# ARTICLE

## SHOULD WE BE AFRAID OF THE CLOUD ACT?

Real Estate and Construction European Law Public Law and Public Procurement Law | 25/06/18 |
Emmanuelle Mignon

The Clarifying Lawful Overseas Use of Data Act (hereinafter the "Cloud Act") was promulgated by the president of the United States on March 23, 2018.Adopted without a real debate after the complex debates on the 2018 budget act, the Cloud Act continues to generate criticism, in the United States and Europe, by civil liberties protection organizations and critics of extraterritoriality of American laws, which are not always understood.Not without a great deal of approximation.

This news flash aims to concretely present what the Cloud Act is, to point out what one should know about it and to explore what French and European authorities' reactions could/should be.

**1 - From the warrant case to Cloud Act**

Title 18 of the United States Code is the equivalent of our criminal code and code of criminal procedure combined.It includes a chapter 121, known under the name Stored Communications Act (hereinafter the "SCA"), introduced in U.S. legislation in 1986.This legislation lays down a principle of confidentiality and protection of communications data (content and information on the user and his communications) processed or stored by data communications, processing and electronic storage service providers.

Typically, this legislation also provides for a certain number of exceptions to the principle thus enacted, such as disclosure that is necessary for providing the service, disclosure at the user's request and the possibility for U.S. authorities, subject to certain procedural and substantive conditions, to request, from the providers of these communications services, data about their clients for criminal proceedings.It is important to note that the Stored Communications Act was adopted for the purpose of expressly making the disclosure of certain communications data by third parties (service providers) in criminal investigations subject to the fourth amendment of the United States Constitution (protection against searches and seizures not ordered by courts and not based on probable cause that the given person has committed or is about to commit a criminal offence and that the places, objects or information mentioned by the warrant are useful to the investigation).

Within this framework, and in a drug trafficking case, in 2013, the U.S. authorities asked Microsoft Corporation to disclose to them the communications data involving a non-US person.Microsoft Corporation refused on the grounds that the data were stored in Ireland and that, to respect Ireland's sovereignty, such a request had to be made through international judicial assistance (meaning through the procedure provided by a mutual legal assistance treaty, the well-known MLAT, or through an international letter rogatory).Firstly, Microsoft argued that it would have been impossible for the U.S. authorities themselves to come to force open the doors of a physical cabinet located in Ireland in which the same data would have been stored in paper format and that, therefore, there was no reason to allow this for a virtual cabinet; secondly, Microsoft argued that such a request risked placing it in a conflicts-of-law situation in the event that an Irish law hindered disclosure of the data.In so doing, Microsoft was looking ahead to the entry into force of the GDPR.

As we know, the Court of Appeals for the 2nd circuit of New York ruled in Microsoft's favor.The U.S. Attorney General then appealed the case to the U.S. Supreme Court, which decided to take on the case.However, perhaps fearing the result of this case, before the Supreme Court handed down its ruling, the U.S. government preferred to have Congress adopt the Cloud Act, thereby settling the issue directly by law.Consequently, the Supreme Court did not rule on the warrant case.

**2 - What does the Cloud Act provide ?**

Although it is more than 10 pages long, the Cloud Act essentially contains two provisions:

- firstly, it provides that all U.S. companies within the meaning of U.S. law, meaning companies incorporated in the United States and companies controlled by it, must disclose to the U.S. authorities, at their request, the communications data under its control without consideration for where such data are stored.Therefore, out with the legal sovereignty of other countries based on the place where data are stored;

- it then provides (and this is by far the longest part of the Cloud Act) that it is possible for the U.S. government to sign international agreements with foreign governments permitting the respective authorities of each country to directly ask providers of data communications, processing and electronic storage services within the other's jurisdiction to disclose the communications data they seek, without going through the longer MLAT or international letters rogatory procedures.

