LA LEVÉE DES OBLIGATIONS DE LOCALISATION DES DONNÉES

RÉSUMÉ

La Commission souhaite mettre en place un principe de libre circulation des données en Europe. **Une des principales implications de l'instauration de ce principe serait la restriction des obligations nationales en termes de localisation des données, qui n'auraient plus qu'un statut d'exception par rapport à ce principe**[1]. L'instauration de ce principe vise à libérer le potentiel économique d'un marché de la donnée unifié au niveau européen, en luttant contre sa fragmentation géographique.

Le Conseil partage les objectifs poursuivis par la Commission mais estime que **la consécration d'un tel principe n'est pas opportune à ce stade**. En effet les principales barrières à la croissance d'une économie de la donnée innovante se situent **moins au niveau des frontières nationales qu'au niveau des stratégies de lock-in et de rétention de données entre acteurs économiques**. Dès lors le principe de libre circulation devrait s'entendre davantage comme concernant la circulation des données entre plateformes qu'entre territoires.

De plus **la fragmentation géographique du marché de la donnée** - et notamment du marché du *cloud computing* - **au niveau européen n'est que marginalement causée par les obligations légales de localisation**. En effet celles-ci ne concernent qu'une part minime des données produites en Europe : en France, par exemple, cinq textes seulement édictent des obligations de localisation. **L'exigence de localisation des données procède d'abord des préférences des consommateurs**, traduisant un manque de confiance important dans l'économie du *cloud computing*. Par ailleurs, l**e manque d'harmonisation des autres marchés uniques (biens, services, capitaux…) et le manque d'harmonisation en termes de règles fiscales paraît un frein plus important** aujourd'hui pour le développement des acteurs européens du *cloud computing*.

Enfin, l**e principe de libre-circulation peut restreindre la capacité des Etats à réguler dans des domaines qui relèvent de l'exercice légitime de leur souveraineté**. Les données comptables et financières relèvent ainsi d'une obligation de localisation à des fins de contrôle fiscal. S'il existe bien des mécanismes de coopération pour faciliter l'accès aux données à travers les frontières, il n'en demeure pas moins que la localisation des données en dehors des frontières nationales pourrait compliquer et ralentir l'exercice de tels contrôles voire favoriser la disparition de pièces et de preuves. De plus, par-delà ces risques liés aux obligations de localisation actuelles, il semble dangereux de limiter la capacité des Etats à réguler dans le futur au regard des incertitudes qui pèsent sur les usages potentiels, au coeur des nouveaux modèles économiques.

Le Conseil recommande donc de mettre en place une harmonisation des obligations de localisation, plutôt qu'une levée par principe de ces obligations, afin de limiter la complexité juridique du marché européen de la donnée. **Cette harmonisation devrait s'accompagner d'une instauration de normes claires et de standards en termes de sécurité et d'accès aux données stockées, au niveau de l'état de l'art**. Cela permettra de construire un espace uniforme, bénéficiant de hauts critères de protection, et d'éviter des phénomènes de "dumping" et de perte de contrôle sur les données, qui pourra servir de modèle pour les traités de libre-échange.

La Commission européenne a annoncé qu'une initiative législative sera lancée en automne 2018 sur la levée des obligations nationales de localisation de données, par l'instauration d'un principe de libre circulation des données.

***De nombreux Etats membres ont en effet mis en place des obligations de localisation de données dans le cadre de politiques publiques diverses** : sécurité nationale, effectivité des contrôles réalisés par les administrations fiscales, conservation des archives publiques, régulation des jeux en ligne. Ces obligations, qui varient d'un État à un autre, peuvent freiner le développement de services de stockage de données et plus largement du cloud computing à travers les frontières. **L'objectif poursuivi par la Commission européenne est donc de lutter contre la fragmentation du marché européen de la donnée**. L'unification des marchés numériques européens vise notamment le développement de champions européens du cloud computing.*

LA LEVÉE DES OBLIGATIONS DE LOCALISATION DE DONNÉES RISQUE DE MANQUER SON OBJECTIF

Les frontières ne sont pas les principales barrières au développement de l'économie européenne de la donnée

La mise en place d'un principe de libre circulation des données vise principalement à faciliter les mouvements de données entre pays, comme cela a pu être fait précédemment sur d'autres marchés (biens, services, capitaux). Un des enjeux liés à l'unification d'un tel marché est notamment celui de la constitution d'un marché européen du cloud computing, tant au niveau de la demande que de l'offre. Au regard de l'avance prise par les acteurs dominants du marché du cloud, il apparaît nécessaire de favoriser l'émergence de nouveaux acteurs innovants.

Néanmoins il semble que les principales barrières à la croissance d'une économie de la donnée innovante se situent moins au niveau des frontières nationales, du fait des obligations de localisation, qu'au niveau des **stratégies de lock-in et de rétention de données entre acteurs économiques**. Il semble ainsi prioritaire de se concentrer avant tout sur les barrières à la circulation des données "trans-plateformes" plutôt que "trans-frontalières", dans la mesure où l'économie numérique est particulièrement marquée par les effets de "silos" de données qui peuvent constituer des obstacles à l'innovation.

