnels que ces derniers peuvent être amené à utiliser dans le cadre de l'exercice de leurs missions. La compromission de la sécurité peut être liée à ces interactions.

En matière de souveraineté, deux questions peuvent être envisagées. Une première question porte sur la gestion spécifique de données sensibles comme les données de santé[54]. Il s'agit alors de s'interroger sur le type de cloud qui doit être utilisé. Prenons l'exemple du Health Data Hub français. Son hébergement par Microsoft a posé problème[55] dans le contexte notamment de la promulgation du Cloud act américain et de la disparition du Privacy Shield[56]. Son hébergement sur un cloud souverain (ou du moins un cloud labellisé comme un cloud de confiance) est présenté comme nécessaire mais va supposer des délais… au moins ceux nécessaires au développement d'une offre alternative dûment labellisée. Une seconde question porte sur l'extraterritorialité et les conditions d'accès d'états étrangers aux données quelles que soient leurs localisations. Il serait possible de s'interroger dans une perspective de droit comparée sur l'exceptionnalité des capacités d'accès états-unienne en comparaison des règles existantes en France ou au Royaume-Uni (David and Gunka, 2021).

En matière d'activités de marché, enfin, il convient de replacer les initiatives européennes et celles des Etats-membres dans la perspective des finalités attribuées aux règles de concurrence et / ou de règlementation des marchés. Un *continuum* de points d'équilibre peut être dessiné entre la politique de concurrence et la politique industrielle.

Il peut premièrement s'agir de garantir une concurrence par les mérites ; c'est le rôle de l'article 102, si on reprend la grille de lecture de l'AG Rantos dans *Servizio Elettrico Nazionale*[57].

---

[54] La logique de protection des données personnelles sur le cloud portée par les institutions européennes, vise à garantir que dans une logique B2C (Business to Consumers), les valeurs fondamentales de l'Union et ses règles de protection de la vie privée notamment, soient respectées (Aktoudianakis A., 2020).

[55] Le Health Data Hub a retiré provisoirement en janvier 2022 sa demande d'autorisation à la CNIL.
https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

[56] L'arrêt Schrems II de la Cour de la Justice, rendu le 16 juillet 2020, a invalidé la notion de protection équivalente (garantie d'un respect d'exigences substantiellement équivalentes) qui permettait le transfert de données entre l'UE et les Etats-Unis. L'importance de la préservation de l'accès au marché européen conduit les autorités américaines à faire évoluer leur règlementation pour se conformer au niveau de protection requis par l'Union européenne. Un *executive order* a été signé en ce sens par le Président Biden le 7 octobre 2022 à la suite d'un accord politique conclu avec la Commission en mars 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
Notons cependant que l'European Data Protection Board a relevé quelques points de préoccupations sur le sujet dans le cadre d'un avis publié le 23 mars 2023.
Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework
https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

[57] Conclusions de l'AG Rantos, Servizio Elettrico Nazionale SpA,, affaire C-377/20, 9 décembre 2021.

L'éviction des offres concurrentes n'est pas un problème en soi dès lors qu'elle procède d'une efficacité supérieure.

Il peut deuxièmement s'agir de la prévention d'une défaillance structurelle de la concurrence. L'*inception impact assessment* de la Commission européenne de juin 2020 qui annonçait un nouvel instrument concurrentiel qui allait trouver une traduction (partielle) dans le DMA est un bon exemple de cette logique[58]. La spécificité de certains marchés – en l'espèce les marchés numériques – fait que ces derniers se structures en écosystèmes fondés sur un phénomène de dominance forte et durable et sur une capacité de la firme pivot à exercer un pouvoir de régulation privée. Cela pose des questions en termes de contestabilité des positions et de loyauté de la concurrence. Il faut alors des instruments complémentaires à ceux du droit de la concurrence pour corriger ces risques qui ne tiennent pas à un problème d'efficacité mais à une neutralisation des conditions de la concurrence libre et non faussée.

Il peut troisièmement s'agir d'une action visant à garantir la pérennité d'une structure donnée du marché, jugée comme souhaitable à long terme pour que les agents économiques puissent exercer une liberté de choix. Il s'agit d'une approche structuraliste qui va considérer que la position dominante est un problème en elle-même quel que soit son mode d'acquisition et quel que soit son mode d'exercice. Il ne s'agit plus seulement de protéger la concurrence (même malgré elle) mais de protéger les concurrents en ce qu'ils sont tenus pour essentiels à l'exercice de liberté de choix (qui peut être conçue comme un instrument nécessaire pour discipliner les acteurs dominants en rendant l'*exit* possible).