Concretely, if the United States signed such an agreement with an imaginary country quite originally called Syldavia, the authorities of Klow could directly ask the service providers within the jurisdiction of the United States to disclose the data placed under their control and which are useful to their investigations, with the exception of data involving U.S. persons (U.S. citizens, permanent residents, companies registered principally in the United States), without going

through the U.S. Justice Department; reciprocally, the U.S. authorities could directly contact the Syldavian providers of data communications, processing and electronic storage services(the very well-known Syldavian "sovereign clouds") to obtain the disclosure of communications data placed under these companies' control without going through the governmental and/or judicial authorities of the Kingdom of the Black Pelican.The legislation does not say it, but the logic of reciprocity naturally means that such requests made by the U.S. authorities cannot involve data involving Syldavian nationals or companies, nor data about nationals or companies within the jurisdiction of the other countries with which Syldavia forms an "*Every closer union*".

The international agreements involved will take the form of executive agreements, meaning agreements that do not require the Senate's approval with a two-thirds majority or the adoption of a law by Congress's two chambers.To enter into force, all that is needed is that the two chambers not oppose it with a joint resolution within 90 days of the signing of the agreements.In exchange, such agreements can be signed only with countries that respect civil liberties and standard democratic principles.And the Cloud Act expressly states that requests for disclosure of data involved in these agreements can only cover serious crimes.

In reality, the Cloud Act organizes at the transatlantic level what the proposed e-Evidence Regulation attempts to organize at the European level:the possibility for law-enforcement authorities to obtain the disclosure of communications data in which they are interested in their investigations by directly contacting the companies processing or storing such data, meaning much more swiftly than within the typical framework of international judicial cooperation.The objective is to place criminal investigations much closer in time to when crimes are committed.

All observers agree that the Cloud Act does not allow one to determine with certainty whether such an executive agreement could be signed with the European Union rather than with the Member States.Perhaps for political posturing, it appears as if U.S. authorities wished to reserve the possibility of not signing such agreements with the countries of the European Union considered, from the viewpoint of protecting rights, as less respectable as others, which explains the idea of agreements signed only with qualifying foreign governments.

Although the United Kingdom began to negotiate an executive agreement with the United States, the majority position of the Member States of the European Union is instead, at this stage, to seek an overall agreement between the European Union and the United States.

**3 - Does the Cloud Act allow U.S. authorities to access without restriction all of the European data processed or stored by service providers within the jurisdiction of the United States ?**

About this issue we have heard a great deal of approximation, if not outright foolishness.

It is certain that the Cloud Act applies to any company within the jurisdiction of the United States which controls computer data its clients entrust to it regardless of the clients' nationality and the physical place where such data are transmitted or stored.The GAFAM are companies within the jurisdiction of the United States, as are their subsidiaries.In this sense, the **Cloud Act is not an extraterritorial law, but only a law that applies to any company within the jurisdiction of the United States in the meaning of U.S. law, which, it is true, is extensive**.

**Even so, the Cloud Act changes nothing about the legal conditions under which such disclosure requests may be made by U.S. authorities.**

Concretely:

- based on the SCA, U.S. authorities may request the disclosure of data by providers of data communications, processing and electronic storage services under their jurisdiction only within the framework of judicial proceedings and if they have a warrant for doing so, meaning one issued by a court and protected by the fourth amendment of the U.S. Constitution (probable cause that the person involved has committed or is about to commit a criminal offence and that the places, objects or information covered by the warrant are useful to the investigation).From this angle, U.S. law is more protective than French law, which allows public prosecutors to make comparable requests.However, as the European Court of Human Rights regularly states, public prosecutors are not an "*impartial and independent court*", not because of the conditions under which its members are appointed (wrong debate), but because it is the authority which prosecutes.

- the SCA also authorizes U.S. governmental authorities to request the disclosure of data or metadata of communications based on court orders.Therefore, these requests are also made with the authorization of a court and must be justified, as with warrants, by the needs of criminal proceedings;

- the possibility, provided by the legislation, for U.S. governmental authorities to obtain the disclosure of content data through administrative, grand jury or trial subpoenas was declared unconstitutional by a December 14, 2010 decision of the Court of Appeals of the 6th circuit of Cincinatti (*United States v. Warshak*) on the grounds that such requests were not placed under the protection of the fourth amendment.This case law has not been upheld or reversed by the Supreme Court of the United States, but it is considered to be indisputable by all actors involved and, due to this fact, the GAFAM do not disclose content data to U.S. authorities based on mere subpoenas.Better yet, in an extremely recent decision (Jun. 22, 2018, *Carpenter v. United States*), the Supreme Court of the United States ruled that the request to disclose geolocalization data emitted by a mobile phone, sent by U.S. authorities to a communications services provider, had to benefit from the protection of the fourth amendment and had to be made through a warrant:a decision that is fully in line with the *United States v. Warshak* decision;

- lastly, it is still possible for providers with whom requests have been made to dispute, in a lower or appeals court, through an action or a preliminary objection (cf. *infra*), the order served on them to disclose to U.S. authorities the communications data entrusted to them.