La fragmentation géographique du marché de la donnée n'est que marginalement causée par les obligations légales de localisation.

- **Peu d'obligations légales de localisation ont été adoptées par les Etats membres de l'Union européenne**

Le Règlement général sur la protection des données (RGPD) adopté en 2016 a permis une avancée majeure : il créé un cadre unifié en matière de protection des données à caractère personnel en Europe. Il supprime également les obligations de localisation de données intra-européenne justifiée par la protection des données personnelles.

Les obligations de localisation pour des motifs autres que la protection des données personnelles concernent **une part minime des données** produites en Europe. En France, par exemple, cinq textes seulement édictent des obligations de localisation. Ces textes concernent des types précis de données et de situations, parfois dans le champ du RGPD ou en dehors du champ des traités européens, et ainsi non affectés par l'instauration d'un principe de libre circulation des données (données de santé, documents marqués secret défense). De plus, un certain nombre de choix de localisation dépendent d'une **mauvaise interprétation** de ces obligations. Ainsi de nombreux participants au marché estiment que le stockage et le traitement des données au sein des frontières nationales sont obligatoires ou conseillés alors que ce n'est pas le cas[2].

- **Les préférences des consommateurs déterminent en grande partie les choix de localisation**

De nombreuses sociétés choisissent de stocker leurs données dans leur pays non pour des raisons légales, mais pour se conformer aux préférences des consommateurs. La localisation est en effet considérée par beaucoup comme garante d'une meilleure sécurité, confidentialité et intégrité des données. 37,7 % des utilisateurs de *cloud computing* ont ainsi plus confiance dans la sécurité de leurs données si elles sont conservées et traitées dans leur pays[3]. **Si les fournisseurs de services de cloud doivent donc développer des infrastructures sur les différents marchés européens, ce n'est pas pour se plier à des obligations légales, mais plutôt pour répondre aux préférences de leurs clients**. Ces préférences reflètent une défiance plus large envers le *cloud computing*, dûe à différentes raisons : inquiétude sur la continuité et la qualité de service, difficultés réelles ou supposées sur l'intégration efficace des applications avec le reste du système d'information, difficultés d'acceptation de la standardisation amenée par le *cloud*[4]... Cette méfiance peut être prévenue en favorisant une meilleure information et formation des acteurs économiques aux enjeux liés au *cloud computing*.

- **Le manque d'harmonisation des autres marchés uniques a un impact plus important sur la fragmentation du marché de la donnée**

Le manque d'harmonisation des règles des autres marchés (biens, services, capitaux…), mais également en termes de règles fiscales, semble un frein plus important aujourd'hui pour le développement des acteurs européens du *cloud computing* que les obligations des localisations. La diversité des règles fiscales ou des dispositions du droit de la consommation ont un impact considérable sur la fragmentation du marché pour les acteurs numériques

IL MANQUE DE GARANTIES SOLIDES EN TERMES DE CONDITIONS D'ACCÈS POUR LES ÉTATS ET DE SÉCURITÉ

- **L'accès des autorités aux données doit être préservé**

Les obligations de localisation visent en premier lieu à assurer aux États une capacité d'accès à certaines données. Ainsi, les obligations de localisation concernant les factures des entreprises ont pour objectif de permettre aux services fiscaux d'assurer leurs missions de contrôle dans les meilleures conditions, notamment dans le cas de perquisitions judiciaires. Il existe ainsi des règles différentes, suivant les pays, en matière de perquisition et de saisies de données, dans les enquêtes fiscales. De la même manière, il peut également apparaître légitime que les Etats puissent conserver ce qui relève des archives publiques et des trésors nationaux au sein de leur territoire. Si, dans ce cas précis, les difficultés d'accès potentielles ne sauraient être aussi importantes que pour le cas de données comptables hébergées à l'étranger, qui peuvent faire l'objet de stratégies de dissimulation volontaire, il semble toutefois que l'accès aux archives peut être rendu plus difficile pour l'Etat si celles-ci sont situées à l'étranger - pour des raisons diplomatiques par exemple.

Les conditions d'accès, notamment en termes judiciaires, sont encore trop peu harmonisées entre les pays de l'Union européenne. Il est donc nécessaire, en amont de la consécration du principe de libre circulation des données, de mettre en place des conditions d'accès européennes harmonisées, à la fois en termes de droit, mais également de capacités techniques. L'efficacité de la transmission des données nécessaires pour les contrôles fiscaux serait ainsi à améliorer.

