Octopus Conference, June 2012

Presentation Marcos Salt, Argentina

Transborder Access to Stored Computer Data in Latin American Countries

1. Objectives of the report

The objective of this presentation is to briefly analyze how Latin American countries work in those cases when it is crucial to access data kept in servers abroad, or even in cases of cloud computing, when it is supposedly impossible to determine the country where the server containing the digital evidence necessary for a criminal investigation is located (i.e. loss of location).

Situations will be analyzed from the current legal perspective and also from a practical point of view: in other words, we will see how the authorities are dealing with this problem in the ongoing investigations in LA countries.

Additionally, I intent to contribute some personal conclusions.

2. Description of the problem

Obtaining digital evidence both for the prosecution of the so-called cybercrimes, and for the investigation of any crime when the evidence is stored on computer systems, has led to the introduction of important changes in the criminal procedure systems, whose rules of evidence were designed bearing physical evidence in mind.

I think that is possible to say that this will become a PARADIGM shift in the criminal procedure law.

Several countries have modified their procedural law to grant the necessary tools for investigations in digital environments. On the contrary, other countries have carried out an analogous application of existing regulations for physical evidence, thus forcing their interpretation for those cases involving digital evidence. I do think this approach presents certain limitations and turns out to be insufficient, and therefore generates important problems which affect both the efficiency of the investigations and the appropriate protection of safeguards, in particular, the right to privacy.

The Budapest Convention noted this issue and designed a number of special procedural instruments for investigations in digital contexts, a fact which I consider one of its most relevant achievements.

However, the evolution of informatics and of communications technologies, specially the growing use of the Internet and the increasing trend towards cloud computing, have forced investigation systems to face new challenges, and added new stress on the traditional principles of criminal law.

In the case of the topic of this presentation, it is one of the most basic principles of criminal and international law which is at stake: Sovereign power- the founding stone

the procedural powers of all governments are based on, and the impassable limit imposed by physical boundaries in a country's prosecution of justice on foreign soil.

The problem arises when the efficiency in certain investigations puts the authorities in one country in the dilemma of needing access to information kept in servers abroad without relying on either the necessary procedural tools, or the necessary international cooperation channels, or the cooperation of the private sector to do so in **the legitimate and prompt way the investigation needs.**

Just like the easy perpetration of crime at a distance was a matter of concern in the investigation of cybercrime, and hence the need to harmonize legislations to avoid the impossibility of prosecution in countries which do not have the adequate penal legislation- computing safe havens- it is also necessary to adjust procedural laws to allow for investigative measures in an attempt to make the criminal prosecution effective. This is why adjusting procedural legislations has become paramount to enable criminal prosecution, and the standardization of legal tools appears to be an unavoidable and fundamental step to achieve efficiency in international criminal cooperation . In fact, I believe cooperation in this area previously requires the adjustment of procedures in the internal legislations of different countries.

In this context, it is nowadays necessary to pay attention to the problem which might result from countries or companies becoming "safe havens of evidence," a factor which could become an obstacle in investigative processes. This might be exemplified by the keeping of relevant information belonging to organized criminal groups in servers located in countries which do not have the suitable procedural instruments, or which do not admit any kind of international cooperation mechanism and guarantee **the inaccessibility of data without any exception.**

This new challenge requires special attention and new solutions which take into account the necessary balance between "the efficiency in the investigation of crimes "and the need of "protection of procedural guarantees in the digital world." Special attention should be given to finding ways to ensure citizens' right to privacy, and the freedom of speech, which could be jeopardized by regulations which lack an adequate balance of the principles at play.

Likewise, the problem puts the regional and international system in crisis in terms of criminal law, as it demands new forms of cooperation or the acceptance of the judicial intervention of one state in another one. This creates the need for new principles which observe a country's concept of sovereign power and the principle of equality, and which yet do not become an excuse to support interventionism.

The problem, which is extremely complex both legally and politically, is inescapably connected to the regulation of the cooperation between the private and the public sectors as in a high percentage of problematic cases, information is in the hands of the private sector- holder of the servers where the data under investigation is kept. Thus, it is not a question of merely international cooperation between countries but also between the private and the public sectors. Both subjects merge and interrelate in an unavoidable way, making the solution even more complex.