Il peut quatrièmement s'agir d'une protection d'un certain type d'acteurs : des complémenteurs jugés stratégiques (dans le secteur du développement logiciel, des services à l'industrie…) ou des fournisseurs de services cloud locaux.

Il peut cinquièmement s'agir d'une politique industrielle *stricto sensu* qui repose sur une régulation asymétrique de la concurrence au profit d'une firme donnée ou sur un soutien direct à celle-ci.

2) Evaluation de ces différents instruments

Les problèmes que posent les instruments sont croissants en fonction de ce continuum et leur efficacité théorique décroissante.

[58] https://competition-policy.ec.europa.eu/public-consultations/2020-new-comp-tool_en

a) L'application des règles de concurrence

Les problèmes de concurrence dans le numérique n'appellent pas de nouvelles théories de l'abus. Les différentes catégories sont connues. La principale difficulté, qui a été l'une des principales origines de la promulgation du DMA, tient à la difficulté spécifique de mise en œuvre de sanctions dissuasives et de mesures correctives réparatrices. Le point essentiel, qui transparait bien dans le cas du cloud, est lié à la question spécifique des abus de dominance relative et de la question de la loyauté des relations commerciales. En d'autres termes, il s'agit de considérer à la fois le grand droit et le petit droit de la concurrence.

b) Les instruments de régulation sectorielle européenne

La stratégie européenne en matière de données (data package) présentée le 19 février 2020[59] illustre l'importance de l'argument de la souveraineté numérique dans la politique suivie par la Commission, politique qui excède de façon très significative le champ de la concurrence.

Trois points sont à considérer.

Premièrement, l'intense production réglementaire européenne a un coût qui est lié à la complexité des textes (voire à leur mise en cohérence). Ce coût est également un coût en termes de conformité qui est comparativement plus lourd pour les petites firmes que pour les grandes si la réglementation impose des contraintes symétriques (ce qui est le cas du RGPD par exemple).

Deuxièmement, la réglementation peut être très coûteuse pour les opérateurs cloud si un degré élevé d'interopérabilité et de portabilité est imposé et si les conditions de compensation de ces coûts sont imparfaites. Cela peut notamment être le cas en l'état actuel des projets relatifs au Data act.

Troisièmement, les régulations asymétriques peuvent avoir un coût politique. Il est normal de faire peser des obligations particulières sur les *bottlenecks*. Cependant, plusieurs effets potentiellement négatifs sont à considérer. D'abord, imposer des contraintes à des opérateurs peut être de nature à limiter leur capacité à générer des gains d'efficience et à les redistribuer aux consommateurs. Il y a des arbitrages à prendre en considération. Ensuite, les opérateurs 'dominants' sont actuellement des opérateurs exclusivement américains. La régulation

[59] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

asymétrique peut dès lors être vue comme discriminatoire par notre partenaire. Il ne s'agit pas d'une mesure protectionniste contre un partenaire commercial (parfois agressif) couplé avec une certaine permissivité vis-à-vis d'opérateurs tiers mais le reflet des positions dominantes (au moins relatives) de l'heure.

c) Quelles évaluations des mesures relevant de la politique industrielle ?

La constitution d'éventuels champions européens, si elle devait s'avérer possible, ne devrait pas seulement se concevoir dans le cadre d'une rivalité vis-à-vis d'un concurrent économique, les Etats-Unis, mais également dans celui d'une rivalité stratégique dans une ère marquée par une compétition entre puissances majeures voire de montée d'agissements hostiles de la part de puissances régionales. Si nous pouvons craindre des premiers des stratégies d'instrumentalisation du droit à des fins unilatérales et opportunistes (*lawfare*), il est nécessaire de se parer contre les agressions directes ou hybrides des seconds, notamment dans la sphère numériques[60].

Quatre niveaux de politique industrielle orientée vers le cloud peuvent être distingués. Leurs effets potentiellement négatifs vont croissant.

Le premier niveau est l'encouragement à la recherche-développement et à l'adoption d'outils permettant potentiellement de limiter le pouvoir économique des hyperscalers et de leur capacité à accéder aux données des firmes, des personnes physiques et des administrations européennes. Il s'agit des solutions de cloud hybrides, des possibilités de diviser certaines tâches entre plusieurs cloud et surtout des technologies permettant de mettre en œuvre un edge computing ou d'utiliser des stratégies de conteneurisation[61].

