Project on Cybercrime
www.coe.int/cybercrime

Strasbourg, 28 October 2010
Provisional/Restricted

Substantive 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

Pedro Verdelho (Portugal)

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

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
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 Scope of this report

1.

On 26 and 27 of August 2010 a workshop was held in Mexico City, under the general topic of "*Meeting the challenge of cybercrime in Latin America*". This regional workshop, co organized by Mexican authorities (the Council of National Security of Mexico) and the Council of Europe, supported by Microsoft, was attended by participants from Argentina, Colombia, Costa Rica, Dominican Republic, Mexico, Paraguay and Peru. All these countries have decided to seek accession to the Budapest Convention and/or are in the process of reforming their respective legislation, regarding cybercrime. The purpose of the workshop was the gathering of decision-makers and subject-matter experts involved in this process in each country, with the objective of analysing existing or draft legislation in view of complying with the Budapest Convention. The final aim of the workshop was to reinforce the process of reform towards the strengthening of legislation and international cooperation against cybercrime.

During the workshop points of view and experiences were exchanged and it was possible to collect information regarding the status of all national legislation and its compliance with the Budapest Convention. The legislative country profiles were updated with information provided by participants.

The scope of this report is to analyse briefly the information collected.

2.

The report will focus only on the substantive criminal provisions of the Convention. It will cover Article 1, regarding definitions, and Articles 2 to 9, referring to substantive criminal law (including provisions on offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences and content-related offences).

It was not considered Article 10 (offences related to infringements of copyright and related rights), because this provision does not create a specific substantive rule regarding cybercrime. In fact, Article 10 generally just states that each signatory Party of the Convention must "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party (…) where such acts are committed wilfully, on a commercial scale and by means of a computer system" – Article 10, 1. In other words, each Party must consider as an infringement to intellectual property law all *online* acts that would be qualified as infringement if they were committed offline.

On the other hand it was not also considered the content of Title 5 (*ancillary liability and sanctions*), including Article 11 (*attempt and aiding or abetting*), Article 12 (*corporate liability*) and Article 13 (*sanctions and measures*). In fact, all the provisions described under Title 5 of Chapter II, Section 1 of the Convention are generic and can be considered respecting all the branches of criminal law. They don't respect specifically cybercrime and its discussion is much broader.

Besides, all the countries referred in this report belong to the roman continental legal family; so, most of these concepts are already converted by national criminal codes.

2 ARGENTINA

4.

Recently, Argentina adopted a binding legal text introducing at the domestic level criminal infringements, in compliance with the Convention on Cybercrime – Law nr 26.388, enacted on 24 of June of 2008 *(B.O. 25/6/200*8). The legislative political option was to amend the existing Penal Code, adding to some of the existing types of crimes some details, to cover also the "cyber side". The general idea of this legal text was to adequate domestic law to the new criminalities, making adjustments and even small changes to classical crimes.

This option – leaving aside the possibility of introducing a separate bill -, was aimed by the simplicity and accessibility of the legal framework: new crimes in a new and autonomous legal text could confuse lawyers and law enforcement agents. On the other hand, it was argued that on the teleological point of view, most of the "cyber infringements" are very close to the classical crimes. The federal nature of Argentinean Republic was also a reason to concentrate in one only legal text all the criminal infringements.

5.

As a general remark, it can be said that the Penal Code from Argentina fully respects the provisions from Budapest Convention. In general terms, all the types of crimes described under the Convention are also qualified as criminal infringements under the Penal Code. It is qualified as crime, illegal access and illegal interception, as it is also described as a crime data and system interference. Besides, Penal Code describes as crimes forgery and fraud, both of them covering all acts respecting computer environment. Respecting child pornography, most of the provisions of the Convention are covered by Argentinean law – as a political option, it was not considered, under the Penal Code, some acts respecting mere possession of child pornography. There was a similar approach respecting provisions of Article 6 of the Convention – Misuse of devices. Penal Code covers most of the aspects of this type of infringement, but does not cover some statements concerning the mere detention of devices and the detention of devices with the intent of use for some specific purposes. These were political options, based on the regular positions of the Constitutional Court of Argentina on this subjects and also based on the fact that incriminating mere possession referring to the specific of the criminal is a concept against national legal tradition.

Last, but not least, it must be referred that Argentinean Law does not include a generic list of definitions, as it results from Article 1 of the Convention.

6.
TABLE 1 - ARGENTINA

Convention of Budapest	**National Law**	**Comments**
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 77** Para la inteligencia del texto de este código, se tendrá presente las siguientes reglas: (…) El término "documento" comprende toda representación de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.	National law does not include a comprehensive list of definitions regarding cybercrime. In fact, referring to these matters, Article 77 of the Penal Code just describes the definitions of "document", "sign" and "subscription". These definitions were included after the revision of Article 77 of the Penal Code by Law number 26.388, enacted on 24 June 24 of 2008. Briefly, according to the law, "document" includes any representations of acts or facts, independently of the medium used to keep, storage, record or transmission. This definition is quite relevant regarding Article 7 of the Convention. All other definitions of the Convention are not covered by national law.

communication's origin, destination, route, time, date, size, duration, or type of underlying service.		
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 153 BIS** Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.	As it was already referred, Law nr 26.388 amended Penal Code. It was, among other, introduced Article 153 bis, describing illegal access. By Article 153 bis it will be punished "whoever intentionally accesses through any means without due authorization or exceeding the authorization, a computer system or computer data with restricted access". It will more severely punished the action if the "access causes damage to a computer system or computer data from a government agency or a public service provider or financial services providers". Law 26.388 also introduced a new Article 157 bis to the Penal Code, that states, among other provisions, that it will be punished whoever "intentionally, illegally or violating confidentiality systems, accesses through any means to a personal data base". These provisions fully comply with Article 2 of the Budapest Convention.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 153** Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o <u>accediere indebidamente</u> a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; <u>o se apoderare</u> indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; <u>o</u>	Article 153 of the Penal Code punishes a wide range of interception of communications. Specifically regarding transmission of computer data, Article 153, paragraph 2 covers the act of whoever "unduly intercepts or captures electronics communications or telecommunications sending by any private system or with restricted access". This provision was introduced by Law 26.388 and follows Article 3 of Budapest Convention.

such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.	
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 183** Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. **ARTICULO 184** La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las	Articles 183 and 184 of the Penal Code describe the classical profile of the crime of damage. They were amended by Law nr 26.388, to cover computer damage. According to Article 183, 2nd paragraph, introduced by Law nr 26.388, it will be punished "whoever destroys or damages computer data, documents or computer systems; or sells, distributes, make available or introduces in a computer system any software with the scope to cause damages". Article 184 states that the penalty will be more severe if the criminal act focuses on computer systems that support health care services, communication services, energy supply, transportation or other public services. These provisions fully comply with Article 4 of the Convention.

	circunstancias siguientes: (…) 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.		Articles 183 and 184 of the Penal Code, amended by Law nr 26.388, describe the classical profile of damage, covering also computer damage. Besides, its broad provision also covers the action of those who "destroy or damage (…) computer systems; or sells, distributes, make available or introduces in a computer system any software with the scope to cause damages" - Article 183, 2nd paragraph, introduced by Law nr 26.388. Article 184 states that the penalty will be more severe if the criminal act focuses on computer systems that support health care services, communication services, energy supply, transportation or other public services. These provisions fully comply with Article 5 of the Convention.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of		Articles 183 and 184 of the Penal Code, amended by Law nr 26.388, describe the classical profile of damage, covering also computer damage. Besides, they cover also system interference. On the other hand, it is described as criminal offence the action of those who "sell, distribute, make available or introduce in a computer system any software with the scope to cause damages" - Article 183, 2nd paragraph, introduced by Law nr 26.388. Article 184 states a more severe penalty for criminal acts focusing on computer systems that support health care services, communication services, energy supply, transportation or other public services.

committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation		Articles 183 and 184 cover partly the provisions of Article 6 of the Convention. Remain uncovered provisions of Article 6 that refer to mere detention of devices and to detention of devices with the intent of use for some specific purposes. Regarding the first case, the Constitutional Court of Argentina has already decided, in other kind of subjects, that this type of provision are unconstitutional, and it was a political option no to include them in the revision of the Penal Code. Referring to the intention of use, also as a political option, as this is a concept against national legal tradition, it was not considered in the legislation.