- **Des standards de sécurité élevés doivent être collectivement définis**

Les obligations de localisation visent également à préserver la sécurité des données stockées. Cet argument peut sembler caduc, puisque dorénavant la sécurité de documents stockées en ligne dépend moins de leur localisation physique que des capacités de chiffrement et de cybersécurité qui sont déployées pour les protéger. La localisation en elle-même ne semble donc pas garantir un meilleur niveau de sécurité. **Néanmoins aux obligations de localisation correspondent l'imposition d'un droit national en termes de standard de sécurité, notamment informatiques, ainsi que la capacité de vérifier l'application de ces normes, notamment par des processus d'auditabilité**.

Il semble donc nécessaire d'**harmoniser, en amont de l'édiction du principe de libre circulation, les standards de sécurité informatiques entre les pays de l'Union européenne, afin que la fin des obligations de localisation ne riment pas avec une diminution du niveau de sécurité et des effets de "dumping" à l'intérieur de l'Union**. Ces standards ne peuvent se résumer à une simple reconnaissance mutuelle de l'équivalence des conditions de protection entre États européens. A cet égard, le modèle de la régulation des données personnelles semble tout à fait pertinent : les obligations de localisation des données personnelles ont été levées dans la mesure où une harmonisation forte des conditions de sécurité et de protection de la vie personnelles a été réalisée. Il s'agit de promouvoir l'état de l'art et d'obliger à la mention systématique des failles de sécurité afin de favoriser la progression du niveau de sécurité de l'ensemble de l'écosystème européen. Des processus d'auditabilité communs doivent être définis de manière corollaire. ***et à l'accès aux données de certains publics.*** *Il semble par exemple urgent de prévoir une exception pou recherches interdisciplinaires qui nécessitent de croiser des bases de données de nature différente.*

LES CONTOURS DE L'HARMONISATION DES CONDITIONS DE LOCALISATION DEMEURENT À PRÉCISER

- **L'impact réel sur la capacité des États à réguler**

Il est nécessaire de mener au préalable des véritables **études d'impact auprès des Etats** afin d'évaluer les risques que leur ferait courir la levée des obligations de localisation. Or il ne semble pas que ce travail ait été mené. Un tel travail permettra notamment de préciser ce qui doit être notamment amélioré dans le cadre de la coopération policière et judiciaire. De la même manière, une étude d'impact pourrait être menée sur les effets de la levée des obligations de localisation sur la sécurité des données, même en cas d'harmonisation des normes de sécurité, afin de déterminer si la localisation physique ne joue véritablement aucun rôle sur la sécurité des données.

En outre, il semble nécessaire d'accroître l'information des États quant à la localisation des données des entreprises qui ont une activité sur leur territoire. Il apparaît que beaucoup d'entreprises ignorent l'endroit où se situent leurs données. Une exigence de communication, à la Commission européenne, de la localisation de leurs données pourrait être instaurée pour les entreprises, dans un double objectif : faire prendre conscience aux entreprises de l'importance de cette question et faciliter les requêtes de la part des autorités nationales.

- **Les conditions d'harmonisation**

La détermination des conditions d'harmonisation des obligations existantes doit être précisée en amont de l'édiction du principe, au risque, sinon, d'assister à des phénomènes de dumping, notamment en termes de sécurité des données. Il semble nécessaire de poursuivre le travail de recensement des obligations de localisation nationales dans une optique de transparence, et de le coordonner à une démarche d'**harmonisation des obligations existantes**. La détermination des obligations de localisation les plus utiles à l'accomplissement des fonctions des pouvoirs publics devra guider le travail d'harmonisation.

En parallèle, il est nécessaire de préciser les conditions de création de nouvelles obligations. Des incertitudes pèsent sur l'usage des données, notamment relativement à l'exercice de la puissance publique des États, ainsi que sur les exigences futures en termes de sécurité. Il semble donc nécessaire de déterminer des procédures de création de nouvelles obligations qui soient suffisamment souples pour être effectives, sans toutefois remettre en cause l'harmonisation du marché.

- **La mise en place d'un cadre de pensée global**

La mise en place d'un cadre général apportant des garanties de confiance pour la circulation des données pourrait ainsi être préférée à la levée des obligations de localisation. C'est l'occasion pour l'Union européenne de créer un paradigme équilibré, qui puisse servir de modèle pour les traités de libre-échange à venir. Il s'agit de proposer une alternative au principe de circulation sans garde fous, en proposant des règles en termes d'accessibilité, contrôles et sécurité, à même d'encourager la libre circulation, et de penser ses implications potentielles en termes de souveraineté et d'extra-territorialité du droit. En effet, ces questions vont devenir de plus en plus pressantes au niveau international, notamment pour les échanges entre les États-Unis et l'Union européenne.

[1] La mise en place du RGPD facilitant la circulation des données personnelles, la mise en place de ce principe vise principalement la circulation des données non personnelles.

[2] Facilitating cross-border data flow, étude de la Commission européenne, 2016

[3] ibidem

[4] https://www.ovh.com/fr/images/news/plan-cloud computing/rapport-cloud computing.pdf, étude OVH - Nouvelle France industrielle, 2014