Le deuxième niveau est celui des standards techniques, des normes et des labels. Le risque de distorsion est limité tout comme les risques d'entrave au développement technique mais il ne saurait pour autant être passé sous silence. Une mauvaise norme peut être sélectionnée à tort. Les entreprises européennes peuvent également capturer la réglementation pour imposer des standards qui leur sont favorables mais qui pourraient entraver le progrès technique ou les

[60] Se reporter notamment à l'actualisation stratégique 2021 publiée par le ministère de la Défense. https://www.defense.gouv.fr/sites/default/files/dgris/REVUE%20STRAT%202021%2004%2002%202021%20FR.pdf

[61] La conteneurisation consiste à rassembler le code du logiciel et tous ses composants (bibliothèques…) de manière à les isoler dans leur propre « conteneur ». L'application peut alors fonctionner quel que soit l'environnement (en termes de système d'exploitation par exemple). Ainsi, la stratégie multi-clouds est plus aisée à mettre en œuvre, la portabilité du conteneur est alors facile à assurer (voir Sultan et al., 2019).

protéger indûment de la concurrence. Le standard technique ou le label doit être accessible à tous les acteurs qui peuvent s'y conformer.

Le référentiel SecNumCloud développé par l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information) fait sens dans ce cadre[62]. Il s'agit de définir un référentiel d'exigences que tout prestataire de services informatiques doit respecter pour être labellisé. Le cloud de confiance doit respecter des exigences en termes de localisation des serveurs, d'habilitation des personnels, de normes techniques etc… (Luzeaux, 2022). Dans le domaine de la souveraineté déclinée sous son volet stratégique, l'article 22 de la Loi de Programmation Militaire de 2013 impose des dispositifs spécifiques pour les firmes exploitant des systèmes considérés comme d'importance vitale[63].

Il convient cependant de relever – en suivant à nouveau le document de consultation de l'Autorité de la concurrence – que les stratégies de labellisation peuvent également avoir pour effet de figer les positions de marché. En effet, dans le cadre de la labellisation comme cloud de confiance, les entreprises de services informatiques susceptibles de mettre en place les stratégies de conformité ont intérêt à développer des partenariats avec les hyperscalers comme nous le verrons infra. Ces partenariats supposent l'accès au code source et la réalisation d'investissements spécifiques. Il est donc nécessaire de constituer des sociétés communes et l'équilibre du marché va naturellement vers des partenariats exclusifs. A l'instar des conclusions des modèles habituels d'économie industrielle, les entreprises actives sur ce marché ont intérêt de nouer de tels partenariats avec les hyperscalers. Les investissements nécessaires et les coûts liés à la conformité peuvent donc renforcer verticalement les positions actuelles sur la chaîne de valeur.

Le troisième niveau d'intervention correspond à l'utilisation de la commande publique comme vecteur de politique industrielle. Elle constitue traditionnellement un de ses outils privilégiés. L'exemple des Etats-Unis est le plus significatif pour illustrer sa portée[64]. Un executive order américain de janvier 2021 établit que le "government should […] procure goods […] materials, and services, from sources that will help American businesses to compete in strategic industries[65]". L'achat public n'a pas qu'une fin de promotion de la base industrielle et

[62] Ce standard doit être appliqué dès que la personne publique manipule des données d'une sensibilité particulière. Ces données doivent alors être protégées contre toute possibilité d'accès sur la base de règlementations non européennes. Par exemple, pour les données de santé, il est nécessaire que les fournisseurs de services clouds soient titulaires d'une habilitation adéquate d'hébergeur de données de santé.
[63] Loi n°2013-1168 du 18 décembre 2013.
[64] Voir l'Inflation Reduction Act, H. R. 5376, promulgué le 16 août 2022.
[65] Executive order n°14005, 86 FR 7475, 25 January 2021.