does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 77** Para la inteligencia del texto de este código, se tendrá presente las siguientes reglas: (…) El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. **ARTICULO 292** El que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio, será reprimido con reclusión o prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado.	National law does not include a comprehensive list of definitions regarding cybercrime. In fact, referring to these matters, Article 77 of the Penal Code just describes the definitions of "document", "sign" and "subscription". These definitions were included after the revision of Article 77 of the Penal Code by Law number 26.388, enacted on 24 June 24 of 2008. Briefly, according to the law, "document" includes any representations of acts or facts, independently of the medium used to keep, storage, record or transmission. In other words, a computer document must be enfaced as a *real life, offline* document (in paper or other). This definition is quite relevant regarding Article 7 of the Convention, because national law does not define, specifically, computer forgery. As it happens with all other cases, computer forgery is punished as a particular modality of common forgery – it is considered as a crime the action of those who produce, totally or partly, a fake document, or produce changes in an authentic document, in such way that can cause damages. The approach from the Argentinean Penal Code and the approach from the Convention are different by nature: Article 7 of the Budapest Convention always refer to data – computer data -, and Article 292 of the Penal Code (as well as Article 293 and 298, describing different modalities of forgery) always refer to document. Nevertheless, there is a common standard in the reality that both of them refer to: a document, according to the Penal Code (Article 77) is "any representation of acts or facts, independently of the medium used to keep, storage, record or transmission". On the other hand, to the Convention

		(Article 1, b), "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". If it is taken into account just computer reality, these two concepts are coincident: a computer document, according to national law is exactly the same as computer data according to the Convention. So, even if they are drafted in a very different base, the two articles are very substantially coincident. For that reason, Article 7 is mostly covered by Penal Code.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 173** Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: (…) 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.	As it happens with computer damage or computer related forgery, among other, computer related fraud is not an autonomous infringement, being a special modality of fraud. Article 173 of the Penal Code, which punishes traditional fraud, was amended by Law 26.388. By this amendment, it was introduced nr 16, that states that it is also considered a fraud the acts of those who defraud by means of any computer manipulation technique, able to change the normal functioning of a computer system or a transmission of data. Article 173, 16 has a very broad approach, which completely complies with Article 8 of the Convention.
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic	**CODIGO PENAL DE LA NACION ARGENTINA (LEY 11.179, actualizada)** **ARTICULO 128** Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare,	Article 128 of the Penal Code punishes whoever produces, finances, offers, sells, publishes, makes available, or distributes by any means, all the representation of a minor of less than eighteen years old, engaged in explicit sexual activities, or all representation of his or hers sexual organs with predominant sexual aim.

law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.	divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.	On the other hand, Article 128 punishes whoever possesses that kind of material with unequivocal aim of distribution or commercialising. These provisions of the Penal Code fully cover Article 9, 1, a, b and c of the Convention. Respecting child pornography, referring to the Convention, Article 9, 1, d is not converted and Article 9, 1, e is just partly covered: the mere possession of child pornography is not punished under the Penal Code, which just punishes the possession with unequivocal aim of distribution or commercialising.

4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.		

3 - CHILE

7.

Within the legislation of Chile, respecting to cybercrime, there are two important legal acts: on one hand, the Penal Code and on the other, a specific law on computer crime (*Ley* 19223, from 7 of June of 1993).

Penal Code is a legal instrument with origin in 1874, but which last version was updated in March 2010. Child pornography is described under the Penal Code, on Articles 366 bis and 374 quinquies. Generically, Article 366 quinquies describes the production of pornographic material with minors and Article 374 bis incriminates the commercial exploitation of that materials. Article 366 bis also defines "pornographic material", stating that it is all kind of representation of a minor engaged in explicit sexual activity, real or simulated, or any representation of their genitals for sexual purposes.

These provisions were introduced in the Code by *Ley* 19927, from 14 of January of 2004. This specific law amended Penal Code and introduced criminal infringements on child pornography.

Ley 19223, from 7 of June off 1993 describes, as crime, some infringements, related to computers. It is a very short legal act, in just 4 articles, describing criminal infringements related to illegal access, illegal interception, data interference and system interference.

8.

As a general remark, it can be said that even if Chile already has, since long time ago, specific regulation on cybercrime, that regulation does not cover all the provisions of Budapest Convention.

Regarding child pornography, as it was said, it is punished under the Penal Code, on Articles 366 quinquies (production of pornographic material) and Article 374 bis (to sell, to import, to export, to distribute, to disseminate or to exhibits pornographic material and also to acquire or to store this kind of material, if done "maliciously"). These provisions cover substantially most of the content of Article 9 of Budapest Convention. They do not cover small details: on one hand, procuring child pornography and on the other the mere possession of child pornography.

Referring to Law 19223, the conclusion is not the same.

Some of the crimes described under Budapest Convention are not included on this national law. It is, above all, the case of Article 6, Article 7 and Article 8 of the Convention. Besides, national law does not include a list of definitions, as required on Article 1 of the Convention.

On other cases, Law 19223 describes crimes also described under the Convention, but national provisions don't comply with the Convention. Last, but not least, some of the provisions of the Convention are fully covered by national law.

Referring to Article 3 of Budapest Convention (illegal interception), it is punished under Article 2 of Law 19223, but this provision is much more narrow than the Convention. It can be found the same conclusion respecting data interference (Article 4 of Budapest Convention): it is punished under Article 3 of Law 19223, but this provision does not include many of the criminal acts described in the Convention.

However, in some situations, the articles of the Convention are fully covered by the provisions of Law 19223. It is the case of Article 2 of Budapest Convention, covered by Article 2 of Law 19223, even if the text of the law could be clearer. But it is also the case of system interference (Article 5 of the Convention), covered by Article 1 of Law 19223, even if this provision has a different approach from Article 5 of the Convention.

9.
TABLE 2 – CHILE

Convention of Budapest	National Law	Comments
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a		National law does not include a comprehensive list of definitions regarding cybercrime.

communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Ley 19223** **Artículo 2°** El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.	Article 2 of Law 19223 punishes those who, with appropriative intent, among other situations, use or have unduly knowledge of information stored within a computer system, intercepts it, or interferes or accesses to it. This provision intends to cover, besides other, illegal access. However, its wording could be clearer: illegal access will be punished just if the agent acts with appropriative intent. Beyond that, this provision covers Article 2 of Budapest Convention.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to,	**Ley 19223** **Artículo 2°** El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.	Article 2 of Law 19223 punishes, besides other, whoever intercepts, or interferes information stored within a computer system. The text of the article requires that the agent acts with appropriative intent, what makes narrow the scope of the provision. This provision intends to cover, besides other, illegal interception, but from the text it can be clearly concluded that it does not cover all the criminal acts described under Article 3 of Budapest Convention.

from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.		
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Ley 19223** **Artículo 1°** El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo. **Artículo 3°** El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.	According to Article 3 of Law 19223, it will be punished whoever alters damages or destroys data stored within a computer system. It is required intention to act (the actual expression is "maliciously"). On the other hand, Article 1 of Law 19223 states that it will be punished whoever, intentionally, destroys or makes unusable an information system, or its parts, or prevents or changes its functioning. This provision, described under paragraph 1, refers to system interference. But on paragraph 2, it is stated that if this kind of acts have, as consequence, to affect data stored in that system, the punishment will be more severe. These provisions cover partly Article 4 of Budapest Convention, but it remains uncovered part of the expressions included in the wording of that Article (such as deletion, deterioration, alteration or suppression).
Article 5 – System interference Each Party shall adopt such legislative and other measures as	**Ley 19223** **Artículo 1°**	According to Article 1 of Law 19223 it will be punished whoever, intentionally (the actual expression is "maliciously") destroys or makes unusable an information system, or its

may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo. **Artículo 3°** El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio	parts, or prevents or changes its functioning. This provision, described under paragraph 1, refers to system interference. Article 1 of the law has a different approach from Article 5 of the Convention, but it can be said that the scope of both provisions are coincident.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;		Current legislation of Chile does not incriminate the acts described under Article 6 of the Convention.

