Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 April 2011
Provisional/Restricted

Criminal procedure law provisions on cybercrime in Latin America

regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru)

Prepared by

Marcos Salt (Argentina)

Project funded by contributions from Estonia, Monaco, Japan, Romania, Microsoft and McAfee and by the Council of Europe

Contact

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-8841-2103
Fax: +33-3-9021-5650
Email: cristina.schulman@coe.int
www.coe.int/cybercrime

Contents

1 Introduction

On 26 and 27 of August 2010 a workshop was held in Mexico City on "Meeting the challenge of cybercrime in Latin America". The regional workshop was organised by Mexican authorities (the Council of National Security of Mexico) and the Council of Europe with the support of Microsoft.

Participants from Argentina, Colombia, Costa Rica, Mexico, Paraguay and Peru as well as public-private sector and academia participated in the event. These countries are analyzing the convenience and possibilities to accede to the Budapest Convention being also in the process of reforming their respective legislation, regarding cybercrime (both in Criminal Substantive law and Criminal procedure law). The workshop gathered decision-makers and subject-matter experts involved in this process in each country and analysed existing or draft legislation in view of reforming the legislation against the Budapest Convention.

During the workshop, points of view and experiences were exchanged on the status of national legislations and their compliance with the Budapest Convention. The legislative country profiles of the different countries were updated with information provided by participants. It was also an important issue during the workshop the relation and cooperation between public and private sector, sharing experiences from the different countries, difficulties and good practices.

The scope of this report is to provide a brief analysis of the criminal procedure provisions from these countries and their compliance with the Budapest Convention.

A point made during the discussions was the slow pace of criminal procedural law reform compared to criminal substantive law reform, which has evolved significantly in the countries analysed. Moreover, the same conclusion can be drawn from the legislative country profiles, which hardly include procedural rules to investigate computer crimes, or crimes committed through computer systems or that require digital evidence, as expressly is required by the Budapest Convention.

As it will be explained in further detail, in these countries the procedural law present shortcomings due to the fact that the evidence chapters of criminal procedural law were drafted to apply to physical evidence, without considering special measures for obtaining digital evidence, with some exceptional isolated measures. Such exception will be noted in the analysis below, however, they do not amount to a comprehensive system of rules as the one established by the Convention.

In reality, the procedural rules that apply to physical evidence are applied by analogy to the challenging situations posed by digital evidence, giving rise to problems in the jurisprudence, which should be resolved[1]. The issue of procedural criminal law reform lagging behind criminal substantive law reform also happened in other regions, such as Europe (in German, Portuguese and Spanish laws).

In spite of that, it should be noted that **during the workshop each the procedural rules proposed by the Convention was analysed and the countries' representatives generally realized the importance of implementing the procedural tools set forth by the Convention on Cybercrime in the national legislations.** Consequently, there was a general agreement on the need to work on future procedural reforms in different countries in order to integrate the powers and procedural tools to the respective Criminal Procedure Codes, adapting them to the specific characteristics of each procedural system, without hindering the constitutional rights sanctioned in each system and the Human Rights Treaties in force in each Region. At the same time, it is important to point out that **the most important regional organizations such as the**

[1] See, Marcos Salt, "Tecnología Informática¿Un nuevo desafío para el Derecho Procesal Penal?

Organization of American States (OAS) and the Meeting of Ministers of Justice and Attorney Generals of the Americas (REMJA), are constantly reminding member states to adapt their legislations taking the Council of Europe Convention as a reference.

Many participants noted that in practice the courts in their countries applied many of the measures set forth by the Convention such as search and seizure of stored computer data (Article 19) or interception of content data (Article 21) are being applied by analogy using other effective rules.

2 General Remarks

It is convenient to shed some light into the recent history of the criminal process in Latin America in order to understand the context in which the procedural systems which are subject of the present study are applied. This would also help to assess the possibilities of introducing amendments to the criminal procedure codes in the region, using similar models, and thus enhancing cooperation between the countries. Moreover, such uniformity would also facilitate technical assistance for the drafting of amendments of procedural rules in the different countries.

Latin American criminal procedural systems share some basic characteristics which were brought about by a reform movement across the continent starting at the beginning of the 80s and still on progress. They are quite modern as they represent (on the criminal system) the principles underlying the political reform movement introduced by democracy in the region, replacing old inquisitorial codes by new ones that respond to a more accusatorial approach, respect of human rights and the rule of law[2].

Even if slight differences exist, the procedural codes of the countries under analysis are part of the mentioned movement, presenting similar structural characteristics, which make it possible to think on a homogenous amendment of their rules to better adapt to the Budapest Convention standards.

Among these countries, Mexico has not adopted yet the reform of the procedural law at federal level, but there is draft currently subject to intense debate both at academic and political levels. The rest of the countries have reformed their procedural legislations, although the process is dynamic and constantly changing.

This political movement made possible to reform in gradual stages virtually all the procedural codes in the region following similar guidelines, which resulted in systems that share many similarities. This is an important advantage considering future regional uniform reforms regarding the compliance with the Convention on Cybercrime and the international cooperation.

These modern codes, however, do not have specific rules governing cybercrime in general and, specially, the peculiar nature of digital evidence; rather the rules on obtaining physical evidence are actually applied by analogy, which creates difficulties in court proceedings.

The similar structural characteristics shared by criminal procedural codes of the countries from the region and the fact that the reform movement is still under way are good starting points for implement the procedural powers with similar structures for an efficient prosecution and better international cooperation in fighting computer related crimes, taking consideration of the compliance with the Convention requirements.

In this sense, as a result of the analysis during the workshop it is possible to conclude that **Criminal Procedure Codes of the countries under analysis on this report have not been adapted according with the challenge of an efficient prosecution and international cooperation on cybercrime**. Instead, they still apply the rules for obtaining physical evidence by analogy. As we will see below on the specific analysis of the situation in the different countries, some countries have introduced isolated rules concerning digital evidence but they still lack an

[2] See, J Maier, K Ambos and J. Woischnik, "Las Reformas Procesales Penales en América Latina", Max Planck Institute, Konrad Adenauer Stiftung, Ad Hoc, Buenos Aires, 2000.

integrated model (for example Chile)[3]. Others, like Argentina or Costa Rica are in a further step as they have already drafted criminal procedure laws using the Budapest Convention as an important model.

However, as it has been previously pointed out, many procedural measures are actually applied using effective rules by analogy. An interesting example in the region is the Dominican Republic, with a Procedural Criminal Code of similar characteristics to that of the countries subject to this analysis, but which has introduced amendments specifically targeted at obtaining digital evidence. Dominican Republic's cybercrime law is one of the most complete of the region with specific procedural rules on this subject.

The Dominican Republic Law goes further than the Budapest Convention and regulate also "data retention obligation" for internet service provider[4], which is an oblihgation at the European Union level but not required by the Convention on Cybercrime, which provides for the obligation of the preservation of data (article 16 and 17 COC)[5]. These is important to clarify, taking in account the controversy generated on different countries from Latin America (also in Europe) about data retention laws.

Another important issue worthwhile mentioning is that many speakers highlighted during the workshop that their countries have set up special offices specifically for cybercrime and that there has been significant progress in training. In some countries these are special units dependant on the police force or other Executive Power dependencies such as the CERTS; in other countries, they reported prosecutors specialized in cybercrime.

[3] See, Marcos Salt , "IDENTITY RELATED CRIME IN LATIN AMERICAN COUNTRIES": "In this sense I point out important deficiencies in procedural laws in the region. If we consider the model proposed by the Council of Europe (Convention on Cyber crime-ETS Nro. 185) for the prosecution of cybercrimes and crimes that require obtaining digital evidence, we can see that most legal systems have not been amended to adapt to the new requirements and apply the rules for obtaining physical evidence by analogy. Some countries have introduced isolated rules concerning digital evidence but they still lack an integrated model. For this reason, I think that this will be one of the key issues to consider in an assistance plan to help countries in the region to adapt their respective laws…".

[4] Article 56. Service providers. Without prejudice to the provisions of Article 47 b) of this law, service providers must store traffic, connection and access data and any other information which might be useful for investigations, for a minimum period of 90 (INDOTEL) will set out the regulations on procedures for obtaining and storing data and information by service providers for a period of 6 months from the publication of this law. These regulations should take into account the importance of preserving evidence, regardless of the number of service providers involved in the data transmission or communication.

5 See Explanatory Report, points 149,150 and 151.

3 Scope of the procedural provisions

Convention on Cybercrime (Article 14 – Scope of procedural provisions)

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i. is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

It is important to point out that in general, criminal procedural laws in Latin American countries (same the countries under analysis on this report) do not limit their application to specific crime investigations. On the contrary, usually the evidence chapter of the criminal procedure code is applicable to any investigation.

There are some specific criminal laws that have specific procedure rules chapters or special powers to law enforcement (such as money laundering laws or kidnapping).

In order to satisfy the compliance with Convention on Cybercrime and for a better legislative policy it is recommended to amend the Criminal Procedure Codes, especially the evidence chapter.

During the workshop, participants stated that it is not problematic to amend the criminal procedure codes in order to introduce provisions on the powers and procedures established under Convention, not only for cybercrimes (article 14 a) but also the situations described in article 14 b and c

4 Conditions and Safeguards

Cybercrime Convetion (Article 15 - Conditions and Safeguards)

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

All the countries analysed in this report have ratified the American Convention on Human Rights (CADH, see Appendix[i]), furthermore, Argentina, for example, has incorporated it to its Constitution.

This international instrument on human rights may be compared to those set forth in article 15, guaranteeing an adequate protection of human rights and freedoms.

Therefore, notwithstanding the particularities of each National Constitution and criminal procedural code, all these countries meet from a legislative standpoint the requirements of article 15, as many of them, protect rights and guarantees in accordance to international standards in their respective laws.

It was also analyzed the possibility that the different countries adopt rules to govern guarantees in a more specific way than in the Convention on Cybercrime, seting forth conditions and safeguards for each one of the procedural measures.[6].

AMERICAN CONVENTION ON HUMAN RIGHTS "PACT OF SAN JOSE, COSTA RICA"

PART I - STATE OBLIGATIONS AND RIGHTS PROTECTED
CHAPTER I - GENERAL OBLIGATIONS
Article 1. Obligation to Respect Rights
1. The States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition.
2. For the purposes of this Convention, "person" means every human being.