Some of the cases the authorities are dealing with today help exemplify the myriad of difficulties of the problems which call for regulatory solutions.

Case 1:

A judge orders a search and seizure warrant in the premises of a bank to get all the data available on suspect X. (The digital forensic expert who is in charge of the investigation, finds the required information but notices that, even if he has access to it from the computing terminals in the bank for which he has the search warrant, the information is located in a server in a foreign country.)

Can the search and seizure of the information be carried out without relying on the mechanisms of international cooperation which bond both countries?

Variation: Let us suppose that there is no access code to be cracked by the investigators, and since the information is available at the terminal for which we have a search and seizure warrant, is it valid to proceed to the copying of the information without moving it, or altering it, or securing it in any way?

Case 2:

In the course of an investigation, it is necessary to gain access to information contained on a webmail account, or to the documents kept in a server whose ISP is abroad. Is it necessary to channel the request through the mechanisms of international cooperation? Should the request be made directly to its commercial office in the country, or to the company headquarters where the server is located?

Sometimes, for technical reasons it is not even possible to know where the information is located at a specific time because it is constantly moved from server to server.

It seems obvious that the traditional general principles currently in force have not been adjusted to the challenges the digital age presents to both areas.

This has become even more noticeable due to the revolutionary changes brought about by the Internet, and turned out to be more complex yet, as a result of the growing tendency to keep information (potential evidence in a criminal investigation) in servers located in foreign jurisdictions or even in various servers located in indeterminate countries (cloud computing.)

Both the internal legislation in different countries and the regional treaties of cooperation currently in force in the criminal field, are still tied to the territoriality principle and the validity and protection of the principle of sovereignty of different countries, in other words, to the physical borders as "impregnable barriers" for the intervention of the legal system of one country in another one. Criminal law, in general, bears territorial application; this means that it has value only within the confines of the territory which sanctioned it, a principle which dominates the application of criminal law in space in such a way that the perpetration of the crime (*forum delicti commissi*), regardless of the ambiguities which the word "perpetration" leads to, determines the applicable criminal law, and solves the legal conflicts which could exist by way of principle.

Power of Procedures: ***Lex fori*** is the principle which rules the application of procedural law when it is necessary to decide the application of *one* of several laws simultaneously in force.

This principle states that the competent court to conduct proceedings applies the procedural law enacted by the sovereign power which created the court ,and which

invested it with its jurisdictional powers. A judge ordinarily applies the law corresponding to the sovereign power which invested it, wherever this might be, except in the case of a clearly stated exception .

In the context of the most important regional agreements, though nimble international cooperation systems are procured, they remain observant of every state's sovereignty and the *lex fori* principle.

The general criteria of these three international tools are:

* A state party is not granted the right to execute jurisdictional functions in another state's territory.

* The applications are executed according to the law of the state required to act. As long as their legislations are not incompatible, the requested state is allowed to apply incompatible forms and procedures specially requested by the soliciting state.

* Both the substantive and the procedural laws of the requested state are applied in the case of injunctions (searches, seizures, embargos, etc.) .

In conclusion, it is possible to say that, according to the general principle of sovereignty which upholds the principles which rule the application of criminal law in space, the procedural powers and tools which every country has to carry out an investigation in digital contexts can be used only by its authorities within its territory.According to the regulations currently in force in the region, in those cases when the authorities notice that the evidence must be obtained in a foreign country, they should request it through the mechanisms of international cooperation existing between them.

3. Practice beats regulations?

According to the information collected from judicial authorities and police forces specialized in investigating technological crimes, there are not any clear, written directives which regulate the issue in the countries of the region. Therefore, in cases similar to the ones in the scenario of Assumption 1 detailed at the beginning of this talk, in general, if it is not necessary to break codes, the investigators will go on to copy the data. Moreover, it is usual not even to inform the judge when getting information has involved entering a server located abroad. In practice, the idea that the information has been accessed through a terminal housed in the location covered by a search and seizure warrant prevails, and the fact that the server is located elsewhere is deemed irrelevant.