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the		

right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.		Current legislation of Chile does not incriminate computer forgery, as described under Article 7 of the Convention.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic		Current legislation of Chile does not incriminate specifically computer-related fraud.

law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.		
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for	**CODIGO PENAL** **Artículo 366 quinquies** El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo. Para los efectos de este artículo y del artículo 374 bis, se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de estos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente seuales. **Artículo 374 bis** El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico,	Child pornography, as a criminal infringement, is punished under the Penal Code. On one hand, on Article 366 quinquies, it is described, as a crime, the production of pornographic material with minors less than 18 years. This Article also defines pornographic material as all kind of representation of a minor engaged in explicit sexual activity, real or simulated, or any representation of their genitals for sexual purposes. On the other hand, Article 374 bis incriminates whoever sells, imports, exports, distributes, disseminates or exhibits pornographic material with minors under 18 years old. It is also incriminated, under this Article, whoever "maliciously" acquires or stores this kind of pornographic material. Most of the content described under Article 9 of Budapest Convention is already covered by these provisions. Just remain uncovered nr 1, d and e (procuring child pornography and the mere possession of child pornography).

oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado medio a máximo. El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio.	

4 COLOMBIA

10.
Since the year 2000, Colombia adopted some legal documents, aiming to create an effective legislative framework regarding reaction against cybercrime. During 2000 it was published the new Penal Code (Law nr 599). Since then, with particular effects respecting cybercrime topics, this fundamental legal instrument was amended by Law nr 1273 and by Law 1276, both of them from 2009. Still in 2009 it was published Law 1336 (from 21 July 2009), that brought new changes to Law 1276 and to the Penal Code.
These bills created at the domestic level, from one side, infringements referring to child pornography, and from the other side, several types of crimes around the so called "new legal interest of the protection of information and of the data, and of the integral preservation of communication and information systems".
All the infringements where introduced directly in the Penal Code, even if they are specifically called "cybercrimes" and are included within Title VII BIS – "From the protection of the information and the data". They have a teleological autonomous treatment.

11.
As a general comment, it can be said that generically, the penal substantive provisions of the Convention on Cybercrime are covered by Colombian national law. In fact, just remain uncovered some second line details.
It is the case of definitions (Article 1) of the Convention: Colombian national law does not provide a systematic list of definitions regarding cybercrime.
On the other hand, regarding Article 6 of the Convention, some details, above all referring to the mere possession of devices, are not incriminated by Colombian Penal Code.
Besides, there is not any specific provision referring to Computer-related forgery (Article 7 of the Convention). In fact, this Article intends to punish the same facts already covered by other articles, but when the author has a specific intention: that the fake computer data are "considered or acted upon for legal purposes as if they were authentic". There is not an economic perspective within this infringement. Most of the material acts incriminated under this article are already incriminated in the Penal Code. But national law does not consider it a crime if there are not economic consequences: damage, loss, or illegal profit.

12.
TABLE 3 - COLOMBIA

Convention of Budapest	National Law	Comments
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant		Colombian national law does not provide a systematic list of definitions regarding cybercrime. Within Colombian Law 597, there are definitions, but just respecting electronic commerce (which is its scope). Besides this, there are no more definitions respecting

to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		cybercrime within national law.
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of	**Código Penal de Colombia** **Artículo 269 A.** **Acceso abusivo a un sistema informático.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a	Article 269-A from the Penal Code describes the crime of illegal access to a computer system, which is fulfilled by whoever accedes to the whole or a part of a computer system, unauthorised, and also by whoever remains inside that system against the will of who has the right to exclude him or her. Article 269-H describes aggravating circumstances for all the cyber crimes described in the Penal Code. According to it, the sanctions will be more severe if the crimes are committed against computer or communication systems

obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. **Artículo 269 H.** **Circunstancias de agravación punitiva.** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada por el poseedor de la in-formación o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para si o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	from the State or the finance sector, by a civil servant, taking advantage of the trust given by the holder of the information, disclosing the content of information, damaging a third party, or to obtain a profit with the action or with terrorist aim or generating a risk to public security or national defence. The provision of Article 269-A fully complies with Article 2 of Budapest Convention.
Article 3 – Illegal interception Each Party shall adopt such legislative and	**Código Penal de Colombia** **Artículo 269 C.**	Article 269-C incriminates the interception of computer data, which is described as the action of whoever, without a

other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Interceptación de datos informáticos.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los tras-porte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. **Artículo 269 H.** **Circunstancias de agravación punitiva.** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada por el poseedor de la in-formación o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para si o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de	previous judicial order, intercepts computer data, in its origin or in the recipient, or inside a computer system, or the electromagnetic emissions originated by a computer system that carries those data. Article 269-H describes common aggravating circumstances for all the cyber crimes described in the Penal Code. According to it, the sanctions will be more severe if the crimes are committed against computer or communication systems from the State or the finance sector, by a civil servant, taking advantage of the trust given by the holder of the information, disclosing the content of information, damaging a third party, or to obtain a profit with the action or with terrorist aim or generating a risk to public security or national defence. The provision of 269-C covers Article 3 of the Convention.

	inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Código Penal de Colombia** **Artículo 269 D.** **Daño informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. **Artículo 269 H.** **Circunstancias de agravación punitiva.** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada por el poseedor de la in-formación o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para si o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.	Article 269-D of Penal Code (computer damage), states that whoever, unauthorised, destroys, damages, deletes, causes deterioration or alteration, or suppresses computer data or an information treatment system or its logic components, will be punished. Article 269-H describes common aggravating circumstances for all the cybercrime described in the Penal Code. According to it, the sanctions will be more severe if the crimes are committed against computer or communication systems from the State or the finance sector, by a civil servant, taking advantage of the trust given by the holder of the information, disclosing the content of information, damaging a third party, or to obtain a profit with the action or with terrorist aim or generating a risk to public security or national defence. This provision is completely in line with Article 4 of Budapest Convention.

	7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Código Penal de Colombia** **Artículo 269 B.** **Obstaculización ilegítima de sistema informático o red de telecomunicación.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. **Artículo 269 H.** **Circunstancias de agravación punitiva.** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones	Article 269-B of Penal Code (illegal objection to a computer system or telecommunication network), states that it will be punished whoever, unauthorised, prevents or hinders the functioning or the normal access to a computer system, computer data stored in there or a telecommunications network. Article 269-H describes common aggravating circumstances for all the cyber crimes described in the Penal Code. According to it, the sanctions will be more severe if the crimes are committed against computer or communication systems from the State or the finance sector, by a civil servant, taking advantage of the trust given by the holder of the information, disclosing the content of information, damaging a third party, or to obtain a profit with the action or with terrorist aim or generating a risk to public security or national defence. This type of crime, corresponding to system interference, is described by Colombian national law in a very broad way, and it is open regarding the action. However, the text covers completely the provision of Article 5 of Budapest Convention.

	3. Aprovechando la confianza depositada por el poseedor de la in-formación o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para si o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of	**Código Penal de Colombia** **Artículo 269 E** **Uso de software malicioso.** El que, sin estar faculta-do para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. **Artículo 269 F.** **Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga,	The provisions of Article 6 of Budapest Convention find equivalent dispositions in more than one article of the Penal Code of Colombia. 269-E of Penal Code (use of malicious software), states that it will be punished whoever, unauthorised, produces, sells, buys, distributes, sends, imports or exports malicious software or other computer programs able to produce damage. On the other hand, Article 269-F incriminates, generically, obtaining and offering by any means of personal codes or personal data contained in computer files or data bases. Article 269-G punishes the activity of those who create and make available to the public web pages, hyperlinks or pop-ups with illegal purposes. It is also covered by this article the activity of those that change the resolution system of domain names, in such way that a Internet user can accede to a different IP, believing that she or he is acceding to her

being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. **Artículo 269 G** **Suplantación de sitios web para capturar datos personales.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.	or his bank or other personal trusted site. It seems that provisions from Article 269-F and 269-G specifically intend to punish the criminal activities known as *phishing* and *pharming*. Regarding Article 6 of the Convention, remain uncovered by national law, above all, the provisions that refer to the possession of the devices (with an exception to devices produced to transfer of assets, with aim of economic profit, by computer manipulation or similar, with loss or damage to a third party, described under Article 269-J – see comment to Article 8 of the Convention). It must be said also that Article 6 of the Convention opens, clearly, the possibility that all the facts can be produced by means of hardware – and not only by the means of software or computer data. But Colombian law is entirely drafted in the direction of software and data, and there is not any reference to hardware.
Article 7 – Computer-related forgery Each Party shall adopt such legislative and		There is not any specific provision on this matter.

