ABOLISHING DATA LOCALISATION RESTRICTIONS

SUMMARY

The Commission wishes to enshrine a principle of free flow of data in Europe. **One of the main consequences of the establishment of such a principle would be the limitation of national data localisation restrictions, which would become exceptions to this general principle**[1]. The establishment of the principle of free flow of data aims at freeing the economic potential of a unified European data market by fighting its geographical fragmentation.

The Council shares the objectives pursued by the Commission, but considers that enshrining such a principle is not adequate at this stage. **Today, it is not so much national boundaries that create roadblocks to the free flow of data than lock-in and data retention strategies between economic stakeholders**. Thus, the principle of free flow of data should be oriented towards a "cross-platform" rather than a "cross-border" free data flow.

In addition, the geographical fragmentation of the European cloud computing market is only partially caused by legal localisation restrictions. In fact, these only apply to a very limited amount of the data produced in Europe. In France, for example, only five regulations impose localisation restrictions. **The need for data localisation mostly originates from consumer's preferences, revealing a fundamental lack of trust in the cloud computing economy**. Furthermore, the present-day lack of harmonisation of other common markets (goods, services, capital,…) and the lack of harmonised taxation rules seem to be an even greater obstacle for the development of European cloud computing actors.

Lastly, the free flow of data principle could restrict the member states' capacity to regulate on legitimate sovereignty-related areas. Fiscal and financial data are subject to localisation restrictions due to tax inspection reasons for instance. **Despite the existence of many cooperation mechanisms that facilitate cross-border data access, the problem remains that the location of data outside national borders could complicate and slow down the exercise of such inspections** to the point of favoring the disappearance of documents and proofs. Besides the risks connected to present-day localisation restrictions, it seems furthermore dangerous to limit the member states' future capacity to regulate, considering the uncertainties connected to potential uses at the heart of economic models that are still emerging.

The Council therefore suggests to **pursue the harmonisation of localisation restrictions rather than their complete abolishment, so as to limit the juridical complexity of the European data market**. Such harmonisation should go hand in hand with **the establishment of clear rules and state of the art security and access standards** for data storage. This a prerequisite for the building of a unified space in Europe with strong protection standards. It aims at avoiding dumping effects and the loss of control over data, which could become an international standards for trade-agreements

The European Commission has announced that a legislative initiative will be launched in autumn 2018 with the purpose of abolishing national restrictions on data localisation by introducing a free flow of data principle.

Several member states have in fact set up data localisation obligations following diverse public policies : *national security, tax investigation efficiency, preservation of national archives, online games regulation. These restrictions, that differ from state to state, could be an obstacle to the development of data storage services and more broadly to cross-border cloud computing services. The Commission aims therefore at fighting the fragmentation of the European data market. The unification of the European data markets aims to foster the development of European champions of cloud computing.*

THE ABOLITION OF DATA LOCALISATION OBLIGATIONS RISKS TO FAIL ITS OBJECTIVES

National borders are not the main obstacles to the development of the european data market

The establishment of the principle of free flow of data aims to ease data movement between countries, as it has been done precedently on others markets (goods, services, capital).

One of the main issue at stake is to create an unified European market for cloud computing, both for the supply and demand side. In the light of the market dominance exercised by a few actors, it seems in fact necessary to encourage the emergence of new innovative pan-European businesses.

Nevertheless, it appears that the main barriers to the growth of an innovative data economy in Europe lie way more **in lock-in and data retention strategies by economic actors than in national barriers.** Thus, the principle of free flow of data should focus on a cross-platform rather than on a cross-border circulation. Digital economy is indeed characterised by a concentration of data which can be against innovation.

The geographical fragmentation of the data market is only partially caused by legal localisation restrictions

- **Only a few legal localisation obligations have been adopted by the member states**

The 2016 General Data Protection Regulation (GDPR) represents a major step forward for the creation of a unified framework for the protection of personal data in Europe. It furthermore outlaws localisation restrictions of intra-european data justified by the protection of personal data.

A very small amount of data is concerned by data localisation obligations, except for privacy reasons (covered by the GDPR). In France, only five obligations have been identified : some of them are not concerned by the the principle of free flow of data (classified data, eg, which are not in the field of European treaties). Furthermore, **some companies misunderstand legal obligations**: a lot of economics actors think that localisation is mandatory when it is not the case[2].

- **Consumer preferences are at the origin of localisation decisions**

In many cases, the need for data localisation originates from the consumer's preferences and not from legal obligations. Localisation is considered by most companies as a guarantee that data are stored with a sufficient level of security, confidentiality and integrity. 37,7 % of users of cloud computing services have no confidence in data storage if their data is not stored and processed in their home countries [3]. **So if cloud providers tend to install data storage facilities in many countries in Europe it is not to conform to legal obligations but mostly to comply with user preferences**. These preferences however reveal a fundamental lack of trust in the cloud computing economy, for a number of reasons : worries about the continuity and quality of services, real or supposed complexities when it comes to integrate applications in a preexistent information system, difficulties to accept the standardisation sometimes imposed by cloud services[4]… Information and formation of economics actors to develop awareness around cloud computing issues could be a way to restore trust in the data economy.