[6] See Convention on Cybercrime, Explanatory Report, points 145-148.

Article 2. Domestic Legal Effects
Where the exercise of any of the rights or freedoms referred to in Article 1 is not already ensured by legislative or other provisions, the States Parties undertake to adopt, in accordance with their constitutional processes and the provisions of this Convention, such legislative or other measures as may be necessary to give effect to those rights or freedoms.
Article 5. Right to Humane Treatment
1. Every person has the right to have his physical, mental, and moral integrity respected.
2. No one shall be subjected to torture or to cruel, inhuman, or degrading punishment or treatment. All persons deprived of their liberty shall be treated with respect for the inherent dignity of the human person.
3. Punishment shall not be extended to any person other than the criminal.
4. Accused persons shall, save in exceptional circumstances, be segregated from convicted persons, and shall be subject to separate treatment appropriate to their status as unconvicted persons.
5. Minors while subject to criminal proceedings shall be separated from adults and brought before specialized tribunals, as speedily as possible, so that they may be treated in accordance with their status as minors.
6. Punishments consisting of deprivation of liberty shall have as an essential aim the reform and social readaptation of the prisoners.
Article 7. Right to Personal Liberty
1. Every person has the right to personal liberty and security.
2. No one shall be deprived of his physical liberty except for the reasons and under the conditions established beforehand by the constitution of the State Party concerned or by a law established pursuant thereto.
3. No one shall be subject to arbitrary arrest or imprisonment.
4. Anyone who is detained shall be informed of the reasons for his detention and shall be promptly notified of the charge or charges against him.
5. Any person detained shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to be released without prejudice to the continuation of the proceedings. His release may be subject to guarantees to assure his appearance for trial.
6. Anyone who is deprived of his liberty shall be entitled to recourse to a competent court, in order that the court may decide without delay on the lawfulness of his arrest or detention and order his release if the arrest or detention is unlawful. In States Parties whose laws provide that anyone who believes himself to be threatened with deprivation of his liberty is entitled to recourse to a competent court in order that it may decide on the lawfulness of such threat, this remedy may not be restricted or abolished. The interested party or another person in his behalf is entitled to seek these remedies.
7. No one shall be detained for debt. This principle shall not limit the orders of a competent judicial authority issued for nonfulfillment of duties of support.
Article 8. Right to a Fair Trial
1. Every person has the right to a hearing, with due guarantees and within a reasonable time, by a competent, independent, and impartial tribunal, previously established by law, in the substantiation of any accusation of a criminal nature made against him or for the determination of his rights and obligations of a civil, labor, fiscal, or any other nature.
2. Every person accused of a criminal offense has the right to be presumed innocent so long as his guilt has not been proven according to law. During the proceedings, every person is entitled, with full equality, to the following minimum guarantees:
a. the right of the accused to be assisted without charge by a translator or interpreter, if he does not understand or does not speak the language of the tribunal or court;
b. prior notification in detail to the accused of the charges against him;
c. adequate time and means for the preparation of his defense;
d. the right of the accused to defend himself personally or to be assisted by legal counsel of his own choosing, and to communicate freely and privately with his counsel;
e. the inalienable right to be assisted by counsel provided by the state, paid or not as the domestic law provides, if the accused does not defend himself personally or engage his own counsel within the time period established by law;
f. the right of the defense to examine witnesses present in the court and to obtain the appearance, as witnesses, of experts or other persons who may throw light on the facts;

g. the right not to be compelled to be a witness against himself or to plead guilty; and
h. the right to appeal the judgment to a higher court.
3. A confession of guilt by the accused shall be valid only if it is made without coercion of any kind.
4. An accused person acquitted by a nonappealable judgment shall not be subjected to a new trial for the same cause.
5. Criminal proceedings shall be public, except insofar as may be necessary to protect the interests of justice.
Article 25. Right to Judicial Protection
1. Everyone has the right to simple and prompt recourse, or any other effective recourse, to a competent court or tribunal for protection against acts that violate his fundamental rights recognized by the constitution or laws of the state concerned or by this Convention, even though such violation may have been committed by persons acting in the course of their official duties.
2. The States Parties undertake:
a. to ensure that any person claiming such remedy shall have his rights determined by the competent authority provided for by the legal system of the state;
b. to develop the possibilities of judicial remedy; and
c. to ensure that the competent authorities shall enforce such remedies when granted.

5 Argentina

It is important to point out that Argentina is a federation composed of 23 Provinces and the city of Buenos Aires.

In accordance to the Federal Constitution, criminal code is a federal matter but procedural law depends on legislative power of each Province. The report will focus only on the federal level.

The Criminal Procedure Code currently in force (law N° 23.984 effective since 1992) does not include specific rules regarding cybercrime as it applies to all types of crimes, nor does it specific rules regarding digital evidence. It includes specific rules with respect to telephone communications interception.

In Argentina, the freedom of evidence applies and so these rules are applied by analogy to the different situations involving digital evidence, although there are practical difficulties related to their application, which underscore the need to introduce amendments.

Cybercrime law 26.388, which was passed on June 4, 2008, sets forth amendments to the Criminal Code, with respect to the definition of key terms such as document, signature, execution, as well as to equating electronic mail to postal mail so that these definitions can be applied to criminal rules governing evidence.

On February 2007, the Executive Power created a special commission to elaborate an integral Draft of criminal procedure law[7] on 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. However, the **draft law has not passed the Congress.** It is important to point out that **this draft was not specially related to cyber crime**.

The draft criminal procedural law establishes in the evidence chapter regulations in order to adjust traditional rules of evidence (search, seizure, interception) to the challenge of digital evidence and the new technological environment. The provisions of the Budapest Convention on Cybercrimes were in particular taken into account[8].

Bearing in mind the difficulties to pass an integral and comprehensive reform of the criminal procedure code, which will take time, and taking into account that Argentina started the official steps to become Party to the Convention on Cybercrime, the executive power created a special commission to reform the evidence chapter of the Criminal Procedure Law in accordance with the Convention on Cyber crime of the Council of Europe. The commission ended his work and presented a draft of law on October 2010 (see full text of the draft of law)[ii] including on the Criminal Procedure Law the powers and procedures provided by the Convention.

[7] Decreto nro. 115 del Poder Ejecutivo Nacional.

[8] See. Marcos Salt, *Law Aspects of Criminal Procedural Law in Argentina,* Octopus, 2008.

CONVENTION ON CYBERCRIME	NATIONAL LAW
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and	**Criminal Procedure law in force** Los medios de prueba en el CPPN están regulados en el titulo III art. 216-278. Los medios de prueba regulados son: Capítulo I (CPP, 216-223), Inspección judicial, CPP; Capítulo II (CPP, 224-230bis) Registro domiciliario y requisa personal; Capítulo III (CPP, 231-238bis) Secuestro; Capítulo IV (CPP, 239-252) Testigos; Capítulo V (CPP, 253-267) Peritos; Capítulo VI (CPP, 268—269) Intérpretes; Capítulo VII (CPP, 270-275) Reconocimientos; Capítulo VIII (CPP, 276-278) Careos. Rige la libertad de probatoria CPP, 206 Art. 206. - No regirán en la instrucción las limitaciones establecidas por las leyes civiles respecto de la prueba, con excepción de las relativas al estado civil de las personas.

ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	Más allá de las previsiones constitucionales antes señalas, el CPP establece en sus primeros artículos como principios rectores del sistema. TITULO I Garantías fundamentales, interpretación y aplicación de la ley Juez natural, juicio previo. Presunción de inocencia. "Non bis in idem". Artículo 1° - Nadie podrá ser juzgado por otros jueces que los designados de acuerdo con la Constitución y competentes según sus leyes reglamentarias, ni penado sin juicio previo fundado en ley anterior al hecho del proceso y sustanciado conforme a las disposiciones de esta ley, ni considerado culpable mientras una sentencia firme no desvirtúe la presunción de inocencia de que todo imputado goza, ni perseguido penalmente más de una vez por el mismo hecho. Interpretación restrictiva y analógica Art. 2° - Toda disposición legal que coarte la libertad personal, que limite el ejercicio de un derecho atribuido por este Código, o que establezca sanciones procesales, deberá ser interpretada restrictivamente. Las leyes penales no podrán aplicarse por analogía. "In dubio pro reo" Art. 3° - En caso de duda deberá estarse a lo que sea más favorable al imputado.
Article 16 – Expedited preservation of stored computer data	**Criminal Procedure Code in force: it does not specifically establish any**

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**obligation to preserve stored computer data** **This data is in general requested through evidence reports to communications service suppliers- telephone or Internet-; or through sworn depositions. The reports reports and depositions are cumpolsory for individuals provided that they are not protected by self incrimination guarantee.** Art. 133. - Los tribunales podrán dirigirse directamente a cualquier autoridad administrativa, la que prestará su cooperación y expedirá los informes que le soliciten dentro del tercer día de recibido el pedido del juez o, en su caso, en el plazo que éste fije. Deber de interrogar Art. 239. - El juez interrogará a toda persona que conozca los hechos investigados, cuando su declaración pueda ser útil para descubrir la verdad. Se aplican también las normas referidas a correspondencia e intervención de comunicaciones. Intercepción de correspondencia **Draft law:** ARTICULO 232 ter.- El juez, o el fiscal cuando se encuentre a cargo de la investigación, podrá ordenar, por auto fundado, a cualquier persona física o jurídica la conservación y protección de datos contenidos en un dispositivo de almacenamiento informático cuando existan razones para suponer que esos datos puedan ser modificados o eliminados. La orden deberá contener con el mayor detalle posible los datos contenidos en un dispositivo de almacenamiento informático a preservar y el tiempo de conservación de los mismos, que podrá alcanzar el término máximo de noventa días, prorrogable por otro idéntico, siempre que se mantengan los motivos que dieron origen como fundamento a la orden. Durante el cumplimiento de la orden, su destinatario deberá adoptar todas las medidas técnicas y organizativas de seguridad necesarias para que aquélla se mantenga en secreto."
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be	**The Criminal Procedure Code in force does not specifically provide for the obligation to preserve traffic data.**

preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**This data is in general requested through evidence reports to communications service suppliers- telephone or Internet-; or through sworn depositions. The reports and depositions are cumpolsory for individuals.** Art. 133. - Los tribunales podrán dirigirse directamente a cualquier autoridad administrativa, la que prestará su cooperación y expedirá los informes que le soliciten dentro del tercer día de recibido el pedido del juez o, en su caso, en el plazo que éste fije. **Draft Law:** ARTICULO 236 bis. El juez podrá ordenar, por auto fundado, la obtención, aún en tiempo real, del contenido de las comunicaciones transmitidas por un sistema informático, para impedirlas o conocerlas. Bajo las mismas condiciones, el juez podrá ordenar también la obtención, aún en tiempo real, de los datos de tráfico correspondientes a esas comunicaciones."
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical	**Criminal Procedure Law in force:** Art. 133. - Los tribunales podrán dirigirse directamente a cualquier autoridad administrativa, la que prestará su cooperación y expedirá los informes que le soliciten dentro del tercer día de recibido el pedido del juez o, en su caso, en el plazo que éste fije. Deber de interrogar Art. 239. - El juez interrogará a toda persona que conozca los hechos investigados, cuando su declaración pueda ser útil para descubrir la verdad. Obligación de testificar **Draft of Law:** ARTICULO 6º.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 232 bis: "Orden de presentación de datos contenidos en un dispositivo de almacenamiento informático y de datos de usuarios y/o abonados". ARTICULO 232 bis.- El juez, o el fiscal cuando se encuentre a cargo de la investigación, podrá ordenar por auto fundado, a cualquier persona física o jurídica la presentación de datos contenidos en un dispositivo de almacenamiento informático que este bajo su poder o control y al que pueda acceder.

provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Asimismo, podrá ordenar a toda persona física o jurídica que preste un servicio a distancia por vía electrónica la entrega de la información que esté bajo su poder o control referida a los usuarios y/o abonados o los datos con los que cuente de los usuarios y/o abonados a dicho servicio."
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data;	**Criminal Procedure Law in Force:** **The rules regarding search and seizure are applied by analogy.** Registro Art. 224. - Si hubiere motivo para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito, o que allí puede efectuarse la detención del imputado o de alguna persona evadida o sospechada de criminalidad, el juez ordenará por auto fundado el registro de ese lugar. El juez podrá proceder personalmente o delegar la diligencia en el fiscal o en los funcionarios de la policía o de las fuerzas de seguridad. En caso de delegación, expedirá una orden de allanamiento escrita, que contendrá: la identificación de causa en la que se libra; la indicación concreta del lugar o lugares que habrán de ser registrados; la finalidad con que se practicará el registro y la autoridad que lo llevará a cabo. El funcionario actuante labrará un acta conforme lo normado por los artículos 138 y 139 de este Código. En caso de urgencia, cuando medie delegación de la diligencia, la comunicación de la orden a quien se le encomiende el allanamiento podrá realizarse por medios electrónicos. El destinatario de la orden comunicará inmediatamente su recepción al Juez emisor y corroborará que los datos de la orden, referidos en el párrafo anterior, sean correctos. Podrá usarse la firma digital. La CORTE SUPREMA DE JUSTICIA DE LA NACION o el órgano en que ésta delegue dicha facultad, reglamentará los recaudos que deban adoptarse para asegurar la seriedad, certidumbre y autenticidad del procedimiento. (Párrafo incorporado por art. 5° de la Ley N° 25.760 B.O. 11/8/2003)

c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Cuando por existir evidente riesgo para la seguridad de los testigos del procedimiento, fuese necesario que la autoridad preventora ingrese al lugar primeramente, se dejará constancia explicativa de ello en el acta, bajo pena de nulidad. Si en estricto cumplimiento de la orden de allanamiento, se encontrare objetos que evidencien la comisión de un delito distinto al que motivó la orden, se procederá a su secuestro y se le comunicará al juez o fiscal interviniente. (Artículo sustituido por art. 3° de la Ley N° 25.434 B.O. 19/6/2001) Orden de secuestro Art. 231. - El juez podrá disponer el secuestro de las cosas relacionadas con el delito, las sujetas a decomiso o aquellas que puedan servir como medios de prueba. Sin embargo, esta medida será dispuesta y cumplida por los funcionarios de la policía o de las fuerzas de seguridad, cuando el hallazgo de esas cosas fuera resultado de un allanamiento o de una requisa personal o inspección en los términos del artículo 230 bis, dejando, constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o al fiscal intervinientes. (Artículo sustituido por art. 5° de la Ley N° 25.434 B.O. 19/6/2001) **Draft law:** En el caso de que en la diligencia se hallaran dispositivos de almacenamiento informático y hubiere motivos suficientes para presumir que estos pudieren contener datos relativos a la investigación, el Juez ordenará que se obtenga una copia forense de tal dispositivo. Para el caso en que fuera imposible, ordenará el secuestro del dispositivo o, en su caso, que se conserven los datos en él contenidos de conformidad con las disposiciones contenidas en el artículo 232 ter, tercer párrafo. El registro de él o los dispositivos hallados no podrá extenderse más allá del objeto de la orden respectiva, bajo pena de nulidad.”
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and	**The Criminal Procedure Code in force does not set forth specific rules about the collection of traffic data in real time.** **Dichos datos suelen ser solicitados a través de pruebas de informes a empresas proveedoras de servicios de comunicaciones —telefónicas o de Internet—; o**

b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**declaraciones testimoniales. Estos informes y declaraciones son obligatorias para los particulares.** Art. 133. - Los tribunales podrán dirigirse directamente a cualquier autoridad administrativa, la que prestará su cooperación y expedirá los informes que le soliciten dentro del tercer día de recibido el pedido del juez o, en su caso, en el plazo que éste fije. Art. 236. - El juez podrá ordenar, mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedirlas o conocerlas. Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él. (Párrafo incorporado por art. 7° de la Ley N° 25.760 B.O. 11/8/2003) En las causas en que se investigue alguno de los delitos previstos en los artículos 142 bis y 170 del CODIGO PENAL DE LA NACION, o que tramiten en forma conexa con aquéllas, cuando existiese peligro en la demora, debidamente justificado, dichas facultades podrán ser ejercidas por el representante del MINISTERIO PUBLICO FISCAL, mediante auto fundado, con inmediata comunicación al Juez, quien deberá convalidarla en el término improrrogable de veinticuatro horas, bajo pena de nulidad del acto y consecuente ineficacia de la prueba introducida a partir de él. (Párrafo incorporado por art. 7° de la Ley N° 25.760 B.O. 11/8/2003) **Draft of Law**: ARTICULO 236 bis. El juez podrá ordenar, por auto fundado, la obtención, aún en tiempo real, del contenido de las comunicaciones transmitidas por un sistema informático, para impedirlas o conocerlas. Bajo las mismas condiciones, el juez podrá ordenar también la obtención, aún en tiempo real, de los datos de tráfico correspondientes a esas comunicaciones.”
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical	**The Criminal Procedure Code in force does not establish specific rules governing the collection of content data in computer systems in real time. The rules about communications interception are applied by analogy.** Art. 236. - El juez podrá ordenar, mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedirlas o conocerlas. Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que

capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	hubiere de las comunicaciones del imputado o de quienes se comunicaran con él. (Párrafo incorporado por art. 7° de la Ley N° 25.760 B.O. 11/8/2003) En las causas en que se investigue alguno de los delitos previstos en los artículos 142 bis y 170 del CODIGO PENAL DE LA NACION, o que tramiten en forma conexa con aquéllas, cuando existiese peligro en la demora, debidamente justificado, dichas facultades podrán ser ejercidas por el representante del MINISTERIO PUBLICO FISCAL, mediante auto fundado, con inmediata comunicación al Juez, quien deberá convalidarla en el término improrrogable de veinticuatro horas, bajo pena de nulidad del acto y consecuente ineficacia de la prueba introducida a partir de él. (Párrafo incorporado por art. 7° de la Ley N° 25.760 B.O. 11/8/2003) **Draft Law**: ARTICULO 236 bis. El juez podrá ordenar, por auto fundado, la obtención, aún en tiempo real, del contenido de las comunicaciones transmitidas por un sistema informático, para impedirlas o conocerlas. Bajo las mismas condiciones, el juez podrá ordenar también la obtención, aún en tiempo real, de los datos de tráfico correspondientes a esas comunicaciones.”

6 Chile

The Procedural Code of Chile is one of the most advanced in the region. It is worth noting that this code was launched along with a whole new judicial organization system, which has been regarded as a model in the region. Even if it does include provisions for gathering of digital evidence (such as art. 222 which establishes an obligation to retain data by ISPs) it is not an integrated system with all the measures established by the convention. In many cases the traditional rules are applied by analogy based on the freedom of evidence principle.

CONVENTION ON CYBERCRIME	**NATIONAL LAW**
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.	**The procedure to punish crimes, felonies and offences is laid donw in the Criminal Procedure Code.** **There is not a specific procedure addressing this type of crimes.**

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	Se encuentran previstas en la Constitución y en el Código Procesal Penal.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**The Criminal Procedure Law does not have such a measure but includes a rule on Data Retention.** Artículo 222 inciso quinto del Código Procesal Penal, norma que regula en forma acotada la obligación de empresas de telecomunicaciones y telefónicas de guardar un listado autorizado de las direcciones IP de sus clientes por al menos 6 meses. Artículo 222.- Interceptación de comunicaciones telefónicas. Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación. La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios. No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados. La orden que dispusiere la interceptación y grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la

	duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes. Las empresas telefónicas y de telecomunicaciones deberán otorgar a los funcionarios encargados de la diligencia las facilidades necesarias para llevarla a cabo. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento. Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**There is not a specific rule for this procedural measure.** Artículo 222 inciso quinto del Código Procesal Penal en los términos anteriormente señalados.

Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**There is not a specific rule on production order of digital data. Rules governing evidence in the Criminal Procedure Law are applied by analogy, which is considered an adequate solution.** Artículo 180.- Investigación de los fiscales. Los fiscales dirigirán la investigación y podrán realizar por sí mismos o encomendar a la policía todas las diligencias de investigación que consideraren conducentes al esclarecimiento de los hechos. Sin perjuicio de lo dispuesto en el Párrafo 1º de este Título, dentro de las veinticuatro horas siguientes a que tomare conocimiento de la existencia de un hecho que revistiere caracteres de delito de acción penal pública por alguno de los medios previstos en la ley, el fiscal deberá proceder a la práctica de todas aquellas diligencias pertinentes y útiles al esclarecimiento y averiguación del mismo, de las circunstancias relevantes para la aplicación de la ley penal, de los partícipes del hecho y de las circunstancias que sirvieren para verificar su responsabilidad. Asimismo, deberá impedir que el hecho denunciado produzca consecuencias ulteriores. Los fiscales podrán exigir información de toda persona o funcionario público, los que no podrán excusarse de proporcionarla, salvo en los casos expresamente exceptuados por la ley. Artículo 19.- Requerimientos de información, contenido y formalidades. Todas las autoridades y órganos del Estado deberán realizar las diligencias y proporcionar, sin demora, la información que les requirieren el ministerio público y los tribunales con competencia penal. El requerimiento contendrá la fecha y lugar de expedición, los antecedentes necesarios para su cumplimiento, el plazo que se otorgare para que se llevare a efecto y la determinación del fiscal o tribunal requirente. Con todo, tratándose de informaciones o documentos que en virtud de la ley tuvieren carácter secreto, el requerimiento se atenderá observando las prescripciones de la ley respectiva, si las hubiere, y, en caso contrario, adoptándose las precauciones que aseguraren que la información no será divulgada. Si la autoridad requerida retardare el envío de los antecedentes solicitados o se negare a enviarlos, a pretexto de su carácter secreto o reservado y el fiscal estimare indispensable la realización de la actuación, remitirá los antecedentes al fiscal regional quien, si compartiere esa apreciación, solicitará a la Corte de Apelaciones respectiva que, previo informe de la

	autoridad de que se tratare, recabado por la vía que considerare más rápida, resuelva la controversia. La Corte adoptará esta decisión en cuenta. Si fuere el tribunal el que requiriere la información, formulará dicha solicitud directamente ante la Corte de Apelaciones. Si la razón invocada por la autoridad requerida para no enviar los antecedentes solicitados fuere que su publicidad pudiere afectar la seguridad nacional, la cuestión deberá ser resuelta por la Corte Suprema. Aun cuando la Corte llamada a resolver la controversia rechazare el requerimiento del fiscal, por compartir el juicio de la autoridad a la que se hubieren requerido los antecedentes, podrá ordenar que se suministren al ministerio público o al tribunal los datos que le parecieren necesarios para la adopción de decisiones relativas a la investigación o para el pronunciamiento de resoluciones judiciales. Las resoluciones que los ministros de Corte pronunciaren para resolver estas materias no los inhabilitarán para conocer, en su caso, los recursos que se dedujeren en la causa de que se tratare.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or	El comiso se encuentra regulado en el artículo 217 del Código Procesal Penal, el cual señala que los objetos y documentos relacionados con el hecho investigado, los que pudieren ser objeto de la pena de comiso y aquellos que pudieren servir como medios de prueba, serán incautados, previa orden judicial librada a petición del fiscal, cuando la persona en cuyo poder se encontraren no los entregare voluntariamente, o si el requerimiento de entrega voluntaria pudiere poner en peligro el éxito de la investigación. Artículo 218 del Código Procesal Penal regula este tema sólo para obtener copias o respaldos de la correspondencia electrónica. Artículo 217.- Incautación de objetos y documentos. Los objetos y documentos relacionados con el hecho investigado, los que pudieren ser objeto de la pena de comiso y aquellos que pudieren servir como medios de prueba, serán incautados, previa orden judicial librada a petición del fiscal, cuando la persona en cuyo poder se encontraren no los entregare voluntariamente, o si el requerimiento de entrega voluntaria pudiere poner en peligro el éxito de la investigación. Si los objetos y documentos se encontraren en poder de una persona distinta del imputado, en lugar de ordenar la incautación, o bien con anterioridad a ello, el juez podrá apercibirla para que los entregue. Regirán, en tal caso, los medios de coerción previstos para los

similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	testigos. Con todo, dicho apercibimiento no podrá ordenarse respecto de las personas a quienes la ley reconoce la facultad de no prestar declaración. Cuando existieren antecedentes que permitieren presumir suficientemente que los objetos y documentos se encuentran en un lugar de aquellos a que alude el artículo 205 se procederá de conformidad a lo allí prescrito. Artículo 218.- Retención e incautación de correspondencia. A petición del fiscal, el juez podrá autorizar, por resolución fundada, la retención de la correspondencia postal, telegráfica o de otra clase y los envíos dirigidos al imputado o remitidos por él, aun bajo nombre supuesto, o de aquéllos de los cuales, por razón de especiales circunstancias, se presumiere que emanan de él o de los que él pudiere ser el destinatario, cuando por motivos fundados fuere previsible su utilidad para la investigación. Del mismo modo, se podrá disponer la obtención de copias o respaldos de la correspondencia electrónica dirigida al imputado o emanada de éste. El fiscal deberá examinar la correspondencia o los envíos retenidos y conservará aquellos que tuvieren relación con el hecho objeto de la investigación. Para los efectos de su conservación se aplicará lo dispuesto en el artículo 188. La correspondencia o los envíos que no tuvieren relación con el hecho investigado serán devueltos o, en su caso, entregados a su destinatario, a algún miembro de su familia o a su mandatario o representante legal. La correspondencia que hubiere sido obtenida de servicios de comunicaciones será devuelta a ellos después de sellada, otorgando, en caso necesario, el certificado correspondiente.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory	**There is not a specific rule.**

transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be	**Section 222 of the Criminal Procedure Code for other type of communications, applies only to crimes punishable by more tan 5 years. This restriction makes it imposible to apply this measure to computer crimes, which are awarded a lesser punishment.**

necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

7 Colombia

Even if the Criminal Procedure Code (law 906, 8/31/2004) does not establish all the procedural measures provided for by the Convention nor an integrated model targeted at the gathering of digital evidence, it includes specific rules concerning digital evidence. Thus, selective search in databases, even if it is a power of the judicial police, while conducting an investigation, on condition that it is used to confirm publicly known information. Moreover, as other codes in the region, it provides for the interception of telephone and other similar communications.

Colombian procedural law includes provisions concerning information given in the Internet or other electronic media. In this way, it sets forth the seizure order for computers and servers, discs and other storage hardware, so that computer crime investigation experts may discover, collect, analyze and safeguard the recovered information. It expressly establishes that the criteria for records and search warrants shall apply by analogy. Last, it provides that the seizure will last the time necessary to capture the information, after which the impounded equipments shall be released.

CONVENTION ON CYBERCRIME	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences	Artículo 24. *Ambito de la jurisdicción penal.* Las indagaciones, investigaciones, imputaciones, acusaciones y juzgamientos por las conductas previstas en la ley penal como delito, serán adelantadas por los órganos y mediante los procedimientos establecidos en este código y demás disposiciones complementarias

specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i.is being operated for the benefit of a closed group of users, and iidoes not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying	Título preliminar, Principios rectores y Garantías procesales. Artículo 1 al 27.

application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	No está regulado.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Partially ruled. Preservation is not cumpolsory although it is an obligation to immediately disclose the traffic data.** Artículo 244. Búsqueda selectiva en bases de datos. La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. Cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos. En estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information"	There is not a procedural rule that adequately addresses this requirement specifically for computer data. The rule about evidence reports may be applied by analogy.

means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or	Artículo 236. Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados. Artículo 244. Búsqueda selectiva en bases de datos. La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de

similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	informaciones de acceso público. Cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos. En estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory	Artículo 235. Interceptación de comunicaciones telefónicas y similares. El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be	Se cumple Parcialmente mediante el siguiente artículo de la ley procesal Artículo 235. Interceptación de comunicaciones telefónicas y similares. El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

8 Costa Rica

Costa Rica's Criminal Procedure Code (Law N° 7594 of April 10, 1996) does not include specific procedural rules regarding digital evidence that adequately meet the European Convention's standards. During the workshop, Costa Rica's representatives stated the convenience of amending their internal legislation, notwithstanding that many of the measures established by the convention are applied by analogy of other criminal rules.

There is also a draft law on the matter included in the country profile.

CONVENTION On CYBERCRIME	**NATIONAL LAW**
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the	"ARTICLE 9.- AUTHORIZATION OF INTERVENTIONS. (DRAFT LAW) The article 9 of the Law about Registration, Seizure and Examination of Private Documents and Interception of Telecommunications No.7425 of August 09th, 1994 will be read as follows: Within the procedure of a police or a jurisdictional investigation, the court can authorized the intervention of oral, written or another type of communications even the permanent, mobiles, wireless or digital telecommunications when it involves the clarification of the following crimes: cyber crimes or executed through the use of computer, electronic, telematic, optical or by magnetic means, kidnapping for the objective of ransom, aggravated corruption, aggravated pimp, manufacture or production of pornography, trafficking of persons and trafficking of persons to trade their organs; aggravated murder; genocide, terrorism and the crimes foresee in the Law on Narcotics, Psychotropic Substances, Drugs of Unauthorized Use, Money-Laundering and related activities, N° 8204 from December 26th, 2001. In the same cases, such courts can authorized the intervention of communications between the presents, except what the second paragraph of article 26 of the present law establishes; when produce within dwellings and private spaces, the intervention can only

measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	be authorized if there are enough signs that an unlawful activity is being executed."
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the	

sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary	

to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or	

arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be	

necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.	

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

9 México

The Criminal Procedure Code of Mexico has not yet been comprehensively reformed. A draft is currently under discussion. It is probable that the procedural system will be of an accusatorial nature similar to the systems of other countries in the region.

It is worth noting that similar to Argentina, Mexico is a federal country, and thus it faces the same difficulties when attempting to adequate its rules to the Convention on Cybercrime requirements.

According to section 278 bis of Mexico's Federal Criminal Procedure Code in force, telecommunications or internet providers shall collaborate with government authorities in the gathering of evidence if so required.

Nota de vigencia: El artículo 133 Bis, reformado por Decreto publicado en el Diario Oficial de la Federación el 23 de enero de 2009, "estará vigente hasta en tanto entre en vigor el sistema procesal acusatorio a que se refiere el Decreto por el que se reforman los artículos 16, 17, 18, 19, 20, 21 y 22, las fracciones XXI y XXIII del artículo 73, la fracción VII del artículo 115 y la fracción XIII del apartado B, del artículo 123 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 18 de junio de 2008" (DOF 23-01-2009, artículo Segundo Transitorio).