other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.		
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Código Penal de Colombia** **Artículo 269 I.** **Hurto por medios informáticos y semejantes.** El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. **Artículo 269 J.** **Transferencia no consentida de activos.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más	Article 8 of the Convention finds correspondence in two different Articles of the Penal Code: Article 269-I describes theft by computer or similar means and Article 269-J describes unauthorised transfer of assets. The first of them, Article 269-I, incriminates the act of stealing, by means of manipulation of a computer system, or an electronic network system, or similar, surpassing computer security measures. Article 269-J qualifies as a crime the act of unauthorised transfer of any assets, with aim of economic profit, by computer manipulation or similar, with economic loss or damage to a third party. It is also incriminated the act of whoever produces, introduces, possesses or makes available software able to practise the previous acts or a common fraud. Both of these articles of Colombian Penal Code have a different approach from Article 8 of the Convention. Maybe, they are inspired in the need to combat certain very expanded modern forms of fraud – mainly *phishing*. However, the major elements of computer fraud can be found there: the economic loss or the intent of profit, from one side, and the broad concept of manipulation of a computer system, that can include all the tipic criminal acts

	grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.	from Article 8 a and b. For these reasons, even with a different approach, Articles 269-I and 269-J cover Article 8 of the Convention.
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include	**Código Penal de Colombia** **Artigo 218** **Pornografía con personas menores de 18 años** El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión 10 a 20 años y multa de 150 a 1500 salarios mínimos legales mensuales vigentes. Igual pena se aplicará a quién alimente con pornografía infantil bases de dados de Internet, con o sin fines de lucro. La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la victima.	According to Article 218 of the Colombian Penal Code (ammended by Law 1336, from 21 of July of 2009) it is a crime to take pictures, make movies, record, produce, make available, offer, sell, buy, possess, store, broadcast or exibit, by any means, for personal use or to share with other, real representations of sexual activity referring to a minor with less than 18 years old. It is also punished whoever feeds, with child pornography, Internet data bases, with or without aim of profit. This provision fully complies with Article 9 of the Convention. The only remark it must be made respects the concept of child pornography. According to the Convention, this concept covers "a person appearing to be a minor engaged in sexually explicit conduct" or "realistic images representing a minor engaged in sexually explicit conduct". The concept in Colombian law refers to "real representations". But, even if the concepts are not coincident, in fact they can be considered compatible.

pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.		

5 COSTA RICA

13.
Since many years ago, Costa Rica has adopted legal texts referring to cybercrime. Penal Code (originally publish in 1970 – Law nr 4573, from 4 of may 1970), was several times amended. Some of those alterations introduced specific rules on cybercrime: Law nr. 7899, of 3 of August from 1999, Law nr. 8143, from 5 of November of 2001 and Law nr 8590, from 18 of July of 2007.As a result, Penal Code includes nowadays many types of crime referring to child pornography (Articles 167, 173, 173bis and 174), and crimes referring to illegal interception, data and system interference and computer fraud (Articles 196bis, 217bis and 229bis).

As a curiosity, Costa Rica has also some special laws, just applicable when some institutions of the State are victim of criminal actions, which describe some of the so called computer crimes, and incriminate the same facts as the Penal Code, if they are committed within the activity of those institutions. It is the case of the Code of Tax Rules and Proceedings ("Código de Normas y Procedimientos Tributarios" - Law nr. 4755, from 3 of May of 1971, amended by Law nr.7900, of 3 of August of 1999), which punishes illegal access and computer damage within computer systems of the Tax Administration.
Also General Law of Customs ("Ley General de Aduanas" – Law nr. 7557, from 20 of October of 1995), which punishes illegal access, data interference and system interference, when committed against the computer systems used by The National Customs Service.
Finally, the Financial Administration and Budget Law ("Ley de Administración Financiera de la República y Presupuestos Públicos" – Law nr. 8131, from 18 of September of 2001) incriminates data interference and system interference when committed against computer systems of the Financial Administration.

14.
At the time of the writing, it was under discussion in the parliament (*Asamblea Legislativa de la República de Costa Rica*[1]) a draft law which scope is to reform the Penal Code, adding to its text a new chapter called "computer crime". That bill, *Proyecto de Lei Ordinario 17613*[2] was presented in December 2009 and there is a great expectation on its approval.

The aim of this law is to update the legal framework, regarding the new realities of cyber criminality and also to comply with Budapest Convention.

15.

In general term, most of the substantive penal provisions of Budapest Convention are already covered by the Penal Code of Costa Rica. But there are still some small gaps.

[1] http://www.asamblea.go.cr
[2] http://www.asamblea.go.cr/Centro_de_Informacion/Consultas_SIL/Pginas/Detalle%20Proyectos%20de%20Ley.aspx?Numero_Proyecto=17613

In fact, in the legislative framework in force, there are no definitions such as the definitions included in Article 1 of the Convention. It seems that the option to include specific definitions in a specific legislative instrument is against national legislative tradition.

On the other hand, within the Penal Code or any other legislation, there are not dispositions complying with Article 6 of the Convention. *Proyecto de Lei Ordinario 17613* will include two new Articles 232 and 233, describing the crime of installation or spread of malicious software and the crime of supplanting electronic pages. These future new provisions will cover part of Article 6 of the Convention, but it will remain uncovered some of the aspects referring the production and diffusion of devices (without concrete installation in a computer system), as it will not be covered the mere possession of devices.
This *Proyecto de Lei Ordinario 17613* will clarify the drafting of the crimes of computer damage (data interference) and computer sabotage (system interference).

It will clarify also illegal access, but without including the mere unauthorized access (which is covered by the law in force). In fact, the weakest point of this draft law is the exclusion of incrimination of the mere access to a computer system, described on the current version of Article 229 bis but not covered by the version of *Proyecto de Lei Ordinario 17613*.
Regarding Article 7 and 8 of the Convention, they are mostly covered by Article 217 bis of the Penal Code, even if there is not a complete coincidence between Article 217 bis of the Penal Code and Articles 7 and 8: national law has a generic formulation and does not mention all the acts described under the Convention, but most of those acts can be considered covered by the generic concepts described under the Penal Code of Costa Rica. Also referring to Article 217 bis, *Proyecto de Lei Ordinario 17613* will clarify the drafting of the article, but without changing the approach

Costa Rica has a much extended incrimination regarding child pornography, which fully complies the provisions of the Convention. Nevertheless, the Penal Code does not have a definition of pornographic material.

16.
TABLE 4 – COSTA RICA

Convention of Budapest	**National Law**	**Comments**
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any		There are not generic definitions referring to cybercrime within the law of Costa Rica. However, it is possible to find a definition of "traffic data" in Executive Decrees like Measures to Protect the Privacy in Telecommunications No.35205, April 16th, 2009, but not exactly in criminal matters. According to Article 5, e, of this legal text, traffic data is any data related to a communication within a telecommunications network.

representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may	**Código Penal** **Artículo 229 bis** **Alteración de datos y sabotaje informático** Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese*,* borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa	Article 229 bis describes the so called crime of alteration of data and computer sabotage. This provision states that it will be punish whoever, unauthorized, by any means, accedes, deletes, suppresses, changes or makes unusable computer data stored in a computer. Therefore, in fact, illegal access, as described under Article 2 of the Convention, is covered by the first paragraph of Article 229 bis of the Penal Code.

require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años. **Código de Normas y Procedimientos Tributarios** **ARTÍCULO 94** **Acceso desautorizado a la información** Será sancionado con prisión de uno a tres años quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente. **Ley General de Aduanas** **Articulo 221** **Delitos informáticos** Será reprimido con prisión de uno a tres años quien: a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas. b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad. c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona. d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La	Identical provisions can be found on the "*Código de Normas y Procedimientos Tributarios*" (Law nr. 4755, from 3 of May of 1971), which Article 94 punishes the access to the information systems or data bases of Tax Administration. Besides, Article 221 of "*Ley General de Aduanas*" (Law nr. 7557, from 20 of October of 1995), describes the so called computer crimes, incriminating, besides other acts, illegal access to the computer systems used by the National Customs Service. *Proyecto de Lei Ordinario 17613* provides a change to Article 229 bis, deleting text referring to illegal access and focusing the scope of this provision on computer damage. On the other hand, illegal access will be more detailed described in Article 231, which provides computer espionage, incriminating obtaining, transmission, copy, change, destruction, use, blocking or recycling of information, by the means of any computer or technologic manipulation. This infringement just refers to information concerning economy commerce. It is extended by Article 288, second paragraph of the *Proyecto* to classified information concerning politics, law enforcement agencies, security, foreign affairs or fight against drug trafficking or organized crime. This draft law excludes the incrimination of the mere access to a computer system, described on the current version of Article 229 bis and not covered by the version of *Proyecto de Lei Ordinario 17613*.