technologique domestique, il peut également avoir une visée défensive en excluant des fournisseurs dont les produits pourraient être les vecteurs de menaces stratégiques. Par exemple la FCC américaine a entamé des contrôles sur des composants fournis par des entreprises publiques chinoises[66] et les gouvernements australiens et américains ont banni l'entreprise Huawei de leurs infrastructures 5G (Mitchell et Samlidis, 2021). Des avantages donnés à des opérateurs européens peuvent se justifier en regard de la présence de risques souverains ou de concurrence déloyale liée à des pratiques de dumping d'états étrangers ou d'absence de réciprocité. Pour autant des risques de capture par les firmes européennes ne doivent pas être niés. La protection contre les concurrents étrangers réduit drastiquement les incitations à l'innovation et a un inéluctable effet inflationniste. Il faut qu'il y ait une concurrence interne suffisante pour limiter les effets négatifs. Cela est relativement le cas aux Etats-Unis mais ce point même est de plus en plus contesté. On retrouve les problèmes classiques de la commande publique. Le primat de la concurrence en la matière a l'avantage de garantir (s'il n'y pas d'ententes) l'efficacité économique de l'acquisition (en termes de *value for money*). Il permet également d'accroître les garanties de régularité de la commande publique en limitant la marge de discrétion de l'acheteur public[67]. Introduire des objectifs additionnels permet de faire des arbitrages dont les termes sont opaques. La redevabilité de la commande publique peut y perdre très significativement. L'intensité et le coût même des soutiens publics sont alors encore moins aisés à mesurer que dans le cas de subventions publiques directes.

Le quatrième niveau correspond à la mise en œuvre d'une politique industrielle telle que celles développées dans l'après-guerre. Il s'agit de la politique des champions nationaux et de sa traduction au niveau européen. Ces politiques sont déjà très difficiles à mettre en œuvre de façon efficace pour un Etat membre. Le pouvoir politique doit pouvoir choisir l'entreprise qui sera la cheffe de file de sa politique. Il doit accepter de lui transférer des ressources publiques et doit prendre en considération le risque de capture. Il doit aussi prendre en considération les risques d'échecs qui sont d'autant plus élevés que des offres concurrentes existent déjà et il doit prendre en compte les phénomènes possibles d'escalade des investissements (i.e. de dilapidation de ressources publiques). Si la politique industrielle ne porte pas sur un acteur en particulier le risque est celui d'un vain saupoudrage. Quand bien même la bonne technologie et la bonne entreprise seraient-elles sélectionnées, reste la question de la capacité de l'Etat membre de disposer de suffisamment de ressources pour rendre son opérateur concurrentiel par rapport

[66] https://www.fcc.gov/document/fcc-scrutinizes-four-chinese-government-controlled-telecom-entities

[67] Pour une analyse des risques discrétionnaires liés à la pluralité d'objectifs assignés à la commande publique, voir Blanchard et Tirole (2021).

à ses rivaux internationaux. Les programmes européens semblent être la clé pour répondre à ces limites. Cependant la multiplication des programmes nommés « l'Airbus *de tel ou tel secteur* » montre que le succès n'est pas assuré. Les programmes en coopération internationale peuvent disposer de l'échelle nécessaire mais voient leur gestion et même leurs performances intrinsèques hypothéqués par les arbitrages entre états participants qui ne se font pas toujours dans le sens de l'intérêt commun et laissent une place parfois préjudiciable aux arbitrages politiques. Cependant, le succès des initiatives européennes ne serait passer que par la seule édiction de réglementations…

Il apparaît que l'évolution des politiques européennes vers des politiques de certifications conduit à des équilibres à la fois plus viables et plus prometteurs que l'ambition de construire *ex nihilo* des champions industriels. Se passer des infrastructures développées par les *hyperscalers* peut être vu comme déraisonnable en termes techniques et financiers. Répliquer leurs investissements passés est hors de portée en termes budgétaires. Qui plus est la performance des services proposés est basée sur les apprentissages algorithmiques réalisés en continu et sur le capital humain dont disposent ces entreprises. Les avantages liés au recours à ces clouds tiennent en outre comme mentionné *supra* à la flexibilité et à la scalabilité qu'ils offrent aux entreprises utilisatrices et à la performance des outils logiciels liés.

La solution est donc plus celle d'un cloud sécurisé (ou de confiance) qu'un cloud souverain. Il s'agit donc de privilégier le traitement des données à la marge du cloud des hyperscalers et d'un stockage sécurisé (en termes de cryptage) sur des infrastructures 'privées', c'est-à-dire des infrastructures privatisées mises en place au sein du cloud des hyperscalers. Il s'agit alors de viser deux objectifs principaux. Le premier est de maintenir une capacité à utiliser plusieurs cloud ou du moins à rester en mesure de passer d'un fournisseur de services à un autre sans risques majeurs au point de vue technique et sans coûts prohibitifs. Il s'agit également de se doter des garanties adéquates pour la sécurisation des données et la résilience des services. Le concept de souveraineté numérique appliquée au cloud peut alors se décliner selon trois niveaux dont le degré d'exigence est de plus en plus élevé[68].