CONVENTION ON BUDAPEST	**NATIONAL LAW**
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation,	El Titulo sexto, capítulo I, se ocupa de los medios de prueba están regulados en los artículos 206-290. Se prevé el principio de libertad probatoria en el artículo 206. Se regulan diversos medios de prueba (Capitulo II, Confesión, art. 207), (Capítulo III, inspección, art. 208-219), (Capítulo IV, Peritos, art. 220-239), (Capítulo V, Testigos, art. 240-257), (Capítulo VI, Confrontación, art. 258-264), (Capítulo VII, Careos, art. 265-268), (Capítulo VIII, Documentos, art. 269-278), (Capítulo IX, Valor jurídico de la prueba, art. 279- 290). **There are no explicit references to digital evidence, but according to section 206- freedom of evidence- the rules may be applied by analogy. In addition, the code authorizes the recording of communications between persons, or any recording, as evidence, provided it complies with certain requirements. (CPM, art. 278).**

provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the	El artículo 154 dispone que al inculpado se le deben hacer saber las garantías que le otorga el artículo 20 de la constitución política de los Estados Unidos Mexicanos. En el artículo 20 de la constitución mexicana se prevén las principales garantías frente al enjuiciamiento en sede penal. Sin perjuicio de que las garantías penales están previstas en otros artículos. Así, por ejemplo, juez natural (CM, art. 13), legalidad (CM, art. 14), inviolabilidad de la privacidad (CM, art. 16), libertad personal (CM, art. 16), etc.

sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**El código procesal vigente no prevé una medida similar.**
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**The procedural code in force does not include a similar measure.**

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**The procedural code in force does not include a similar measure.** Artículo 278 Bis.- Las comunicaciones entre particulares podrán ser aportadas voluntariamente a la averiguación previa o al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma. El tribunal recibirá las grabaciones o video filmaciones presentadas como prueba por las partes y las agregará al expediente. Las comunicaciones que obtenga alguno de los participantes con el apoyo de la autoridad, también podrán ser aportadas a la averiguación o al proceso, siempre que conste de manera fehaciente la solicitud previa de apoyo del particular a la autoridad. De ser necesario, la prueba se perfeccionará con las testimoniales o periciales conducentes. En ningún caso el Ministerio Público o el juez admitirán comunicaciones que violen el deber de confidencialidad que establezca la Ley, ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber. No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber. Las empresas concesionarias y permisionarias del servicio de telecomunicaciones o de internet, estarán obligadas a colaborar con las autoridades para la obtención de dichas pruebas cuando así lo soliciten. Cualquier omisión o desacato a esta

	disposición será sancionada por la autoridad, en los términos del artículo 178 del Código Penal Federal. Carecen de todo valor las comunicaciones que sean obtenidas y aportadas en contravención a las disposiciones señaladas en este Código.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be	**The effective procedural code does not include a similar measure. Based on the freedom of evidence principle the rules of search and seizure of physical evidence may be applied by analogy.**

necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**The procedural code in force does not include a similar measure.**

Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Even if the procedure code does not provide for a similar measure specifically for comunications transmitted by means of a computer system, the general rules goberning communications interception are applied.** Artículo 278 Ter.- Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el Procurador General de la República o los servidores públicos en quienes delegue la facultad, la autoridad judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves. El Ministerio Público será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen. En la autorización, el juez determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración. En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenará que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio y video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

	El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo, sin que ello suceda, el juez que autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las investigaciones, los originales y sus copias, y ordenará su destrucción en presencia del Ministerio Público.

10 Paraguay

As is the case with most of the procedural codes passed in the 90's, the Criminal Procedure Code (law n° 1286-98) of Paraguay does not include rules regarding digital evidence, and collection of information through electronic media. Traditional evidence rules are applied by analogy, with measures regarding communications interception.

CONVENTION ON CYBERCRIME	**NATIONAL LAW**
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.	Artículo N° 200 - INTERVENCIÓN DE COMUNICACIONES El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas. El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. La intervención de comunicaciones será excepcional. Artículo N° 199 - APERTURA Y EXAMEN DE CORRESPONDENCIA Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta. Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario. Artículo N° 198 - INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA Siempre que

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Artículo N° 192 - OPERACIONES TÉCNICAS Las restricciones establecidas para el allanamiento de domicilios o habitaciones no regirán para las oficinas administrativas o edificios públicos, templos o lugares religiosos, establecimientos militares, lugares comerciales de reunión o de esparcimiento, abiertos al público y que no estén destinados a habitación familiar. En estos casos se podrá prescindir de la orden de allanamiento con el consentimiento expreso y libre de las personas a cuyo cargo estén los locales. En caso de negativa o imposibilidad material de conseguir el consentimiento, se requerirá la orden de allanamiento y se podrá hacer uso de la fuerza policial para su cumplimiento. Quien prestó el consentimiento será invitado a presenciar el registro. Para el ingreso y registro de oficinas dependientes de un poder del Estado se necesitará autorización del funcionario competente. Si durante el desarrollo del procedimiento, quien dio la autorización, la niega o expresa haberla consentido por coacción, la prueba de la libertad del consentimiento corresponderá a quien lo alega. En el acta respectiva se consignarán los requisitos previstos por este código y el consentimiento otorgado. Artículo N° 195 - ORDEN DE SECUESTRO No podrán ser objeto de secuestro: 1) las comunicaciones escritas entre el imputado y las personas que puedan abstenerse de declarar como testigos por razón de parentesco o que deban hacerlo en razón del secreto;

	2) las notas que hayan tomado los nombrados anteriormente sobre comunicaciones confiadas por el imputado, o sobre cualquier circunstancia, a las cuales se extienda el derecho o el deber de abstenerse de declarar; y, 3) los resultados de exámenes o diagnósticos relativos a las ciencias médicas realizados bajo secreto profesional. La limitación sólo regirá cuando las comunicaciones u objetos estén en poder de aquellas personas que pueden abstenerse de declarar; o en el caso de abogados y profesionales de las ciencias médicas, si están archivadas o en poder del estudio jurídico o del establecimiento hospitalario y consultorios privados. Artículo N° 183 - REGISTRO Cuando haya motivo suficiente que permita suponer que en un lugar público existen indicios del hecho punible investigado o la presencia de alguna persona fugada o sospechosa, si no es necesaria una orden de allanamiento, la policía realizará directamente el registro del lugar. Cuando sea necesario realizar una inspección personal o el registro de un mueble o compartimento cerrado destinado al uso personal, en lugar público, regirán análogamente los artículos que regulan el procedimiento de la inspección de personas o vehículos. Se invitará a presenciar el registro a quien habite o se encuentre en posesión del lugar, o cuando esté ausente, a su encargado y, a falta de éste, a cualquier persona mayor de edad. Cuando sea posible se conservarán los elementos probatorios útiles. Artículo N° 176 - INSPECCIÓN DEL LUGAR DEL HECHO La policía deberá custodiar el lugar del hecho y comprobará, mediante la inspección del lugar y de las cosas, los rastros y otros efectos materiales que sean consecuencia del hecho punible.

	El funcionario policial a cargo de la inspección labrará un acta que describa detalladamente el estado de las cosas y cuando sea posible, recogerá y conservará los elementos probatorios útiles, dejando constancia. El acta será firmada por dos testigos hábiles, en lo posible vecinos del lugar, que no deberán tener vinculación con la policía; bajo esas formalidades podrá ser incorporada al juicio por su lectura. Artículo N° 173 - LIBERTAD PROBATORIA Los hechos y circunstancias relacionados con el objeto del procedimiento podrán ser admitidos por cualquier medio de prueba, salvo las excepciones previstas por las leyes. Un medio de prueba será admitido si se refiere, directa o indirectamente, al objeto de la investigación y es útil para el descubrimiento de la verdad. El juez o tribunal limitará los medios de prueba ofrecidos cuando ellos resulten manifiestamente excesivos.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular	Constitución Nacional: Artículo N° 16 - De la defensa del juicio La defensa en juicio de las personas y de sus derechos es inviolable. Toda persona tiene derecho a ser juzgada por tribunales y jueces competentes, independientes e imparciales. Artículo N° 17 - De los derechos procesales En el proceso penal, o en cualquier otro del cual pudiera derivarse pena o sanción, toda persona tiene derecho a: 1. que sea presumida en su inocencia 2. que se le juzgue en juicio público, salvo los casos contemplados por el magistrado para salvaguardar otros derechos 3. que no se le condene sin juicio previo fundado en una ley anterior al hecho del proceso, ni que se le juzgue por tribunales especiales 4. que no se le juzgue mas de una vez por el mismo hecho. No se pueden reabrir procesos fenecidos, salvo la revisión favorable de sentencias penales establecidas en los casos previstos por la ley procesal

the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	5. que se defienda por si misma o sea asistida por defensores de su elección 6. que el Estado le provea de un defensor gratuito, en caso de no disponer de medios económicos para solventarlos 7. la comunicación previa y detallada de la imputación, así como a disponer de copias, medios y plazos indispensables para la preparación de su defensa en libre comunicación 8. que ofrezca, practique, controle e impugne pruebas 9. que no se le opongan pruebas obtenidas o actuaciones producidas en violación de las normas jurídicas 10. el acceso, por sí o por intermedio de su defensor, a las actuaciones procesales, las cuales en ningún caso podrán ser secretas para ellos. El sumario no se prolongará mas allá del plazo establecido por la ley, y a 11. la indemnización por el Estado en caso de condena por error judicial Articulo 17 – De los derechos procesales Articulo 18 - De las restricciones de la declaración Articulo 19 - De la prisión preventiva Articulo 20 - El objeto de las penas Articulo 21 – De las reclusión de personas Articulo 30 – De las señales de comunicación electromagnética CPP: Articulo 1 – Juicio Previo
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order	Código Procesal Penal: Artículo N° 228 - INFORMES El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Código Procesal Penal: Artículo N° 228 - INFORMES El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar. Resolución 1134/2006 " Reglamento del Servicio de Acceso Internet" Art. 17: " El Prestador instalará en el país, un sistema de gestión, cuyo propósito es la gestión técnica y administrativa del servicio. El sistema deberá registrar al menos: - Habitación/deshabilitación, de estaciones del usuario, velocidad de transmisión, volumen de tráfico, datos de facturación. Se deberá mantener archivos históricos de los registros.

Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Artículo N° 52 - FUNCIONES DE INVESTIGACION Corresponde al Ministerio Público, por medio de los agentes fiscales, funcionarios designados y de sus órganos auxiliares, dirigir la investigación de los hechos punibles y promover la acción penal pública. Con este propósito realizará todos los actos necesarios para preparar la acusación y participar en el procedimiento, conforme a las disposiciones previstas en este código y en su ley orgánica. Tendrá a su cargo la dirección funcional y el control de los funcionarios y de las reparticiones de la Policía Nacional, en tanto se los asigne a la investigación de determinados hechos punibles. Otros Medios de Prueba Artículo N° 228 - INFORMES El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar. Artículo N° 58 - FUNCIÓN Los agentes y funcionarios de la Policía Nacional, en su función de investigación de hechos punibles, actuarán a través de cuerpos especializados designados al efecto, y a iniciativa del Ministerio Público ejecutará los mandatos de la autoridad competente, sin perjuicio del régimen jerárquico que los organiza.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly	Artículo N° 183 - REGISTRO Cuando haya motivo suficiente que permita suponer que en un lugar público existen indicios del hecho punible investigado o la presencia de alguna persona fugada o

access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	sospechosa, si no es necesaria una orden de allanamiento, la policía realizará directamente el registro del lugar. Cuando sea necesario realizar una inspección personal o el registro de un mueble o compartimento cerrado destinado al uso personal, en lugar público, regirán análogamente los artículos que regulan el procedimiento de la inspección de personas o vehículos. Se invitará a presenciar el registro a quien habite o se encuentre en posesión del lugar, o cuando esté ausente, a su encargado y, a falta de éste, a cualquier persona mayor de edad. Cuando sea posible se conservarán los elementos probatorios útiles. Artículo N° 192 OPERACIONES TECNICAS y Artículo N° 193 - ENTREGA DE COSAS Y DOCUMENTOS Para mayor eficacia y calidad de los registros e inspecciones, se podrán ordenar operaciones técnicas o científicas, reconocimientos y reconstrucciones. Artículo N° 196 - PROCEDIMIENTO La orden de secuestro será expedida por el juez, en una resolución fundada. Artículo N° 198 - INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Regirán las limitaciones del secuestro de documentos u objetos.

Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Código Procesal Penal: Artículo N° 228 - INFORMES El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. (TRAFICO) Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and	Artículo N° 200 - INTERVENCIÓN DE COMUNICACIONES El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas. El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de

b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. La intervención de comunicaciones será excepcional. Artículo N° 199 - APERTURA Y EXAMEN DE CORRESPONDENCIA Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta. Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario. Artículo N° 198 - INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Regirán las limitaciones del secuestro de documentos u objetos.

11 Perú

In accordance with Article 104 of the Constitution of Peru passed by Law No. 28269 on July 4, 2004, the national Congress delegated to the Executive Power, the power to pass through a congressional order a new Criminal Procedure Code and its implementation. The Peruvian Criminal Procedure Code was made law by Congresional Order 957 and published on July 29, 2004.

The evidence chapter of the Criminal Procedure Code and the Country Profile do not contain any specific rules relating to the gathering of digital evidence. The majority of the measures provided by the Convention could only be complied with by applying effective rules by analogy. These provisions should be amended if adequate compliance with the Convention on Cybercrime requirements is to be met.

The Peruvian Criminal Procedural Code provides for the interception, recording and register of telephone communications, and other means of communication, but only for serious crimes. It establishes that the prosecutor may request such a measure to the judge if the alleged crime is one punishable by imprisonment of more than four years. It also establishes rules providing the way in which the recording shall be done, through tape recording or other analogous technical means that ensure a reliable method as well as privacy of the information.

The recording must be delivered to the prosecutor who will order to be kept following strict safety and privacy measures. The prosecutor shall also have a written transcript of the content made and a deed executed, besides of keeping the original tape. The irrelevant recordings will be eventually given back to the affected persons, and the transcript destroyed by the Attorney General's Office.

The Peruvian Criminal Procedure Code dictates that telephone and communications companies shall allow interceptions, tapings or recordings, or be punished for contempt of a government authority.

CONVENTION ON CYBERCRIME	**NATIONAL LAW**
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention;	El CPP prevé en la Sección II: La prueba, Título III: la búsqueda de pruebas y restricción de derechos, específicamente en su capítulo VI : La Exhibición Forzada y la incautación , comprendiendo: Exhibición e incautación de bienes, la exhibición e incautación de actuaciones y documentos no privados. Posteriormente, en su Capítulo VII: El control de las Comunicaciones y Documentos Privados.

b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International	Artículo VIII: DEL TÍTULO PRELIMINAR DEL CÓDIGO PROCESAL PENAL DEL 2004: Legitimidad de la Prueba 1- Todo medio de prueba será valorado sólo si ha sido obtenido e incorporado al proceso por un procedimiento constitucionalmente legítimo 2- Carecen de efecto legal las pruebas obtenidas, directa o indirectamente, con violación del contenido esencial de los derechos fundamentales de la persona. 3- La inobservancia de cualquier regla de garantía constitucional establecida a favor del procesado no podrá hacerse valer en su perjuicio.

Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for	There is not a procedural rule that adequately addresses this requirement. Artículo 221°.- Conservación y exhibición 1- Según la naturaleza y estado del bien incautado, se dispondrá su debida conservación o custodia. **Artículo 230°.- Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación**

the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	There is not a procedural rule that adequately addresses this requirement. **Articulo 230°.- intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación** 1.-El fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al juez de la investigación preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4 del artículo 226. 2.- La orden judicial puede dirigirse contra el investigado o contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que recibe o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación. 3.- El requerimiento del fiscal y en su caso la resolución judicial que la acuerda deberá indicar el nombre y dirección del afectado por la medida, así como, de ser posible, la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir o grabar o registrar. También indicará la forma de la intercepción, su alcance y su duración, al igual que la autoridad o funcionario, policial o de la propia fiscalía, que se encargará de la diligencia de interceptación y grabación o registro. 4.- Las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les citara como testigo al procedimiento. 5.- Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o hubiere trascurrido el plazo de duración fijado para la misma, ella deberá

	ser interrumpida inmediatamente. 6- La interceptación no podrá durar más de treinta días. Excepcionalmente podrá prorrogarse por plazo sucesivo previo requerimiento del fiscal y decisión motivada del juez de la investigación preparatoria.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	There is not a procedural rule that adequately addresses this requirement. **Articulo 230°.- intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación** **(....)** 4.- Las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les citara como testigo al procedimiento.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be	There is not a procedural rule that adequately addresses this requirement. The search and seizure rules are applied by analogy.

necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	There is not a procedural rule that adequately addresses this requirement **Articulo 230°.- intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación** 4.- Las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les citara como testigo al procedimiento. 6- La interceptación no podrá durar más de treinta días. Excepcionalmente podrá prorrogarse por plazo sucesivo previo requerimiento del fiscal y decisión motivada del juez de la investigación preparatoria.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and	**Articulo 230°.- intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación** 4.- Las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les

b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	citara como testigo al procedimiento. 6- La interceptación no podrá durar más de treinta días. Excepcionalmente podrá prorrogarse por plazo sucesivo previo requerimiento del fiscal y decisión motivada del juez de la investigación preparatoria.

12 Appendix

***DECLARATIONS/RESERVATIONS/DENUNCIATIONS/WITHDRAWLS CADH**

Chile:
(Declaration made at the time of signature)
The Delegation of Chile signs this Convention, subject to its subsequent parliamentary approval and ratification,
in accordance with the constitutional rules in force.
(Reservations made at the time of ratification)
Recongnition of Competence:

a) The Government of Chile declares that it recognizes, for an indefinite period of time and on the condition of reciprocity, the competence of the Inter-American Commission on Human Rights to receive and examine communications in which a State Party alleges that another State Party has committed a violation of the human rights established in the American Convention on Human Rights, as provided for in Article 45 of the Convention.

b) The Government of Chile declares that it recognizes as binding, ipso facto, the jurisdiction of the Court on all matters relating to the interpretation or application of the Convention in accordance with its Article 62.

In making these declarations, the Government of Chile places on record that this recognition of the competence and jurisdiction of the Commission applies to events subsequent to the date of deposit of this instrument of ratification or, in any case, to events which began subsequent to March 11, 1990.
Moreover, in acknowledging the competence and jurisdiction of the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights, the Government of Chile declares that, when these bodies apply the provisions of Article 21.2 of the Convention, they may not make statements concerning the reasons of public utility or social interest taken into account in depriving a person of his property.

Argentina:
(Reservation and interpretative declarations made at the time of ratification)
The instrument of ratification was received at the General Secretariat of the OAS on September 5, 1984, with a reservation and interpretative declarations. The notification procedure of the reservation was taken in conformity with the Vienna Convention on the Law of Treaties signed on May 23, 1969.
The texts of the above-mentioned reservation and of the interpretative declarations are the following:
I. Reservation:
Article 21 is subject to the following reservation: "The Argentine Government establishes that questions relating to the Government's economic policy shall not be subject to review by an international tribunal. Neither shall it consider reviewable anything the national courts may determine to be matters of 'public utility' and 'social interest', nor anything they may understand to be 'fair compensation'."
II. Interpretative Declarations:
Article 5, paragraph 3, shall be interpreted to mean that a punishment shall not be applied to any person other than the criminal, that is, that there shall be no vicarious criminal punishment.
Article 7, paragraph 7, shall be interpreted to mean that the prohibition against "detention for debt" does not involve prohibiting the state from basing punishment on default of certain debts, when the punishment is not imposed for default itself but rather for a prior independent, illegal, punishable act.
Article 10 shall be interpreted to mean that the "miscarriage of justice" has been established by a national court.
Recognition of Competence:
In the instrument of ratification dated August 14, 1984, and deposited with the General Secretariat of the OAS on September 5, 1984, the Government of Argentina recognizes the competence of the Inter-American Commission on Human Rights and on the jurisdiction of the Inter-American Court of Human Rights. This recognition is for an indeterminate period and on condition of reciprocity on all cases related to the interpretation or application of the Convention cited, with the partial reservation and bearing in mind the interpretative statements contained in the instrument of ratification.