	pena será de seis meses a un año si el empleo se facilita culposamente.	
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Código Penal** **Artículo 196 bis** **Violación de comunicaciones electrónicas** Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.	According to Article 196 bis, it is considered violation of electronic communications the act of whoever obtains, accedes, changes, suppresses, intercepts, interferes, makes available to other or diverts messages, data and pictures stored in electronic means, computers, magnetic or telematic. Article 3 of Budapest Convention describes this crime just as the interception without right, made by technical means, of non-public transmissions of computer data. Thus, even with a different approach, Article 196 bis complies with the Convention. On the other hand, *Proyecto de Lei Ordinario 17613* provides a change to Article 196 of the Penal Code, punishing in a clear manner the violation of electronic communications with a new scope, in a more precise wording.
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in	**Código Penal** **Artículo 229 bis** **Alteración de datos y sabotaje informático** Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se	Under the first paragraph of Article 229 bis of the Penal Code it is described the crime of alteration of data and computer sabotage. This Article states that it will be punished whoever, unauthorized, by any means, accedes, deletes, suppresses, changes or makes unusable computer data stored in a computer. So, data interference, as described under Article 4 of the Convention, is covered by the first paragraph of Article 229 bis of the Penal Code. Identical provisions can be found on the "*Código de Normas y Procedimientos Tributarios*" (Law nr. 4755, from 3 of May of 1971), which Article 95 punishes destruction, making unusable, alteration or transfer of

serious harm.	impondrá pena de prisión hasta de ocho años. **Ley General de Aduanas** **Articulo 221** **Delitos informáticos** Será reprimido con prisión de uno a tres años quien: a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas. b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad. c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona. d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente. **Ley de Administración Financiera de la República y Presupuestos Públicos** **Artículo 111** Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la administración financiera y de proveeduría, alguna de las siguientes acciones: a) Apoderarse, copiar, destruir, alterar, transferir o	any computer program or data base used by Tax Administration. Besides, Article 221 of "*Ley General de Aduanas*" (Law nr. 7557, from 20 of October of 1995), describes the so called computer crimes, incriminating, besides other acts, destruction, making unusable, alteration, making available or transfer of any computer programs or data base used by the National Customs Service. The same Article punishes whoever damages hardware that supports the functioning of the computer systems designed to the operations of National Customs Service, with the scope of numbing or obtaining profit. On the other hand, "*Ley de Administración Financiera de la República y Presupuestos Públicos*" (Law nr. 8131, from 18 of September of 2001), describes under Article 111 a so called computer crime. According to this provision, it will be a crime the unauthorized destruction, alteration or transfer of information, computer programs or data base from the Financial Administration. It is also a crime to cause damage to software and hardware, machines or accessories that support the functioning of the services of Financial Administration. *Proyecto de Lei Ordinario 17613* provides a change to Article 229 bis, deleting text referring to illegal access and focusing the scope of this provision on computer damage. The great advantage of this draft law is to clarify the aim of this crime, including all the kind of acts also described on Article 4 of the Convention. In fact, the option of the draft law is to divide the original article 229 bis and to created two new articles: on one side, Article 229 bis (directed to software and unrecoverable files) and Article 229 ter (directed to hardware).

	mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido. b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos. c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas. d) Utilizar las facilidades del sistema para beneficio propio o de terceros. **Código de Normas y Procedimientos Tributarios** **ARTÍCULO 95** **Manejo indebido de programas de cómputo** Será sancionado con pena de tres a diez años de prisión, quien sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or	**Código Penal** **Artículo 229 bis** **Alteración de datos y sabotaje informático** Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el	Under the first paragraph of Article 229 bis of the Penal Code it is described the crime of alteration of data and computer sabotage. This Article states that it will be punished whoever, unauthorized, by any means, accedes, deletes, suppresses, changes or makes unusable computer data stored in a computer. On the other hand, under paragraph 2, it is stated that it will be also a crime if these acts (described on paragraph 1) have as consequence the numbness or the impossibility of use of a computer program, a data base or a computer system.

suppressing computer data.	programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años. **Ley General de Aduanas** **Ley No. 7557, de 20 de octubre de 1995** **Articulo 221** **Delitos informáticos** Será reprimido con prisión de uno a tres años quien: a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas. b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad. c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona. d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente. **Ley de Administración Financiera de la República y Presupuestos Públicos** **Ley No 8131, de 18 de setiembre de 2001** **Artículo 111** Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares	So, system interference, as described under Article 5 of the Convention, is covered by the first paragraph of Article 229 bis of the Penal Code. Besides, Article 221 of "*Ley General de Aduanas*" (Law nr. 7557, from 20 of October of 1995), describes the so called computer crimes, incriminating, besides other, the acts of whoever damages hardware that supports the functioning of the computer systems designed to the operations of National Customs Service, with the scope of numbing or obtaining profit. On the other side, Article 111 of "*Ley de Administración Financiera de la República y Presupuestos Públicos*" (Law nr. 8131, from 18 of September of 2001, describes a so called computer crime. According to it, it will be a crime to cause damage to software and hardware, machines or accessories that support the functioning of the services of Financial Administration. *Proyecto de Lei Ordinario 17613* provides a change to Article 229 bis, deleting text referring to illegal access and focusing the scope of this provision on computer damage. All the references to system interference of the version in force of Article 299 bis are deleted by that draft law. On the other hand, this bill will add a new crime to Penal Code, on the new Article 229 ter, defining computer sabotage. Under this article it will be punished whoever, with aim of profit, destroys, changes, numbs or makes unusable data stored in a data base, or prevents, changes, hinders or modifies without authorization the functioning of a computer system. This future new organization of the chapter referring to computer crimes within the Penal Code will have the advantage of clarifying the types of crime and its

	que realicen, contra los sistemas informáticos de la administración financiera y de proveeduría, alguna de las siguientes acciones: a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido. b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos. c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas. d) Utilizar las facilidades del sistema para beneficio propio o de terceros.	protect interests.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the		There is not any disposition, within the national legislation, complying with Article 6 of the Convention. However, *Proyecto de Lei Ordinario 17613* provides a new Article 232, describing the crime of installation or spread of malicious software. According to this article, it will be punished whoever, unauthorized, by any means, installs malicious software in a computer system. It will be also punished who induces other by mistake to install malicious software, or who distributes this kind of software. This legal project also includes a new Article 233, providing the crime of supplanting electronic pages, which includes the acts of who, inducing wrongly other to practise an act, obtains confidential information from a person, with aim of profit. These new provisions, from Articles 232 and 233 will complain, even if not completely, with Article 6 of the Convention. In fact, it will not be covered some of the aspects referring the production and diffusion (without

whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items		concrete installation in a computer system), as it will not be covered the mere possession of devices. On the other hand, specifically regarding intellectual property, there are rules which punish the misuse of devices if they can break or "crack" effective technological measures. The fabrication, import, distribution, offer or traffic of devices, products, parts or services that can help to evade effective technological measures designed to protect communication, reproduction, access or publication of intellectual property are punished. In fact, according to Law 8039, of 10 Octtober 2000, referring to proceedings to respect intellectual property rights, on Article 2 bis, defines technological measure as any device that can control the access to any protected work, interpretation or execution covered by intellectual property right. Besides, Article 62 punishes any alteration or suppression, change or deterioration of that device. Finally, on Article 62 bis, it is incriminated to produce, import, distribute, offer or sell such kind of devices.

referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Código Penal** **ARTÍCULO 217 bis** **Fraude informático** Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.	Article 217 bis of the Penal Code of Costa Rica covers Articles 7 and 8 of the Convention. In fact, both of the infringements are partly coincident: Article 7 punishes forgery on computer data with or without aim of profit. Thus, Article 7 regards the data and its integrity. However, it allows a Party of the Convention to require a dishonest intent, in view of criminalization. From the other side, Article 8 generically punishes manipulation of those data envisaging the loss of property of other person. Article 217 bis requires the intent of obtaining economic advantage and it will be committed by whoever interferes in the result of treatment of data in a computer system, by the means of use of forged or incomplete data, unduly use of those data or any other action focusing in the processing of the system data. There is not a complete coincidence between Article 217 bis of the Penal Code and Article 7 of the Convention but, globally, it can be said that most of the content of Article 7 is included in Article 217 bis. *Proyecto de Lei Ordinario 17613* provides a new draft of Article 217 bis, but this new draft maintains this perspective, focusing the aim of profit or the economic loss of other.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the	**Código Penal** **Artículo 217 bis** **Fraude informático** Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de	The Penal Code of Costa Rica covers, by Article 217 bis, the provisions of Article 8 of the Convention. Article 8 punishes manipulation of data envisaging the loss of property of other person. Article 217 bis requires the intent of obtaining economic advantage and it states that it will be committed a crime by whoever interferes in the result of treatment of data in a computer system, by the means of use of forged or

causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.	incomplete data unduly use of those data or any other action focusing in the processing of the system data. Article 217 bis has a more generic formulation than Article 8 referring, for example, to all action that focuses in the processing of data of the system. This formulation does not mention all the acts described under Article 8 of the Convention, but mostly of those acts can be considered covered by the generic concepts described. *Proyecto de Lei Ordinario 17613* provides a new draft of Article 217 bis, but this new draft maintains this perspective, focusing the aim of profit or the economic loss of other.
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in	**Código Penal** **Artículo 173** **Fabricación, producción o reproducción de pornografía** Será sancionado con pena de prisión de tres a ocho años, quien fabrique, produzca o reproduzca material pornográfico, utilizando a personas menores de edad, su imagen y/o su voz. Será sancionado con pena de prisión de uno a cuatro años, quien transporte o ingrese en el país este tipo de material con fines comerciales. **Artículo 173 bis** **Tenencia de material pornográfico** Será sancionado con pena de prisión de seis meses a dos años, quien posea material pornográfico en el que aparezcan personas menores de edad, ya sea utilizando su imagen y/o su voz.” **Artículo 174** **Difusión de pornografía** Quien comercie, difunda o exhiba material pornográfico a	Respecting to child pornography, the Penal Code from Costa Rica has a comprehensive approach, incriminating all kind of acts, committed or not by Internet and computer systems. In other words, national law does not include specific provisions describing child pornography by the means of a computer system: the provisions on child pornography are comprehensive and are applicable to offline or online situations. According to Article 173, it will be punished whoever produces or reproduces pornographic material using minors. Article 173 bis incriminates the mere possession of such kind of material. Finally, Article 174 describes and punishes diffusion of pornography, and also the exhibition, distribution or sale, by any means, of pornographic material with minors or where minors can be seen. It is also punished under this article the possession with those purposes. Costa Rica has a much extended incrimination regarding child pornography, which fully covers the provisions of the Convention. Nevertheless, the Penal Code does not have a

a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	personas menores de edad o incapaces, será sancionado con pena de prisión de uno a cuatro años. La misma pena se impondrá a quien exhiba, difunda, distribuya o comercie, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o donde se utilice su imagen, o lo posea para estos fines.	definition of pornographic material. The only reference regarding this definition is the mention of the expression "image and voice", with regard to the material, on Articles 173 and 173 bis. However, according to national law, it is valid within national legislation the definition stated on Article 2, c) of the Optional Protocol to the Convention on the Rights of the Child, which entered in force on 18 of January of 2002. This rule defines child pornography as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. And it is an integrating part of the law of Costa Rica.

6 MEXICO

17.

The Mexican Republic is a federal state: in the same geographic borders coexist, at different levels, a Federal Penal Code, applicable all over Mexico, and state penal regulations, applicable within each federate state.

Respecting to cybercrime, at the state level, it can be found several scattered regulations, which have already incriminated many situations: illegal access, computer damage, communications interceptions, credit cards cloning, copyright infringement, illegal content on the networks, violation of personal intimacy, infringement of the security of computer systems, denial of service, extortion by the means of electronic instruments or child pornography. All this crimes are strictly just applicable at the local level, in the state that drafted and passed them.

It has not been drafted, until now, any federal specific law on this subject. Also at the federal level, the existing regulations seem that they have responded to specific needs and did not face globally cybercrime phenomena. The existing cyber-related infringements are described under the Federal Penal Code, even if there is information about some crimes described in specific and special laws – for example referring to the stock exchange markets.

Within the Federal Penal Code (a law from 1931, but many times amended – the last amendment was introduced in August 2010), it can be found infringements referring specifically to computer damage and illegal access (Article 211 bis 1, Article 211 bis 2, Article 211 bis 3, Article 211 bis 4 and Article 211 bis 5). Within them, there are special rules applicable to crimes committed against the computer systems from the Mexican State and from institutions from the financial system.

Besides, the Federal Penal Code also describes some crimes not specifically applicable to the cyber environment, but also used by interpreters to cover infringements online. It is the case of illegal interception of communications – all kind of communications (Article 173 and Article 177) and also the case of child pornography (Article 202 and Article 202 bis).

18.

As a global comment, it can be said that Mexico has still a route to do regarding criminalising cybercrime realities.

Regarding the compliance with Budapest Convention, national law does not include, first of all, a list of definitions regarding cybercrime.

Concerning to the crimes, Federal Penal Code incriminates computer damage (data interference, under Article 4 of Budapest Convention), in a very comprehensive way. On the other hand it is also incriminated child pornography (described on Article 9 of the Convention). But in this case, the lack of a substantive definition of child pornography leaves outside the infringement all pornographic situations with a person appearing to be a minor and realistic images representing a minor, both of them engaged in sexually explicit conduct.

On regard of illegal access, Federal Penal Code does not cover in a sufficient manner the criminal acts described on Article 2 of the Convention. At federal level it is just incriminated to know information, or to take note of information stored in a computer system. Especially, Mexican federal law does not cover the mere act of access a computer system.

Finally, concerning illegal interception (Article 3 of the Convention), Federal Penal Code prefers a generic approach, providing a crime of violation of communications, on Article 173, applicable to all kind of communications, that does not specifically refers to computer data, what can cause difficulties in concrete cases of transmissions of computer data.

Respecting all other infringements described in the Convention (Article 5 – system interference, Article 6 – misuse of devices, Article 7 – computer-related forgery and Article 8 – computer-related fraud), they are not considered on Mexican Federal Penal Code.

19.
TABLE 5 – MEXICO

Convention of Budapest	National Law	Comments
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		There are not generic definitions in any legislative instrument, specifically regarding cybercrime.
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally,	**CÓDIGO PENAL FEDERAL** **Artículo 211 bis 1** Al que sin autorización modifique, destruya o provoque pérdida de información contenida	Articles 211 bis 1 to Article 211 bis 5 describe complex infringements, close to the crimes of computer damage and of illegal access. They are the only special rules, at the federal level, specifically applicable to computer systems. On Article 211 bis 1, it is described

the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **Artículo 211 bis 2** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o	a general infringement; on Articles 211 bis 2 and 211 bis 3 the forbidden action must reach computer systems of the State or from Public Security; finally, on Articles 211 bis 4 and 211 bis 5 the action must be directed to the computer systems of institutions of the financial system. All the types of crimes are, mainly, directly to computer or data damage. All of them incriminate the unauthorised alteration, destruction or generating of loss of information stored in a computer system protected by any security mechanism. Besides, it is also incriminated, on Article 211 bis 1, Article 211 bis 2 and Article 211 bis 4, to take notice or copy information stored in a computer system protected by any security mechanism. As illegal access, these provisions don't cover enough Article 2 of the Convention. In fact, it is just incriminated to know information, but it is not incriminated to access a computer system. In other words, the mere act of accessing is not incriminated.

	hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 4** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.	
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the	**CÓDIGO PENAL FEDERAL** **Artículo 173** Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad: I - Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y II - Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se	Federal Penal Code describes, in a generic approach, the crime of violation of communications, on Article 173, incriminating the unduly opening and the unduly interception of an others written communication. On the other hand, Article 177 punishes whoever intercepts private communications without a judicial order. These generic provisions cover generically Article 3 of the Convention. However, the wording of the law just refers to communication, and not to other kind of eventual

offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	imponga de su contenido. **Artículo 177** A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.	transmission of computer data. As they are generic provisions, applicable to all kind of communications, it seems that the lack of reference to computer data in the type of crime can cause difficulties in concrete cases.
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CÓDIGO PENAL FEDERAL** **Artículo 211 bis 1** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **Artículo 211 bis 2** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos	Articles 211 bis 1 to Article 211 bis 5 describe, besides other, crimes of computer damage. These are the only special rules, at the Federal level, specifically applicable to computer systems. On Article 211 bis 1, it is described a general infringement; on Articles 211 bis 2 and 211 bis 3 the forbidden action must reach computer systems of the State or from Public Security; finally, on Articles 211 bis 4 and 211 bis 5 the action must be directed to the computer systems of institutions of the financial system. All the types of crimes are, mainly, directly to computer or data damage. All of them incriminate the unauthorised alteration, destruction or provocation of loss of information stored in a computer system protected by any security mechanism. Specifically referring to the data bases of the National Public Security System, there a special incrimination, regarding whoever intentionally and without right, inputs data in those data bases with the purpose of damaging that information or the system that stores it (*Ley General del Sistema Nacional de Seguridad Pública*, Article 139). Even if generally these crimes cover Article 4 of Budapest Convention, some of the wording described in that crime of the Convention is not considered on the Federal Penal Code.