A computer expert specialized in obtaining digital evidence who was interviewed about the subject explained to me: 'The problem with lawyers is that they have lost their common sense: *they want to apply principles and concepts from a world with physical borders to the Internet phenomenon, which is borderless by nature"*. Obviously, it is not that we, jurists, do not have common sense, but, rather, that we are bound by legal regulations which might have become outdated.

The truth is that, according to experts and police force specialists, in their everyday practice, if the search warrant enables them to have access to a location and, in turn, to the information in the computer terminals there, they will do so regardless of the place where the data is held. That is to say that, in practice, the criterion applied

was that of *"location of the terminal from where the information is accessed."* If the location of the terminal is covered by the search warrant, they do not pay attention to the location of the server they are accessing. There seems to be only one exception: the access to the information should not entail carrying out special computing operations such as "cracking access codes."

In the case of the cooperation of the public sector with the private one, there are no clear rules either. Still less are there regulations stemming from international laws or agreements. On the contrary, in practice the situation is solved by means of formal or informal agreements with different companies, and they are not the same agreements, nor are they applied similarly in all the countries of the region. Often, they are not actually "agreements" but "unilaterally" drawn up guidelines which the private sector hands in to the authorities (of the different countries). These include details on the information which can be obtained, how it can obtained, under what conditions, and which the mechanisms to get it are.

This anomy is peculiar as, in fact, the private sector has actually become a kind of lawmaker which regulates how and when it cooperates with the authorities of the various countries. This entails a risk, not only in terms of the efficiency of the investigations but also in terms of the protection of personal data which could be subject to regulations which are barely clear and constantly changing.

It is worth mentioning that, in two of the scenarios described at the beginning of the paper, transborder access to data takes place without the participation of the authority of the state where the server holding the information is, and without any letter rogatory.

I believe the absence of legal discussion on both subjects at the legal or academic level has favored these practices which have led to the solution of these problems so far. This has happened without any legal consideration for the possible violation of the principles of sovereign power or the possible nullity of the evidence obtained. It is obvious that this solution, primarily based on the ignorance of the problem on the part of the operators of the judicial system, will not be definitive, and will demand clearer regulatory solutions.

4. Conclusions

- Efficiency in the investigations in digital contexts calls for tackling the problems derived from countries or companies becoming *safe heavens of evidence,* a factor which might hinder the investigations by taking advantage of the huge development of cloud computing and the possibility of information storage in other jurisdictions.
- Generally speaking, both in the legislation of the Latin American countries and in the regional cooperation agreements , sovereignty has such influence that it determines the procedural powers and procedural tools applied by every country for investigations in digital contexts within their own territory (*lex fori*). Thus, due to the regulations in force in the region, if the evidence must be obtained in a foreign country, the authorities should request the

information to that country through the appropriate mechanisms of international cooperation existing between them.

- The new mechanisms provided by procedural law and international cooperation must ensure that the efficiency in the investigation does not become a threat to human rights, an excuse to justify interventionism between countries and the excessive intervention of the state in the activities of service companies.
- From my point of view, Art. 32 in CoC does not address the practical problems that the transborder access to data generates nowadays, and requires some reinterpretation or re-elaboration in the light of the growth of the storage of information through cloud computing, and of the experience gained in the last few years.
- Thus, I would advise the introduction of guidelines or recommendations which contribute to the practical application of rules, or even some amendment or additional protocol on digital evidence where this subject is dealt with special attention .
- I understand it is necessary to take a different approach to the situation of the data, which though stored in another territory, is undeniably under the control of an individual or corporate identity in the territory where the investigation is taking place.
- A new interpretation of the concept lawful *authority to disclosure data* is necessary. Since it will always implies a weakening in the sovereign power of states, this possibility must be foreseen as an exception, and the sending of a prompt notification to the state where the information is stored should be introduced.
- It is necessary to regulate the **procedures** for the application of measures which imply transborder access, that is to say, not only to define the exceptional cases where this course of action is admissible, but also the way they will be carried out, and the safeguards inherent to that measure.