The instrument of ratification further notes that the obligations undertaken by virtue of the Convention shall only be effective as regards acts that have occurred after the ratification of the above-mentioned instrument.

Colombia:
Recognition of Competence:
On June 21, 1985, presented an Instrument of acceptance by which recognizes the competence of the Inter-American Commission on Human Rights for an indefinite time, on the condition of strict reciprocity
and nonretroactivity, for the cases involving the interpretation or application of the Convention, and reserves the right to withdraw its recognition of competence should it deem this advisable. The same Instrument recognizes the jurisdiction of the Inter-American Court of Human Rights, for an indefinite time, on the condition of reciprocity and nonretroactivity, for cases involving the interpretation or application of the Convention, and reserves the right to withdraw its recognition of competence should it deem this advisable.

Costa Rica:
Recognition of Competence:
Presented on July 2, 1980, at the General Secretariat of the OAS an instrument recognizing the competence of the Inter-American Commission on Human Rights and the jurisdiction of the Inter-American Court of Human Rights, in accordance with Articles 45 and 62 of the Convention.
(Declaration and reservations made at the time of ratification)
1)That Costa Rica declares that it recognizes, without conditions and while the American Convention on Human Rights remains in effect, the competence of the Inter-American Commission to receive and examine
communications in which a State Party alleges that another State Party has committed a violation of human rights established by the cited Convention.
2) That Costa Rica declares that it recognizes, without conditions and while the American Convention on Human Rights remains in effect, the mandatory jurisdiction of the Court, as a matter of law and without a specific convention on the Inter-American Court on Human Rights, on all cases relating to the interpretation or application of such multilateral treaty.

Mexico:

DECLARATION FOR RECOGNITION OF THE JURISDICTION OF THE
INTER-AMERICAN COURT OF HUMAN RIGHTS

1. The United States of Mexico recognizes as binding ipso facto the adjudicatory jurisdiction of the Inter-American Court of Human Rights on matters relating to the interpretation or application of the American Convention on Human Rights, in accordance with article 62.1 of the same, with the exception of cases derived from application of article 33 of the Political Constitution of the United States of Mexico.
2. Acceptance of the adjudicatory jurisdiction of the Inter-American Court of Human Rights shall only be applicable to facts or juridical acts subsequent to the date of deposit of this declaration, and shall not therefore apply retroactively.

3. Acceptance of the adjudicatory jurisdiction of the Inter-American Court of Human Rights is of a general nature and shall continue in force for one year after the date on which the United States of Mexico gives notice that it has denounced it.
(Declarations and reservation made at the time of ratification)

The instrument of accession was received at the General Secretariat of the OAS on March 24, 1981, with two interpretative declarations and one reservation. Notification of the reservation submitted was given in conformity with the provisions of the Vienna Convention on the Law of Treaties, signed on May 23, 1969. The twelve-month period from the notification of aid reservation expired on April 2,

1982, without any objection being raised to the reservation.
The texts of the interpretative declarations and the reservation are the following:
Interpretative Declarations:

With respect to Article 4, paragraph 1, the Government of Mexico considers that the expression "in general" does not constitute an obligation to adopt or keep in force legislation to protect life "from the moment of conception", since this matter falls within the domain reserved to the States.
Furthermore, the Government of Mexico believes that the limitation established by the Mexican Constitution to the effect that all public acts of religious worship must be performed inside places of public worship, conforms to the limitations set forth in Article 12, paragraph 3.Reservation:

The Government of Mexico makes express reservation to Article 23, paragraph 2, since the Mexican Constitution provides, in Article 130, that ministers of denominations shall not have an active or passive vote, nor the right to associate for political purposes.

On April 9, 2002, the Government of Mexico notified the General Secretariat of its intention to partially withdraw its interpretative declarations and reservation, which now read as follows:
Interpretative declaration
With respect to Article 4, paragraph 1, the Government of Mexico considers that the expression "in general" used in that paragraph does not constitute an obligation to adopt, or keep in force, legislation to protect life "from the moment of conception," since this matter falls within the domain reserved to the States.
Reservation
The Government of Mexico makes express reservation to Article 23, paragraph 2, since the Mexican Constitution provides, in Article 130, that ministers of denominations shall not have a passive vote, nor the right to associate for political purposes.

Peru:

Recognition of Competence:

Presented on January 21, 1981, at the General Secretariat of the OAS an instrument recognizing the competence of the Inter- American Commission on Human Rights and the jurisdiction of the Inter-American Court of Human Rights, in accordance with Articles 45 and 62 of the Convention.
Withdrawl of Declaration/Reservation: 07/09/99
Withdrawl of Denunciation: 01/31/01

Paraguay:

Recognition of competence

The aforementioned instrument of the Government of Paraguay states:
I. That, by virtue of the enactment of Decree No. 16,078 of January 8, 1993, which recognizes the competence of the Inter- American Court of Human Rights for the interpretation and application of the American Convention on Human Rights or Pact of San Jose, Costa Rica.
II. This recognition is for an indefinite period, and should be interpreted in keeping with the guiding principles of international law, in the sense that this recognition pertains expressly to events occurring after this declaration and only on the condition of reciprocity.

[i] PROYECTO DE LEY DE REFORMA PUNTUAL DEL CÓDIGO PROCESAL PENAL DE LA NACIÓN. MODIFICACIÓN DEL TITULO III MEDIOS DE PRUEBA.

(PE- /10)

1.1.1
1.1.2 BUENOS AIRES, de octubre de 2010

AL HONORABLE CONGRESO DE LA NACIÓN:

Tengo el agrado de dirigirme a Vuestra Honorabilidad con el objeto de someter a su consideración un proyecto de ley de reforma puntual del Código Procesal Penal de la Nación.

El presente proyecto de ley está enmarcado dentro de una serie de iniciativas que este se están llevando adelante, desde hace tiempo, de conformidad con las más avanzadas propuestas que en materia de cibercriminalidad y obtención de pruebas digitales se han venido desarrollando en el ámbito internacional.

En ese sentido no está de más recordar que el 23 de noviembre de 2001, en la ciudad de Budapest, Hungría, los Estados miembros del Consejo de Europa y otros Estados firmantes elaboraron y suscribieron el Convenio sobre cibercriminalidad ("Convención de Budapest") en el que se abordó la temática vinculada con los delitos cometidos a través del uso de nuevas tecnologías de la información y las comunicaciones y que consta de diversas secciones que abarcan cuestiones referidas al derecho penal sustantivo, al derecho procesal penal y a la cooperación internacional.

Fue a raíz de ello que, durante el primer semestre de 2008, personal del MINISTERIO DE RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO, del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS, de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN dependiente de la SUBSECRETARÍA DE TENCOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, del MINISTERIO PÚBLICO FISCAL DE LA NACIÓN, representantes del sector académico, del privado y expertos en general, realizaron una labor de revisión del articulado de la Convención de Budapest y determinaron su grado de receptividad en las normas vigentes en nuestro país e identificaron posibles puntos de conflicto.

El 4 de junio de 2008 se sancionó la Ley Nº 26.388 por la cual se modificó el Código Penal Argentino al que se le incorporaron un conjunto de delitos vinculados con la criminalidad informática.

Con posterioridad, en el marco de la Conferencia sobre Cooperación contra el Cibercrimen (*Octopus Interface Conference: Cooperation against Cybercrime)*, organizada por el Consejo de Europa y desarrollada entre los días 23 y 25 de marzo de 2010 en Estrasburgo, Francia, la delegación argentina hizo entrega a las autoridades del mencionado organismo regional de la solicitud del JEFE DE GABINETE DE MINISTROS para que el país fuese invitado a acceder a la Convención de Budapest. A tal fin, la reforma introducida por la Ley Nº 26.388 al Código Penal, antes referida, fue presentada como el cumplimiento suficiente del requisito de adecuación de la ley de fondo a los parámetros de la Convención de Budapest.

Luego, de manera conjunta, el JEFE DE GABINETE DE MINISTROS y el MINISTRO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS, como continuación de la labor oportunamente iniciada desde la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN crearon una Comisión Técnica Asesora en Materia de Cibercrimen, bajo la coordinación de ésta última y la SUBSECRETARÍA DE POLÍTICA CRIMINAL, con el fin de desarrollar y formular una propuesta en relación con aquellas cuestiones procesales requeridas para hacer efectiva la lucha contra esa tipología de delitos y el tratamiento de las pruebas digitales respecto de esos y cualquier otro delito.

Así las cosas, el 20 de septiembre de 2010, el Consejo de Europa, luego de un proceso de consulta de estilo, remitió la invitación para que la Argentina accediese a la Convención de Budapest.

Es por lo hasta aquí expuesto que se propicia el presente proyecto de ley. Como antes se refirió, el capítulo procesal es una parte importante del Convenio de Budapest -cfr. sección segunda del capítulo 2- con una funcionalidad clara: sus previsiones no se limitan solo al ciberdelito, sino que se permiten la investigación de cualquier otro delito -cfr. artículo 14.2-.

En ese sentido esta reforma resulta por demás oportuna puesto que si bien en nuestro ámbito rige el principio de libertad probatoria, la aplicación analógica de algunas de las reglas contenidas en los capítulos II y III del Código Procesal Penal de la Nación ha derivado en soluciones contrapuestas para casos idénticos.

En primer lugar, en el proyecto se plantea el agregado de una prohibición de idénticas características a la contenida en el artículo 185 del Código Procesal Penal de la Nación con el objeto de no alterar su sistematicidad.

Luego, ya específicamente en lo que respecta a las previsiones de la Convención de Budapest y a su receptación, se plantea la modificación del artículo 224 del código de rito por vía del agregado de dos párrafos finales vinculados con el hallazgo de dispositivos de almacenamiento informático, la obtención de una copia forense de los mismos o, en su caso, el secuestro de dichos dispositivos -cfr. artículo 19 de la Convención de Budapest-.

En el mismo sentido, se prevé el agregado de un artículo -224 bis-que, específicamente vinculado con los dispositivos de almacenamiento informático, prevé la posibilidad de ordenar el registro remoto de aquéllos.

En lo que respecta a la requisa personal regulada en el artículo 230 del Código Procesal Penal de la Nación, se prevé la incorporación de un segundo párrafo vinculado con el hallazgo de un dispositivo de almacenamiento informático y la remisión, para la actuación, a las reglas del articulo 224 ya referidas.