Unlike what has been written on numerous occasions, the Stored Communications Act as modified by the Cloud Act **does not give U.S. authorities a blank check to access, without restriction or review, all of the data entrusted to providers of data communications, processing and electronic storage services within the jurisdiction of the United States.**

In addition, the Cloud Act explicitly provides that service providers from whom the data are requested still have the possibility of objecting to such requests on grounds that the requests, if granted, **would lead to violations of foreign countries' legislation and such fact would expose them to penalties (conflicts-of-law situation).**

The conditions for objecting to such requests are different depending on whether executive agreements exist with the countries whose laws may be violated:

- in cases where there is an executive agreement between the United States and the given country, the objection proceeding, which comes in addition to any other cases of objections based on the lawfulness or merits of the request, must be brought within 14 days.To assess whether there are grounds for quashing or modifying the request for disclosure, the court must take into account the serious nature of the risk of penalties to which the provider is exposed in the other country and the interests, for justice, in modifying or quashing the request.The interests of justice are assessed based on the following criteria:the interests of the United States, including the governmental entity seeking to require disclosure of the disputed information; the interests of the qualifying foreign government in preventing any disclosure, prohibited under its legislation, of the disputed information; the location and nationality of the customer and the nature of such customer's connection to the United States; the nature of the provider's ties with the United States; the importance to the investigation being carried out of the information required to be disclosed for the investigation; the possibility for the governmental entity to obtain in an as acceptable manner the information requested by means with fewer negative consequences;

This objection proceeding, called a comity analysis, is not applicable when the data whose disclosure is requested involves a United States person, meaning a citizen of the United States, a person admitted for permanent residence, an unregistered organization are large number of whose members are American citizens or persons admitted for permanent residence, or any company registered in the United States; and

- in the absence of an executive agreement, the provider may also refuse to disclose the requested data based on the common law principles of comity, meaning based on the principle of international comity recognized by American courts, according to which, for the application of U.S. law, one must take into account the important interests of other countries and, if applicable, not apply or apply in a nuanced manner U.S. legislation.Unlike the previous proceeding, the criteria a court must use to rule on the merits of such an objection are not stated by the act (they result from case law).In addition, when the proceeding is based on a warrant, the objection is not direct.It takes the form of a defense argument against the petition to find the company with whom the request is made guilty of contempt of court.

It is not easy to understand the differences or, above all, the reason for being of this double objection proceeding in the case of a conflict of laws, depending on whether the foreign country whose law may be violated has or has not signed an executive agreement.The objective of the United States appears to have been to encourage having executive agreements signed by preparing a direct and clear objection proceeding, whereas the principle of international comity as resulting from only the common law case law of American courts is sometimes criticized for being insufficiently precise and foreseeable.

**4 - Do French or European laws exist that may hinder requests from American authorities for data stored in Europe?**

There are at least three.

The first one is act no. 68-678 of July 26, 1968, on the disclosure of economic, commercial, industrial, financial or technical documents and information to foreign natural persons or legal entities, referred to as the "French blocking act" (as opposed to the European blocking regulation, Council regulation no. 2271/96 of November 22, 1996, on protection against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, which attempts, firstly, to counter the effect of certain U.S. sanctions against European countries with activities in countries subject to U.S. embargos).