	de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 3** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a	

	sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 4** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **Artículo 211 bis 5**	

	Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. **Ley General del Sistema Nacional de Seguridad Pública.** **Artículo 139** Se sancionará con dos a ocho años de prisión y de quinientos a mil días multa, a quien: I. Ingrese dolosamente a las bases de datos del Sistema Nacional de Seguridad Pública previstos en esta Ley, sin tener derecho a ello o, teniéndolo, ingrese a sabiendas información errónea, que dañe o que pretenda dañar en cualquier forma la información, las bases de datos o los equipos o sistemas que las contengan;	

	(…)	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.		There is not any specific legislation referring system interference.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability		There is not any legislation covering Article 6. However, *Ley de Instituciones de Crédito* (Credit Institutions Law), refers, specifically to credit and debit cards. On Article 112 bis, this law punishes whoever, without a legitimate reason, produces, reproduces, imports, prints or sells a credit or a debit card. It also punishes whoever obtains or sells information on banking accounts and whoever copies the data stored in a a credit or a debit card. Last, but not least, Article 112 bis punishes whoever, unduly, possesses or obtains, uses or sells devices able to obtain, copy or reproduce information stored within a credit or a debit card, with the aim of profit.

attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.		There is not any specific provision referring computer-related forgery.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its		There is not any specific provision referring computer related-fraud.

domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.		
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor	**CÓDIGO PENAL FEDERAL** **Artículo 202** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa. A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o	On Article 202 and Article 202 bis of the Federal Penal Code the law describes infringements related to child pornography. Article 202 states that it will be punished whoever prints, records, makes pictures or movies describing real or simulated exhibitionists corporal, lascivious or sexual acts in which take part minors under 18 years. These facts will be punished if the agent acts with aim of exhibit the materials, or transmit them in telecommunications or computer system network, or similar. But it will also be incriminated whoever reproduces, stores, distributes, sell, buys, rents, exhibits, promotes, transmits, imports or exports such materials. On the other hand, according to Article 202 bis, it will be incriminated who stores, buys, rents these materials for his own purposes, without aim of commercialisation. These provisions include criminal acts that comply with Article 9 of Budapest Convention. However, the Federal Penal Code does not provide a comprehensive definition of child pornography. Article 202 refers to real or simulated exhibitionists corporal, lascivious or sexual acts in which take part minors under 18 years. But this definition expressly excludes from the

engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores. **Artículo 202 BIS** Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.	infringement the situations described under nr 2 b and c of Article 9 (pornography with a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct).

7 PARAGUAY

20.

Within Paraguayan penal system, all the infringements respecting cybercrime are described on the Penal Code (Law nr 1160/97). Even if this is a modern legal instrument that entered in force in 1997 there are not many provisions respecting computers and cybercrime infringements. Within this code, it is classified as crime child pornography (Article 140), violation of the secret of communication (Article 146), data alteration (Article 174 and Article 248), data and document destruction (Article 253) computer sabotage (Article 175) and computer fraud (Article 188).

Beyond Penal Code, for the current time, there is not any further legislation on this matter. However, there is political interest, from the Congress, in the introduction of a new legal framework on cybercrime. In fact, it was introduced in the Congress, during March 2010, a draft law which scope is to change the Penal Code, specifically on regard of computer crimes. This bill, *Proyecto de Ley 3221*[3], is currently under discussion at the *Camara de Diputados*. It recognizes that technological development has surpassed all the expectations on this matter and on the capacity of anticipation of the misuse of technologies on criminal activities; so, it aims to enlarge criminalization to new realities, according to the international trends on this subject. This draft law will amend some articles of the Penal Code. It will be the case of Article 140 (pornography related with children and teenagers), Article 175 (computer systems sabotage) and Article 188 (fraud by means of a computer system). On the other hand, this bill will add new articles to the Penal Code. Besides other, Article 146-B (illegal access to data), 146-C (data interception), 146-D (preparation of illegal access and data interception) and174-B (illegal access to computer systems).

21.

Some of the provisions of Budapest Convention are completely covered by Penal Code from Paraguay. Some other, are partly covered, or have a different formulation, that neither does nor create always the need to adapt them. Finally, some provisions of the Convention are not covered at all by Paraguayan penal law, even if in some cases the *Proyecto de Ley 3221* already reduces the gaps.

Article 4 of Budapest Convention is already covered by Penal Code.

The same conclusion can be obtained regarding Article 8 of the Convention, even if in this case Penal Code of Paraguay has a different and more generic conceptual approach than the Convention.

Respecting Article 5, it is not completely covered, but most of the criminal acts described under the Convention are also considered in the Penal Code. In other words, there remain some wording differences. The same kind of differences can be underlined regarding Article 7 of Budapest Convention, which typical facts are not entirely covered national law, even if the generic kind of criminal acts described under the Convention are also considered in the Penal Code.

Currently, there are not legal provisions covering Article 2 (illegal access), Article 3 (illegal interception) and Article 6 (misuse of devices) of the Convention. However, *Proyecto de Ley* 3221 already describes new provisions (Article 146 B and Article 174 B), creating new crimes of illegal access to data and illegal access to computer systems, which will comply with the provisions of Budapest Convention.

Regarding Article 3 of the Convention, also the *Proyecto de Ley* 3221 includes a new provision (Article 146 C), creating a new crime of data interception. Such provision will comply with Article 3 of the Convention.

[3] http://www.diputados.gov.py/silpy/main.php?pagina=info_proyectos&&paginaResultado=info_tramitacion&idProyecto=3221

Finally, respecting Article 6 of the Convention, that has not yet any correspondence on national law, *Proyecto de Ley* 3221 will add an Article 146-D to Penal Code (punishing preparation of illegal access or data interception) and also will amend Article 188 (incriminating the production, obtaining for him or other, sell, storage or making available to other software that allows the user to practise, in general terms computer-related fraud). These amendments will approach Penal Code from Article 6, but it will remain uncovered, on one side, procuring for use and the mere possession of devices, and on the other, incriminating a wide range of devices that can be used to commit crimes.

22.
TABLE 6 – PARAGUAY

Convention of Budapest	**National Law**	**Comments**
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated		There is not a comprehensive list of definitions on regard of cybercrime, in the Penal Code or other legal instrument. Nevertheless, some particular definitions can be found within the Penal Code. On Article 174-B, nr 2, it is stated that computer system is any device, itself or in connexion or relation with other, which function is the automatic treatment of data, by the means of software. This definition follows Article 1, a of Budapest Convention. On the other hand, on Article 174, nr 3, it is stated that computer data refers just to the data stored or transmitted electronically, or magnetically, or in other way not immediately visible. This definition has a different approach from the definition stated on Article 1, b of the Convention.

by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.		There is not any legal provision covering Article 2. However, on *Proyecto de Ley* 3221, there is a provision (Article 146 B), creating a new crime of illegal access to data. By this provision, it will be punished whoever, unauthorized and violating security measures, obtains access to data. On the other hand, this bill includes also a new Article 174 B, defining the crime of illegal access to computer systems. According to this new rule, it will be punished whoever accedes to a computer system, using on this action a fake identity or exceeding an authorization. With this provision, if it is adopted by *Camara de Diputados*, Penal Code from Paraguay will comply with the provisions of Budapest Convention.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CODIGO PENAL DE PARAGUAY** **Artículo 146** **Violación del secreto de la comunicación** 1º El que, sin consentimiento del titular: 1. abriera una carta cerrada no destinada a su conocimiento; 2. abriera una publicación, en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación; 3. lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido	It is not clear nowadays if a computer communication can be considered a "closed letter" or a "publication", as Article 146 requires. This provision from Penal Code punishes the violation of communication, but it is not draft envisaging electronic realities. Thus, Article 3 of Budapest Convention is not covered by Paraguayan law. *Proyecto de Ley* 3221, nevertheless, includes a new provision (Article 146 C), creating a new crime of data interception. According to it, it will be punished whoever, by technical means, obtains data from a non-public transfer of data or from an electromagnetic radiation from a processing device. Such a text will comply with Article 3 of the Convention.

