Aspects of Criminal Procedural Law in Argentina.

The purpouse of this brief presentation is to inform about the reform underway in Criminal Procedure Law and its compliance with the standards of the CoC.

This is an important issue and we believe that the compliance with CoC provisions it is harder to solve than the substantial criminal law (definition of crimes) in which there is more consensus in the comparative law[1].
On the other side, Procedural and international cooperation provisions of CoC are more controversial in the academic an political discussion[2] , not only in Argentina, also in other countries that are analyzing CoC.

On February 2007 the Executive Power created a special commission. One of the main issues of this commission was to elaborate an integral Draft of criminal procedure law[3] in order to modify the federal system. The commission ended its work on 6th September 2007 and sent the Draft of Criminal Procedure Law to the Minister of Justice. **The Draft of Law has not been already sent to the Congress.**

It is important to point out that **this draft (and in general, the objective of the commission) is not specially related to cyber crime**. It's an integral reform of the Criminal Procedure Law and, because of that reason, CoC procedural provisions were only taking in account in the evidence chapter. But to analyze in a correct manner the compliance between the text of the draft of Criminal Procedure Law and the CoC provisions, is necessary to review the entire system of the draft an not only some articles isolated dedicated to the digital evidence.

Regarding this report, it is important to note that the Draft of Criminal Procedural Law establishes in the evidence chapter, some regulations in order to suit traditional rules of evidence (search, seizure, interception) to answer

[1] Also Argentina has a draft of criminal substantive law regarding cyber crime with enormous consensus in the academic and political world that we believe it has not conflicts with the requirement of the CoC.
[2] In addition , Argentina is a federal country composed by 23 provinces and the city of Buenos Aires. In accordance with the Federal Constitution, Criminal Code is a federal matter but procedural law depends of the legislative power of each province (state).
[3] Decreto nro. 115 del Poder Ejecutivo Nacional.

the challenge of digital evidence and the new technological environment. In the Draft, the rules of the European Convention on Cybercrimes were specially taken in account.

Besides I think that the draft, in general, satisfy the requirements of the CoC , we have to highlight that some of the procedural issue of CoC were not been stipulated in the draft. In some cases, it was believed that they were issues that should been seen in a future modification of Telecommunications Law (for instance, the Draft do not establish the obligations of service providers and other data holders).
In relation to international cooperation, it was out of the power of the Commission.

In order to article 14 of CoC is important to point out that the draft of Criminal Procedure Law doesn't limit the application of the evidence rules analyzed to specific crime investigations. Contrary, it is applicable to every investigation involving digital evidence or committed by means of a computer system.

In order to article 15 of CoC, the analysis requires the systematic study of the complete draft and its references to the Constitution and the International Human Rights Conventions. The correct analysis to understand that the draft do satisfy the requirements of CoC remit to general rules stipulated in the general principles of the draft, specially articles 4 and 6 and article 137.

In order with article 16 of CoC, Article 181[4] of the Draft of Criminal Procedure Law establishes a law framework in order to the **expedited preservation of stored computer data and traffic data**. The article establishes that the Prosecutor[5] can issue an order to retain informatics data for 90 days in order to request a judicial order to allow use it in a criminal proceeding. The Draft of Law does not have a specific provisions directly prescribed to the partial disclosure of traffic data (COE, 17). The Draft of Law neither refers to an obligation of the data holder to keep the confidential of the order of preservation.

In order with article 18 of CoC, general rules of evidence can be applied to satisfy article 18.a and partially 18.b. but it could be necessary to modify the Telecommunications Law to regulate in a proper way obligations of service provider.

In order with article 19 of the CoC, article 181 of the draft establishes the collection of evidence in informatics systems **with a judicial order** (search and seizure) giving the tools to implement the article 19 of the CoC. The article 181 divides the search of computer data (*"The Judge could, as a result of a request and by a grounded resolution, order **a search** of an informatics system or part of it, or a computer-data storage medium..."*) from the seizure(*"to **seize** the components of the system, **obtain a copy or preserve the data** or other interesting issue to the investigation"*).
Even the draft doesn't provide specified rule to allow the extension of the search to other system in connection (art. 19, 2 CoC) it can be interpreted by

---

[4] Article 181. The Judge could, as a result of a request and by a grounded resolution, order **a search** of an informatics system or part of it, or a computer-data storage medium, in order to **seize** the components of the system, **obtain a copy or preserve the data** or other interesting issue to the investigation, under the conditions establishes in Section 167.
Even before the initial request, the Prosecutor could order the preservation or protection of informatics and electronics data when there are grounds to believe the data could be loss or modify. This measure could be extended for 90 days, in order to obtain the judicial order.
Once the components of the system was seized or it was obtained a copy of the data, they will be analyze by the Prosecutor, who will decide if the components will be remain seized or the data will be keep. If the Prosecutor evaluates the opposite he will order the devolution of the components or the destruction of the data's copies which were made. The Party could request to the Judge the devolution of the components or the destruction of the data's copies.
(It is important to point out that this is not an official translation of the Spanish version)

[5] According to the Draft of Criminal Procedure Law the criminal investigation is headed by the Prosecutor with judicial control.

the general rule of the draft that allow the authorities to ask to the judge the extension of any search.
In relation with rule 19, 4 (CoC) it is not covered by the draft. There is a discussion about the risk of the self incrimination that this article could implies.

The article 190[6] of the draft establishes the interception of any kind of communications, always issued by a Judge. **This article could be use to satisfy Section 20 and 21 CoC**:

- **a.** real time collection of traffic data (*"Under the same conditions **could order to obtain traffic data related to any kind of communications"***)
- **b.** real time interception of content data (*interception or record of phone calls and any **other communications made by other technical media***)

In this case, article 190 do establishes the obligation for telecommunications provider to keep the order confidential.

---

[6] **Article 190 Interception, copy and record**
The Judge, as a result of a request and by a grounded resolution, could order the interception or record of phone calls and any **other communications made by other technical media** by the accused or other people who communicate to the accused. Under the same conditions **could order to obtain traffic data related to any kind of communications**.
The request and, in that case, the judge resolution which authorizes the interception or recording, should mention telephone line's data or other communication, if it is possible the personal data of the person affected by the measure, also should mention its duration and the authority in charge of the task.
The provider communication companies should allow the immediate implement of the measure, if not they will criminally prosecute. All those who will be dealing with the judicial order and the companies' officials must keep confidentiality in connection with the measure and they could reveal the information only if the judicial authority allow them to do it.
If the grounds which were taken in account to order the measure disappear, the time granted expires, or if the objective of the judicial order has been achieved , this should be interrupt immediately.
Apart from those complex investigations, the wiretapping should not been for more than 30 days, an extension for other 30 days could be granted just once if it is requested by a Party and it is grounded by the Judge. This should be ground in principles of necessity, subsidiary and proportionality based on the results obtained.
Exceptionally, when the results show the necessity of its extension could be authorize other extensions. In any case the wiretapping could last more than 180 days, base on the same conditions.

Note: It is important to state that the articles commented are integrated in a whole draft of Criminal Procedure Law that is in the beginning of its discussion which probably take a long time of analysis. The articles related to cyber crime could be improve in this analysis or could be separate in a special law if it is necessary to satisfy CoC requirements before the approval of the Criminal Procedure Law.