Subject to treaties and international agreements, **the French blocking act prohibits all persons with French nationality or who habitually reside in France or all legal entities who have their head office or an establishment in France, from disclosing to foreign public authorities economic, commercial, industrial, financial or technical documents or information that may infringe upon France's sovereignty, security or essential economic interests or upon public policy (Article 1), it prohibits all persons from requesting, seeking or disclosing economic, commercial, industrial, financial or technical information aimed at establishing evidence for foreign judicial or administrative proceedings or within the framework of such proceedings (Article 1 *bis*), it enacts an obligation for persons with whom such requests are made to**

**promptly inform the Minister of Foreign Affairs (Article 2, the violation of which is not penalized) and it provides for a criminal sentence of 6 months' jail time and a fine of 18,000 euros (90,000 euros for a legal entity) in case of a violation of the prohibitions enacted by the act's first two articles (Article 3).**

Very clearly, requests for disclosure of data U.S. authorities make with the GAFAM under the Cloud Act could be within the scope of Article 1, and even more so within the scope of Article 1 *bis* of the French blocking act, and expose these companies and their French subsidiaries to the corresponding penalties.**Therefore, they should be able to object to the disclosure of such data by invoking the principle of international comity based on one or other of the proceedings mentioned above.**

It is true that American courts give only little consideration to the French blocking act given the fact that the penalties it provides are never actually imposed.In a sadly well-known decision of June 15, 1987 (*Société Nationale Industrielle Aérospatiale v. U.S. District*, no. 85-1695), the Supreme Court of the United States refused to take this act into consideration, thereby releasing a company of its obligations under U.S. law, mainly relying on the fact that French companies which disclose information in violation of the provisions of the blocking act are not actually penalized.

Nevertheless, it should be noted that, since this decision, criminal penalties based on the blocking act have been pronounced at least one time by a French court and upheld by the French Supreme Court (Cass. Crim., Dec. 12, 2007, appeal no. 07-83.228, *Christopher X*).Also to be noted is that, after this ruling, the Court of Chancery of the State of Delaware (Feb. 21, 2014, *Activision Blizzard Inc. Stockholder litigation*, Cons. C.A., no. 8885-VLC) accepted, given the French blocking act, to favor, for seeking evidence in a U.S. court proceeding, the use of procedures provided by the Hague Convention of 1970 rather than the U.S. discovery procedure (but by setting reduced deadlines to implement them subject to making U.S. procedures take precedence).

Articles 44 et seq. of the European Parliament and Council (EU) Regulation 2016/679 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the well-known GDPR), govern the conditions under which personal data may be transferred to third countries or international organizations.

Generally speaking, such transfers are possible only:

In addition, Article 48 of the GDPR states, so that everything is quite clear, that:"*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.*"

Here, the Commission has adopted no general adequacy decision for transfers of data to U.S. public authorities.The mechanism provided by the privacy shield agreements covers only transfers to U.S. companies that have self-certified as unreservedly adhering to the principles contained in this agreement, and not to governmental entities.The unilateral commitments, which, moreover, are rather vague, made by U.S. public authorities within the framework of the privacy shield are not equal to the Commission's recognition that the transfer of data to these authorities provides an adequate level of personal data protection and, therefore, such a transfer is possible on the basis of Article 45 of the GDPR.

Similarly, in the absence of an agreement with the United States, such a transfer cannot be justified in Article 46 without an ad hoc mechanism allowing the given European nationals to have the safeguards and legal remedies comparable to those resulting from the GDPR.

Lastly, such a transfer is not within the scope of the exceptions in Article 49, and in particular not within the exception provided by Article 49, paragraph 1, point d) of the regulation ("*the transfer is necessary for important reasons of public interest*").This exception in effect covers only the public interests of a Member State of the Union or the Union itself, as the European Data Protection Committee (which has replaced the WP29) has just fittingly indicated in its Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, published on May 25, 2018.Hence, it is not because the fight against terrorism is an objective shared by all countries, obviously including the United States, and recognized by their respective legislation, that this objective justifies the transfer of personal data to third countries, including the United States, or international organizations, even if such data are requested by administrative or judicial authorities.Any other interpretation of Article 49 1 d), moreover, would have been incompatible with Article 48.

On the other hand, still according to these guidelines, the principle of reciprocity in international relations is a public interest.Under these conditions, the existence of an international agreement on international police or judicial cooperation could allow the transfer of personal data to the authorities of a third country on the basis of Article 49 1 d) (which would then be superfluously added to Article 48).