Le premier niveau, celui de la souveraineté liée aux données, est celui de l'utilisation d'une multiplicité de clouds publics accompagnée des garanties idoines en matière de cryptage des données, de localisations des serveurs et de constitution des équipes. Un ensemble de

[68] Nous reprenons ici la classification proposée durant la conférence organisée à Aix-en-Provence le 6 mars 2023 par Romain Deslorieux (voir note 1, *supra*).

technologies d'accroissement de la sécurité (*sovereign enhancement technologies*) peut alors être développée pour permettre une utilisation sécure des services cloud proposés par les hyperscalers. La dimension technique est ici liée à la sécurité des données et au contrôle sur ces dernières notamment en termes d'accès[69].

Le second niveau correspond à une souveraineté opérationnelle passant par la mise en place de cloud de confiance. La dimension technique en jeu est alors celle de la certification des mesures de sécurité prises par l'opérateur. Le cloud utilisé est toujours un cloud public mais une surcouche logicielle joue le rôle d'une protection.

Le troisième niveau est celui de la souveraineté technique. Il s'agit alors d'une capacité à développer son propre cloud ou du moins à opérer un cloud avec ses propres logiciels et de mettre en place l'intégralité des technologies nécessaires. Les stratégies de cloud privé et de multicloud sont alors possibles tout comme le recours à des technologies d'edge computing ou de conteneurisation.

Cette dernière solution est la plus satisfaisante dans une optique de souveraineté conçue comme une garantie de contrôle et de résilience. Elle ne permet pas cependant de tirer profit des investissements déployés et des capacités développées par les hyperscalers. Elle concerne plus à ce titre les activités de défense. Le point d'équilibre est donc plus à rechercher dans les différents partenariats mis en place entre des opérateurs européens et des hyperscalers, à l'instar des sociétés communes entre Thales et Google (SENS[70]), CapGemini et Orange avec Microsoft (Bleu[71]), Atos avec Amazon (en octobre 2022), Dassault-Systèmes et Bouygues avec Outscale (en octobre 2022). A titre d'exemple, dans le cas de SENS, la majorité des parts de la société commune est détenue par Thales lequel doit accéder au code de son partenaire pour pouvoir satisfaire aux exigences de l'ANSSI en termes de conformité[72] pour obtenir la certification de cloud de confiance.

GAIA-X témoigne également d'un même schéma d'évolution allant d'une ambition de développement d'un cloud alternatif à la mise en place d'un cloud sécurisé reposant sur les offres commerciales des hyperscalers. Comme le note Baur (2023, p.15) : "[GAIA-X] is not meant to replace hyperscalers like Amazon Web Services, Microsoft, or Google. Instead, it

[69] Ces exigences de cryptage des données apparaissent notamment aux articles 4 et 32 du RGPD et à l'article 9 du Règlement DORA.
[70] Communiqué de presse du 6 octobre 2021
[71] Communiqué de presse du 22 juin 2022
[72] Absence de *back doors* par exemple.

intends to create a platform where European companies and users can book and connect to cloud services adhering to European regulation. This standardisation and interoperability are meant to prevent lock-in effects (i.e. the dependence on one specific cloud environment)". La standardisation, l'interopérabilité et la portabilité jouent donc un rôle à la fois politique (en ce qu'elles portent des valeurs et offrent des garanties) et un rôle économique (permettant un marché fluide et prévenant les situations de concurrence faussée et les phénomènes d'exercice d'abus de pouvoir économique).

L'hybridité des solutions permet de concilier la performance en termes économiques et le degré de contrôlabilité et de résilience à même de satisfaire l'exigence de souveraineté.

La logique de la souveraineté conçue comme la préservation d'une capacité de contrôle, d'action autonome et de maîtrise des vulnérabilités à des fins de résilience peut se retrouver dans de nombreuses initiatives européennes lesquelles dessinent in fine un modèle spécifique et adapté aux enjeux du cloud. La logique est celle d'une régulation déléguée (Kirat et Marty, 2015) qui fait reposer la certification sur la mise en place d'une politique de conformité reposant sur des mesures de gouvernance interne et de due diligence en matière d'identification et de gestion des risques. Cette logique est à l'œuvre dans le cadre du chapitre 5 du règlement européen DORA, relatif à la gestion des risques liés aux prestataires tiers de services TIC. Ce Règlement (Digital Operational Resilience of the Financial Sector[73]) est entré en vigueur en janvier 2023. Cette même logique s'applique dans le cadre de la directive NIS 2 (Network and Information Security) relative à la cybersécurité dans l'espace européen qui a été publiée le 27 décembre 2022[74]. La logique est donc celle d'une double exigence de transparence et de due diligence qui fait écho aux exigences posées par la loi pour une République Numérique de 2016[75].