Asimismo, y con el fin ya mencionado de conservar la sistematicidad del Código Procesal Penal de la Nación se prevé el agregado de un último párrafo al artículo 231 para el supuesto que lo secuestrado sea un dispositivo de almacenamiento informático, caso en el que, nuevamente, deberá estarse a las reglas contenidas en el artículo 224 cuya reforma también se postula.

Con el fin de adecuar acabadamente nuestro código de rito a las previsiones del instrumento internacional europeo de referencia, se ha proyectado la previsión de la orden de presentación de datos contenidos en un dispositivo de almacenamiento informático y de datos relativos a los usuarios de servicios a distancia por vía electrónica -artículo 232 bis, cfr. artículo 18 de la Convención de Budapest- y de la orden de conservación y protección de datos contenidos en un dispositivo de almacenamiento informático -artículo 232 ter, cfr. artículos 16 y 17 de la Convención de Budapest-.

Finalmente, se proyecta el agregado de un artículo vinculado con la obtención en tiempo real del contenido de las comunicaciones transmitidas por un sistema informático y de los datos de tráfico correspondientes a esas comunicaciones -artículo 236 bis, cfr. artículos 20 y 21 de la Convención de Budapest-.

En este punto no está de más referir que si bien, como antes se refirió, la reforma que se propicia está vinculada con la necesidad de llenar, en lo inmediato, un vacío legal en la materia, el contenido de este proyecto guarda concordancia y coherencia con las reglas que previstas en el Proyecto de Código Procesal Penal de la Nación elaborado por la Comisión Asesora para la Reforma de la Legislación Procesal Penal -Decreto PEN 115/2007- en la que estuvieron representados el estamento judicial, el político, el académico y de la que formaron parte los más importantes especialistas en la materia .

Por lo expuesto, teniendo en cuenta los consensos existentes en consultas formuladas a fuerzas de seguridad y proveedores de servicios electrónicos, y otras instituciones y

sectores interesados de la sociedad, la iniciativa propuesta fortalecerá los mecanismos de prueba previstos en nuestro código de forma, de modo de ubicar al mismo en los más modernos estándares internacionales.

Dios guarde a Vuestra Honorabilidad.-

MENSAJE N°
CRISTINA FERNÁNDEZ DE KIRCHNER
Aníbal D. Fernández.- Julio Alak.-
2 PROYECTO DE LEY
El Senado y Cámara de Diputados,...

REFORMA DEL CÓDIGO PROCESAL PENAL DE LA NACIÓN

ARTICULO 1°.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 185 bis:
"Secuestro de dispositivos de almacenamiento informático: Prohibición.
ARTICULO 185 bis.- Los funcionarios de la policía y fuerzas de seguridad no podrán acceder a los dispositivos de almacenamiento informático que secuestren, sino que los remitirán intactos a la autoridad judicial competente; sin embargo, en los casos urgentes, podrán ocurrir a las más inmediata, la que autorizará el acceso si lo creyere oportuno."

ARTICULO 2º.- Modifícase el artículo 224 del CÓDIGO PROCESAL PENAL DE LA NACIÓN que quedará redactado de la siguiente manera:
"ARTICULO 224.- Si hubiere motivo para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito, o que allí puede efectuarse la detención del imputado o de alguna persona evadida o sospechada de criminalidad, el juez ordenará por auto fundado el registro de ese lugar.
El juez podrá proceder personalmente o delegar la diligencia en el fiscal o en los funcionarios de la policía o de las fuerzas de seguridad. En caso de delegación, expedirá una orden de allanamiento escrita, que contendrá: la identificación de causa en la que se libra; la indicación concreta del lugar o lugares que habrán de ser registrados; la finalidad con que se practicará el registro y la autoridad que lo llevará a cabo. El funcionario actuante labrará un acta conforme lo normado por los artículos 138 y 139 de este Código.
En caso de urgencia, cuando medie delegación de la diligencia, la comunicación de la orden a quién se le encomiende el allanamiento podrá realizarse por medios electrónicos. El destinatario de la orden comunicará inmediatamente su recepción al juez emisor y corroborará que los datos de la orden, referidos en el párrafo anterior, sean correctos. Podrá usarse la firma digital. La Corte Suprema de Justicia de la Nación o el órgano en que ésta delegue dicha facultad, reglamentará los recaudos que deban adoptarse para asegurar la seriedad, certidumbre y autenticidad del procedimiento.

Cuando por existir evidente riesgo para la seguridad de los testigos del procedimiento, fuese necesario que la autoridad preventora ingrese al lugar primeramente, se dejará constancia explicativa de ello en el acta, bajo pena de nulidad.
Si en estricto cumplimiento de la orden de allanamiento, se encontrare objetos que evidencien la comisión de un delito distinto al que motivó la orden, se procederá a su secuestro y se le comunicará al juez o fiscal interviniente.
En el caso de que en la diligencia se hallaran dispositivos de almacenamiento informático y hubiere motivos suficientes para presumir que estos pudieren contener datos relativos a la investigación, el Juez ordenará que se obtenga una copia forense de tal dispositivo. Para el caso en que fuera imposible, ordenará el secuestro del dispositivo o, en su caso, que se conserven los datos en él contenidos de conformidad con las disposiciones contenidas en el artículo 232 ter, tercer párrafo. El registro de él o los dispositivos hallados no podrá extenderse más allá del objeto de la orden respectiva, bajo pena de nulidad."

ARTICULO 3º.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 224 bis:
"Registro de dispositivos de almacenamiento informático.
ARTICULO 224 bis.- Si existieren motivos para presumir que un dispositivo de almacenamiento informático contiene datos relativos a la investigación y fuera posible el registro de tal dispositivo por medios técnicos y en forma remota, así se ordenará con los mismos recaudos del artículo anterior. En tal caso, su objeto deberá estar precisamente detallado, bajo pena de nulidad."

ARTICULO 4º.- Modifícase el artículo 230 del CÓDIGO PROCESAL PENAL DE LA NACIÓN que quedará redactado de la siguiente manera:
"ARTICULO 230.- El juez ordenará la requisa de una persona, mediante decreto fundado, siempre que haya motivos suficientes para presumir que oculta en su cuerpo cosas relacionadas con un delito. Antes de proceder a la medida podrá invitársela a exhibir el objeto de que se trate.
Si el objeto se tratase de un dispositivo de almacenamiento de datos informáticos, el decreto deberá asimismo individualizarlo y proceder de conformidad con lo establecido en el artículo 224.
Las requisas se practicarán separadamente, respetando el pudor de las personas. Si se hicieren sobre una mujer serán efectuadas por otra.
La operación se hará constar en acta que firmará el requisado; si no la suscribiere, se indicará la causa.
La negativa de la persona que haya de ser objeto de la requisa no obstará a ésta, salvo que mediaren causas justificadas."

ARTICULO 5º.- Modifícase el artículo 231 del CÓDIGO PROCESAL PENAL DE LA NACIÓN que quedará redactado de la siguiente manera:
"ARTICULO 231.- El juez podrá disponer el secuestro de las cosas relacionadas con el delito, las sujetas a decomiso o aquellas que puedan servir como medios de prueba.
Sin embargo, esta medida será dispuesta y cumplida por los funcionarios de la policía o de las fuerzas de seguridad, cuando el hallazgo de esas cosas fuera resultado de un allanamiento o de una requisa personal o inspección en los términos del artículo 230 bis, dejando constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o al fiscal intervinientes.
Cuando lo que se secuestre sea un dispositivo de almacenamiento informático la diligencia se realizará de la forma prevista en el artículo 224, último párrafo."

ARTICULO 6º.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 232 bis:
"Orden de presentación de datos contenidos en un dispositivo de almacenamiento informático y de datos de usuarios y/o abonados".
ARTICULO 232 bis.- El juez, o el fiscal cuando se encuentre a cargo de la investigación, podrá ordenar por auto fundado, a cualquier persona física o jurídica la presentación de datos contenidos en un dispositivo de almacenamiento informático que este bajo su poder o control y al que pueda acceder.
Asimismo, podrá ordenar a toda persona física o jurídica que preste un servicio a distancia por vía electrónica la entrega de la información que esté bajo su poder o control referida a los usuarios y/o abonados o los datos con los que cuente de los usuarios y/o abonados a dicho servicio."

ARTICULO 7º.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 232 ter:
"Orden de conservación de datos contenidos en un dispositivo de almacenamiento informático.
ARTICULO 232 ter.- El juez, o el fiscal cuando se encuentre a cargo de la investigación, podrá ordenar, por auto fundado, a cualquier persona física o jurídica la conservación y protección de datos contenidos en un dispositivo de almacenamiento informático cuando existan razones para suponer que esos datos puedan ser modificados o eliminados.
La orden deberá contener con el mayor detalle posible los datos contenidos en un dispositivo de almacenamiento informático a preservar y el tiempo de conservación de los mismos, que podrá alcanzar el término máximo de noventa días, prorrogable por otro idéntico, siempre que se mantengan los motivos que dieron origen como fundamento a la orden.
Durante el cumplimiento de la orden, su destinatario deberá adoptar todas las medidas técnicas y organizativas de seguridad necesarias para que aquélla se mantenga en secreto."

ARTICULO 8º.- Incorpórase el siguiente artículo con su epígrafe al CÓDIGO PROCESAL PENAL DE LA NACIÓN, que se individualizará como artículo 236 bis:
"Intercepción de datos informáticos.
ARTICULO 236 bis. El juez podrá ordenar, por auto fundado, la obtención, aún en tiempo real, del contenido de las comunicaciones transmitidas por un sistema informático, para impedirlas o conocerlas.
Bajo las mismas condiciones, el juez podrá ordenar también la obtención, aún en tiempo real, de los datos de tráfico correspondientes a esas comunicaciones."

ARTICULO 9º.- Las provincias procederán, dentro del plazo de un año a partir de la vigencia de esta ley, a revisar las legislaciones procesales respectivas a efectos de concordarlas con las disposiciones contenidas en la presente.

ARTICULO 10º.- Comuníquese al PODER EJECUTIVO NACIONAL.

CRISTINA FERNÁNDEZ DE KIRCHNER
Aníbal D. Fernández.- Julio Alak.-