Therefore, the transfer of personal data to American authorities, performed by a GAFAM pursuant to a request based only on the Cloud Act and not on an MLAT-type international agreement or the implementation of an international letter rogatory, would not be consistent with the GDPR.Such a violation of the GDPR's rules can be subject to an administrative fine of up to 20,000,000 euros or, in the case of a company, up to 4% of the total worldwide annual turnover of the previous fiscal year.Given their potential importance, we hope that, pursuant to the principle of international comity, U.S. courts will more carefully consider, for the blocking act, the tricky situation in which, to respect its obligations under the Cloud Act, a company violates the GDPR.

Lastly, the European Union has recently adopted a regulation to protect trade secrets, European Parliament and Council (EU) Directive 2016/943 of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, the transposition of which into French law is imminent.Soon, a new Article L. 151-6 of the French Commercial Code should provide that, "*trade secrets are not enforceable when the obtaining, use or disclosure of the secrets is required or authorized by European Union law, treaties or international agreements in force or national law, including in the exercise of investigative, oversight, authorization or sanction powers of court or administrative authorities.*"Conversely, the disclosure of data covered by trade secrets to U.S. authorities, outside of any international agreement, meaning based only on a unilateral request made with a GAFAM by U.S. authorities under the Cloud Act, is prohibited and exposes the provider that discloses such data to being held civilly liable.

**5 - Confronted with the Cloud Act, what should French and European authorities do?**

The situation is not very simple because European authorities are actually conflicted between the concern to protect the data of corporations and European nationals and the interest for law-enforcement authorities to be able to swiftly recover disclosed date directly from service providers without going through the cumbersome international judicial cooperation procedures.Many European leaders approve the Cloud Act, as they approved the position of the U.S. Justice Department in the warrant case, and consider that, at the heart of it, the new U.S. legislation is in line with the proposed e-Evidence Regulation of which they were the pioneers.These actors are pushing for the negotiation and signing of an executive agreement with the United States.As a general rule, this would have the advantage of creating the possibility for the GAFAM to object to requests for disclosure from U.S. authorities for European data within the new comity analysis objection procedure, which on the face of it is more reassuring than application of only the case law principle of international comity.

However, we still need to know what is behind this concept of an executive agreement.Indeed, the European Union and its Member States cannot accept to sign one or several agreements of this kind pursuant to which the United States, due to the importance of the GAFAM in the digital economy, would have access to worldwide, including European, data, regardless of their storage place, whereas European authorities could access data stored in the United States, but in no event involving US persons.The only possible attitude for the European Union, an attitude that would show a real concern for reciprocity and a fair balance between the need for fighting against crime and for protecting the Union's fundamental interests, would be to negotiate an agreement with the United States under which the authorities of each country would have smooth access to the data necessary for fighting against crime, and only such data, without consideration of their storage place and without discrimination as to the nationality of the persons or companies involved; with such an agreement necessarily having to be based on homogenous judicial review proceedings safeguarding the protection of the economic interests and fundamental rights of each partner's nationals.

If such agreement turned out to be possible, the European Union would then have to take the necessary steps to make the principle of international comity effective in U.S. courts.

At the French level, it would suffice to decide to apply the blocking act, after having strengthened it if necessary, notably by increasing the level of criminal penalties and by asking public prosecutors to initiate criminal proceedings.At the European level, it would suffice to enact an equivalent regulation prohibiting, subject to heavy penalties, any person or company registered or having an establishment within the European Union, from disclosing, outside of any international agreement, to private persons or foreign authorities, economic, commercial, industrial, financial or technical information involving European companies.Europe did this for personal data, therefore, potentially including the personal data of dangerous criminals.One cannot see why it would not do the same for its companies.

It is said that all blocking acts are ineffective because they place European companies between a hammer (the penalties that may be imposed by U.S. authorities on their U.S. interests) and an anvil (the penalties that may be imposed by European authorities on their European interests).The Iranian case is at the heart of this issue.However, the situation here is very different because the entities that may be placed in the vise are not European companies, but the European subsidiaries of U.S. companies, which is very different.

To conclude, it is not the Cloud Act that is dangerous for European companies.It is the way in which the European Union is going to react and the risks caused by the slowness of its decision-making process, if not its paralysis.