L'action des pouvoirs publics européen est progressivement passée d'une logique de champion national (pouvant être conçue dans une perspective défensive ou offensive) à une logique

[73] Le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique (dit règlement DORA). Ce dernier règlement porte sur la résilience opérationnelle des services numériques dans le secteur financier reliés au cloud. Il impose la mise en œuvre de procédures d'évaluation des risques et de mesures adéquates pour garantir la résilience des services. Son périmètre d'application tient aux entreprises actives dans le secteur financier et aux prestataires intervenant pour celles-ci. Son entrée en vigueur est prévue pour janvier 2025.

[74] La nouvelle directive adopte une démarche basée sur les risques pour définir les obligations pesant sur les fournisseurs de services et couvre désormais les entités publiques.
Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

[75] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

d'action répondant à un modèle de constitutionnalisme numérique (Codagnone et Weigl, 2023) visant à garantir à la fois une concurrence à égalité des armes dans la sphère économique et le respect de valeurs fondamentales dans les rapports entre les firmes de la donnée d'une part et les individus et les institutions publiques d'autre part. Cette ambition peut paraître comme plus raisonnable à plusieurs égards. Premièrement, elle fait écho à l'impossibilité d'un rattrapage dans un secteur caractérisé par de très forts coûts fixes et des avantages liés à une arrivée précoce sur le marché. Deuxièmement, elle répond aux problèmes auxquels la politique européenne est confrontée, en l'espèce la limitation des moyens budgétaires mobilisables et les difficultés de coordination entre les états membres dont les intérêts et les conceptions peuvent être hétérogènes sinon conflictuelles. Garantir des conditions d'une concurrence respectueuse des intérêts légitimes des entreprises européennes utilisatrices des services de cloud (qui ne sont pas que des PME) est à la fois consensuel et ne se heurte pas aux écueils habituels associés aux politiques industrielles. Troisièmement, cette politique pourrait être la plus adaptée dans le cadre de l'évolution même des technologies liées au cloud vers des possibilités accrues de traitement des données à la périphérie du réseau. Mettre l'accent sur les protocoles d'interopérabilité, favoriser les stratégies multiclouds, contraindre à la portabilité des données pourrait alors être un instrument déterminant pour permettre aux firmes européennes de bénéficier des services rendus par les hyperscalers sans entrer dans des relations asymétriques concurrentiellement dangereuses. Comme le note Luzeaux (2022, p.19), l'accent passe de l'objet technique lui-même à ses conditions d'utilisation.

Conclusion

La question du cloud souverain illustre la fin d'une possible naïveté initiée dans les années 1990 à l'heure où l'on croyait à la fin de l'histoire, à la pacification des relations internationales par le doux commerce ou encore à la déclaration d'indépendance de l'Internet[76]. La rivalité inter-étatique est revenue. La concurrence inter-entreprises peut avoir sous certaines conditions des effets destructeurs qu'il s'agit de gérer (Ezrachi et Stucke, 2020). De la même façon des états alliés peuvent nous livrer du moins une guerre économique, du moins adopter des attitudes hostiles dans la sphère commerciale, au moyen parfois d'une instrumentalisation du droit. Quant aux états hostiles, la possible commission d'actes relevant d'une guerre hybride ne constitue pas une vue de l'esprit. L'U.E. et ses états membres ont raison de se saisir de ces

[76] Voir la déclaration d'indépendance de l'internet (Barlow, 1996)

questions. L'Union n'est pas qu'une zone de libre-échange mais un projet politique portant des valeurs propres et incarnant des intérêts géopolitiques évidents. L'U.E. n'est pas réductible à sa politique de concurrence et son histoire même (cf. la Communauté Européenne du Charbon et de l'Acier) montre deux choses. Premièrement, la concurrence n'est pas seulement une fin comme on pourrait le considérer dans une optique ordolibérale mais aussi un moyen. Un moyen de construction de l'Union et de promotion de sa compétitivité économique. Deuxièmement, de 1950 au milieu des années 1980, le projet européen était vu comme devant reposer sur un équilibre entre concurrence et politique industrielle (Warlouzet, 2008).

Cet équilibre n'a pas vu le jour. Il s'agit de le faire advenir mais surtout sans se renier et sans oublier que la concurrence demeure essentielle comme contrepouvoir. Il est de son rôle de protéger les consommateurs et les entreprises contre les pratiques anticoncurrentielles mais également contre toutes les pratiques de concurrence déloyale. Le cas des abus de dépendance économique est symptomatique des problématiques du cloud. Nous pourrions également y ajouter dans une perspective de commerce international des questions de réciprocité et d'absence de distorsions ou de mise en œuvre de pratiques hostiles dans les champs économiques, politiques et sécuritaires.