- **The lack of harmonisation of other single markets have a more crucial impact on the fragmentation of the data market**

The lack of harmonisation of the rules of other markets (goods, services, capital), but also of the fiscal rules appears to be a more major obstacle to the development of European actors in the field of cloud computing than legal obligations. **The diversity of fiscal and consumer laws have a significant impact on market fragmentation for digital businesses**.

SOUND GUARANTEES ON STATE ACCESS AND SECURITY ARE STILL MISSING

- **Legal access to data must be granted**

Localisation restrictions aim first and foremost at granting state authorities access to specific data. Tax records thus serve the purpose of enabling tax services to ensure control enquiries in the best conditions - judicial searches in particular. Country-specific rules relative to search and data capture in tax investigations are therefore the norm. Similarly, it seems legitimate that public authorities keep the ability to preserve their public archives and their national treasures within their territory. If, in this particular case, the potential access difficulties are not as great as in the case of tax records hosted abroad - which may be part of voluntary concealment strategies - it appears that access to archives can be made more difficult for the state's authorities if these are located abroad - for diplomatic reasons, for example.

Conditions of access - for judicial cooperation notably - are still unsufficiently harmonized among EU member states. Prior to the enshrinement of a free flow of data principle, it is thus necessary to establish European-wide harmonized conditions of access both in terms of law and of technical capabilities. Data transmission efficiency between fiscal administrations could for example be improved.

- **High security standards must be collectively defined**

Localisation restrictions equally aim at preserving the security of stored data. As the security of online stored documents seem henceforth better determined by encryption and cyber security techniques deployed to protect them, rather than by their physical location, this argument may seem lapsed. Localisation itself does not seem able to grant a higher level of security. Nevertheless, localization obligations correspond to the imposition of national law in terms of safety standards, notably in computer security, as well as the capability to implement these norms, notably through audit procedures.

Prior to the enshrinement of a free movement principle, **it seems therefore necessary to harmonize computer security standards among EU member states. The main reason is to avoid that the end of localisation restrictions equals to a lessening of the level of security and to the emerging of dumping effects within the Union**. These standards cannot be limited to a simple mutual realization of the equivalence of the protection conditions between the EU member states. In that regard, the regulation model of personal data seems fully pertinent. Data localisation restrictions have been abolished as long as the strong harmonisation of security and privacy protection conditions has been completed. It is a matter of promoting the best practices and of imposing the report of system failures in order to foster the advancement of the level of security of the European ecosystem as a whole. Additional common audit procedures must be defined as well.

THE OUTLINE OF LOCALISATION HARMONISATION CONDITIONS ARE YET TO BE DEFINED

- **The real impact on member state's capacity to regulate**

It would be necessary to conduct preliminary **impact studies within member states** so as to precisely estimate the risks connected to the abolishment of data localisation restrictions. Similar studies do not seem to have been performed yet. Building on the outcomes of these enquiries, it would be possible to focus on aspects of the police and judicial cooperation that still need to be improved. A similar impact study could be implemented on the consequences of the abolition of data localisation restrictions on data security, so as to verify if physical localisation does not play any role in data security. This may also be done assuming harmonized security norms.

Moreover, it seems necessary to increase the information of States as to the location of the data of the companies which have an activity on their territory. It appears that many companies are unaware of where their data are located. A requirement to communicate to the European Commission the location of specific type of data could for instance be introduced with a dual objective : to raise awareness of the importance of this issue and to facilitate requests from national authorities.

- **Conditions for harmonization**

The definition of harmonization conditions should go hand in hand with the establishment of the principle. Failure to do so could could foster dumping phenomena - of data security in particular. It seems necessary to operate an inventory of national localisation restrictions with a particular transparency intent, as well as to coordinate an **harmonization campaign of existing restrictions**. The harmonisation work should be led by the detection of the those restrictions that better help public administrations to perform their public authority.

Parallel to that, it is necessary to define terms and conditions for the creation of new restrictions. Uncertainties are an obstacle to data usage. The exercise of the state's public authority and future security needs appear to concern most of these restrictions. It seems therefore necessary to set up procedures for the creation of new restrictions that would be flexible enough to be efficient, but that would not put the market's harmonization into question.

- **Establishing a global framework**

The establishment of a global framework fostering trust guarantees for data circulation should be preferred to the simple abolition of localisation restrictions. It is an opportunity for the European Union to create a new balanced paradigm that can serve as model for future free trade treaties. This could be an alternative to the principle of free flow without safeguards - which would mean rules for access, controls and security able to encourage free movement - and to think about potential consequences for sovereignty and the extra-territoriality of law. These issues will in fact become increasingly urgent on an international level, in particular when exchanges between the United States and the European Union are concerned.

[1] The implementation of the RGPD aims to facilitate the circulation of personal data. In parallel the implementation of this principle is mainly aims at the circulation of non-personal data.

[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