Les objectifs du projet de Data act participent de cette logique : faciliter l'accès, la portabilité et l'utilisation des données par les consommateurs et les entreprises, tout en préservant les incitations aux investissements et à l'innovation des opérateurs de services cloud ; développer les solutions techniques permettant un usage plus large aux techniques d'*edge computing,* élaborer des normes exigeantes d'interopérabilité et enfin mettre en place des garanties contre les possibilités de transfert illicite de données. Il ne s'agit pas de substituer aux solutions d'infonuagiques actuelles mais de renforcer la souveraineté des acteurs économiques, des pouvoirs publics et des citoyens de l'Union.

Références

Aktoudianakis A., (2020), "Fostering Europe's Strategic Autonomy. Digital sovereignty for growth, rules and cooperation", *European Policy Centre – Konrad Adenauer Stiftung,* December.

Barlow J.P., (1996), *A declaration of independence of cyberspace*

Baur A., (2023), “European Dreams of the Cloud: Imagining Innovation and Political Control”, *Geopolitics*, forthcoming.

Benzina K., (2019), “Cloud Infrastructure-as-a-Service as an Essential Facility: Market Structure, Competition, and the Need for Industry and Regulatory Solutions”, *Berkeley Tech. LJ*, 34, p.119 et s.

Blanchard O. and Tirole J., (2021), *The Major Future Economic Challenges*, report of the international commission mandated by the President of the French Republic, France Stratégie, Paris.

Bômont C., (2018), “Maîtriser le cloud computing pour assurer sa souveraineté », *in* Taillat S., Cattaruzza A. et Danet D., eds, *La cyberdéfense*. *Politiques de l’espace numérique,* Armand Colin, pp.91-98

Bômont C. et Cattaruzza A., (2020), « Le cloud computing : de l’objet technique à l’enjeu géopolitique. Le cas de la France », *Hérodote*, 2020/2, n°177-178, pp.149-163.

Bougette P., Gautier A. and Marty F., (2022), "Business Models and Incentives: For an Effects-Based Approach of Self-Preferencing?", *Journal of Competition Law and Practice*, 13(2), pp.136-143, March.

Bradford A., (2020), *The Brussels Effect. How the European Union Rules the World*, Oxford University Press.

Burwell F. and Propp K., (2020), “The European Union and the Search for a Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World”, *Issue Brief Atlantic Council*, June.

Cervi G.V., (2022), “Why and how does the EU rule the global digital policy: an empirical analysis of EU regulatory influence in data protection laws”, *Digital Society*, 1(18).

Chen A., (2021), *The Cold Start Problem: How to Start and Scale Network Effects*, New York, Harper Business

Codagnone C. and Weigl L., (2023), “Leading the Charge on Digital Regulation: The More, the Better, or Policy Bubble?”, *Digital Society*, 2023(2-4), pp.1-25.

Danet D. et Desforges A., (2020), « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géostratégiques », *Hérodote*, 2020/2, n°177-178, pp.179-195.

Davis F.T. et Gunka C., (2021), « Perquisitionner les nuages – Cloud Act, souveraineté européenne et accès à la preuve dans l’espace pénal numérique », *Revue critique de droit international privé*, 2021/1, n°1, pp.43-66

Ezrachi A. and Stucke M., (2020), *Competition Overdose: How Free Market Mythology Transformed Us from Citizen Kings to Market Servants*, Harper Collins.

Gros P., (2019), « Le « cloud tactique », un élément essentiel du système de combat aérien futur », *Défense et industrie*, Fondation pour la Recherche Stratégique, n°13, juin, pp.1-9.

Hubert P. et Marty F., (2019), *La concurrence au secours de l'économie numérique : conséquences attendues pour le consommateur, regards croisés*, Fauves éditions, Paris.

Iansiti M. and Lakhani K., (2020), *Competing in the Age of AI. Strategy and Leadership When Algorithms and Networks Run the World*, Harvard Business Review Press.

Jin C., Peng S. and Wang P., (2022), "Sticky Consumers and Cloud Welfare", *Working paper*, https://chuqingjin.github.io/files/cloud_inertia_ChuqingJin.pdf

Kirat T. and Marty F., (2015), "The Regulatory Practice of the French Financial Regulator, 2006-2011 – From Substantive to Procedural Financial Regulation", *Journal of Governance and Regulation*, volume 4 - 2015, Issue 4 (continued – 4), pp.441- 450.

Limonier K., (2018), « Des cyberespaces souverains ? Le cas de la Russie », *in* Taillat S., Cattaruzza A. et Danet D., eds, *La Cyberdéfense - Politique de l'espace numérique* Armand Colin, pp.123-129.

Luzeaux D., (2022), "Cloud Souverain : souveraineté et résilience, ou confiance ? », *Revue Défense Nationale*, n°855, décembre, pp.14-21.

Marty F., (2012), "Concurrence et politique industrielle : analyse de logiques distinctes", *in* de Beaufort V. (s.d.), *Entreprises stratégiques nationales et modèles économiques européens*, Bruylant, Bruxelles, octobre 2012, pp.131-153.

Marty F., (2019), "Plateformes de commerce en ligne et abus de position dominante : réflexions sur les possibilités d'abus d'exploitation et de dépendance économique", *Revue Juridique Thémis de l'Université de Montréal*, volume 53, pp. 73-104.

Marty F., (2020), « Accès aux données, coopétition intra-plateforme et concurrence inter-plateformes numériques », *Revue d'économie industrielle*, 169, 2020-1, pp. 221-246

Marty F. and Mouton J., (2022), « Ecosystems as Quasi-essential Facilities: Should We Impose Platform Neutrality? », *Journal of Law, Market & Innovation*, 1,3, November 2022, pp.108-134.

Marty F. and Pillot J., (2021), "Cooperation, dependence, and eviction: how platform-to-business coopetition relationships should be addressed in mobile telephony ecosystems" *in* Michal Gal and David Bosco eds. *Challenges to Assumptions in Competition Law*, Edward Elgar, April 2021, pp. 2-22

Mastor W., (2008), « L'état d'exception aux États-Unis : le USA PATRIOT Act et autres violations « en règle » de la Constitution », *Cahiers de la recherche sur les droits fondamentaux*, 6-2008, pp.61-70.

Mazzar M.J. et al., (2019), *Hostile Social Manipulation. Present Realities and Emerging Trends*, RAND, January, https://apps.dtic.mil/sti/citations/AD1081269

Mitchell A.D. and Samlidis T., (2021), "Cloud services and government digital sovereignty in Australia and beyond", *International Journal of Law and Information Technology*, vol 29, pp.364-394.

Nocetti J, (2018), « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018-2, pp.15-27.

Poirier L., (1982), *Essai de stratégie théorique*, volume 1, Fondation pour les études de défense nationale, Paris.

Sultan S. et al., (2019), "Container Security: Issues, Challenges, and the Road Ahead", *IEEE Access*, volume 7, April, pp. 52976-52996, https://doi.org/10.1109/ACCESS.2019.2911732

Taillat S., (2016), « Un mode de guerre hybride dissymétrique ? Le cyberespace », *Stratégique*, 2016/1, n°111, 89-106

Toledano J., (2020), *Gafa – reprenons le pouvoir*, Odile Jacob, Paris

Trumen P., (2019), "Challenged by 'Digital Sovereignty'", *Journal of Internet Law*, 23(6), pp.12-13

Varghese B. et al., (2021), "Revisiting the Arguments for Edge Computing Research", *IEEE Internet Computing*, volume: 25, issue: 5, September, pp.36-42, https://doi.org/10.1109/MIC.2021.3093924

Velliet M., (2023), "Souveraineté numérique : politiques européennes, dilemmes américains », *Notes de l'IFRI*, janvier.

Warlouzet L., (2008), « Europe de la concurrence et politique industrielle communautaire La naissance d'une opposition au sein de la CEE dans les années 1960 », *Histoire, Economie & Société*, 2008/1, pp. 47-61.

DOCUMENTS DE TRAVAIL GREDEG PARUS EN 2023
GREDEG Working Papers Released in 2023

2023-01 Thierry Blayac, Patrice Bougette & Florent Laroche
What Drive HSR' Prices and Frequencies? An Analysis of Intermodal Competition and Multiproduct Incumbent's Strategies in the French Market

2023-02 Guilhem Lecouteux & Léonard Moulin
Cycling in the Aftermath of COVID-19: An Empirical Estimation of the Social Dynamics of Bicycle Adoption in Paris

2023-03 Frédéric Marty
Les politiques publiques européennes en faveur d'un cloud souverain : fondements, modalités de mise en oeuvre et évaluation critique