	de tal publicación para sí o para un tercero, será castigado con pena privativa de libertad de hasta un año o con multa. 2º La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte.	
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CODIGO PENAL DE PARAGUAY** **Artículo 174** **Alteración de datos** 1º El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. 2º En estos casos, será castigada también la tentativa. 3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible. **Artículo 253** **Destrucción o daño a documentos o señales** 1º El que con la intención de perjudicar a otro: 1. destruyera, dañara, ocultara o de otra forma suprimiera un documento o una graficación técnica, en contra del derecho de otro a usarlo como prueba. 2. borrara, suprimiera, inutilizara o alterara, en contra del derecho de disposición de otro, datos conforme al artículo 174, inciso 3º, con relevancia para la prueba, o 3. destruyera o de otra forma suprimiera	Article 174 of the Penal Code describes the crime of data alteration. This infringement incriminates whoever deletes, suppresses, makes unusable or alters data. For this purpose, it is stated that the word data refers to computer data stored or transmitted electronically, or magnetically, or in other way not immediately visible - Article 174, nr 3. This crime requires aim of harm the right of disposal of the owner of the data. Besides, Article 253 also states that it will be incriminated whoever deletes, suppresses, makes unusable or alters data, if they are relevant to the obtaining of evidence. Generically, these provisions cover Article 4 of Budapest Convention, even if there a light wording difference between the two texts.

	mojones u otras señales destinadas a indicar un límite o la altura de las aguas, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos, será castigada también la tentativa.	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**CODIGO PENAL DE PARAGUAY** **Artículo 175** **Sabotaje de computadoras** 1º El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante: 1. un hecho punible según el artículo 174, inciso 1º, o 2. la destrucción, inutilización sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos, será castigada también la tentativa.	According to Artícle 175 of the Penal Code, it will be punished computer sabotaje. This provision incriminates the hindering of the processing of critical data by the means of computer damage or by destruction, making unusable, subtraction or alteration of an installation of data processing, of a storage unity or other vital parts of a computer system. Some of the typical facts that integrate the description of Article 5 of Budapest Convention are not covered by Article 175, even if in general, beyond these details, most of the criminal acts described under the Convention are also considered in the Penal Code. *Proyecto de Ley* 3221 that will amend also Article 175, will not focus on those gaps. The scope of the draft law is to enlarge the extent of the incrimination. In current Article 175, the acts will be punished only if its target is a company, or an establishment, or a public entity. According to *Proyecto de Ley* 3221 it will be also punished the action against mere citizens or individuals.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of:		Currently there is not any provision complying with Article 6 of the Convention. However, *Proyecto de Ley* 3221 will add an Article 146-D to Penal Code, punishing preparation of illegal access or data interception. According to this new article, it will be punished to produce, disseminate or making accessible by any other means to a third person a security code, other access key or any software that allows the user to accede data. This provision will partly comply with Article 6 of Budapest Convention. But this Article 6 is much broader

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not		than codes and access keys, incriminating also, generically, a wide range of devices that can allow producing the same effects. It is true that *Proyecto de Ley* 3221 will also amend Article 188 ("fraudulent computer operations"), which incriminates in general terms computer-related fraud. This draft law will add a new paragraph 3 to Article 188, covering the production, obtaining for him or other, sell, storage or making available to other software that allows the user to practise the facts described on Article 188. Nevertheless, on the other hand, it remains uncovered procuring for use and the mere possession of these kinds of devices.

concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**CODIGO PENAL DE PARAGUAY** **Artículo 248** **Alteración de datos relevantes para la prueba** 1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos será castigada también la tentativa. 3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º.	There is a direct correspondence between Article 7 of the Convention and Article 248 of the Penal Code. Article 248 incriminates whoever alters data in such a way that it seems to be unauthentic. Those data must be relevant for evidence purposes. Wording of Article 7 of Budapest Convention is not entirely covered by the typical facts described on Article 248. However, the kind of criminal acts described under the Convention are also considered in the Penal Code. *Proyecto de Ley* 3221 will not amend this Article 248, but will introduce a new Article 248-B, extending the incrimination to forgery or alteration of data from credit or debit cards and other electronic means of payment.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of	**CODIGO PENAL DE PARAGUAY** **Artículo 188** **Operaciones fraudulentas por computadora** 1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. programación falsa; 2. utilización de datos falsos o incompletos; 3. utilización indebida de datos; o 4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el	The Penal Code from Paraguay covers computer-related fraud on Article 188. This provision ("fraudulent computer operations") incriminates whoever interferes in the result of data processing, by the means of the use of false or incomplete data, or the unduly use of data, or other unduly interferences on the processing of data. These acts must be practised with the aim of obtaining economic profit and the result must be the economic loss of a third person. Article 188 has a broad approach ("other interferences"), which completely complies with Article 8 of the Convention. *Proyecto de Ley* 3221 will amend Article 188, mainly

procuring, without right, an economic benefit for oneself or for another person.	patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.	clarifying the wording. But also adding a new paragraph 3, to cover the production, obtaining for himself or other, sell, storage or makes available to other software that allows to the user practise the facts described on Article 188.
Article 9 – Offences related to child pornography 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that	**CODIGO PENAL DE PARAGUAY** **Articulo 140** **Pornografía relativa a niños y adolescentes** 1º El que: 1. por cualquier medio produjere publicaciones, que contengan como temática actos sexuales con participación de personas menores de dieciocho años de edad y que busquen excitar el apetito sexual, 2. organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales. 3. distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del inciso 1°, será castigado con pena privativa de libertad de hasta cinco años. 2º El que reprodujera publicaciones según el numeral 1. del inciso 1º, será castigado con pena privativa de libertad de hasta tres años o multa. 3° La pena de los incisos anteriores podrá ser aumentada hasta diez años, cuando:	There is not a definition of child pornography in the Penal Code. However, on Article 140, that describes pornography related with children and teenagers, it is stated that it is punished to produce publications containing, as theme, sexual acts with the participation of minors under 18 years. Under Article 140 it will be punished also whoever distributes, imports, exports, offers, changes, exhibits, diffuses, promotes or finances the production or reproduction of that kind of material. But it is also punished the possession of such material, with the purpose of sexual excitement. This last reference was deleted on *Proyecto de Ley* 3221, that just will state, instead, that it will be punished the mere possession of that kind of materials. Beyond that, *Proyecto de Ley* 3221 does not bring other changes. This is a general provision, applicable online and offline. Even in the absence of a definition of child pornography, it is clear that Article 140 does not cover nº 2 b and c of Article 9, because just punishes acts referring to minors. Finally, also outside the incrimination, remains uncovered the activity of procuring child pornography.

visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	1. las publicaciones y espectáculos en el sentido de los incisos 1º y 2º se refieran a menores de catorce años 2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo; 3. el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente; 4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; 4° El que con la intención prevista en el numeral 1. del inciso 1º obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3º, será castigado con pena privativa de libertad de hasta tres años o con multa. 5° Se aplicará, en lo pertinente, también lo dispuesto en los artículos 57 y 94. 6° Los condenados por la comisión de hechos punibles descriptos en este artículo, generalmente no podrán ser beneficiados con el régimen de libertad condicional.	

8 PERU

23.

Peru does not have a specific law on cybercrime. The current legislation in force regarding cybercrime is the Penal Code. In fact, within the Penal Code (*Decreto Legislativo* nº 635, published on 8 of April 1991), there are some crimes related to computers and computers systems. It is namely the case of Articles 207-A to 207-C, introduced by *Ley* nº 27309, published on 17 of July of 2000. Besides these so called computer crimes, Penal Code also includes Article 183-A, incriminating child pornography.

This is a very outdated legislation and there is notice that, in the past, a proposal of alteration of this law was discussed in the Congress, but could not be well succeeded.

Currently, it is under discussion within the Ministry of Justice a new draft proposal of a new law. Within Ministry of Justice, it was organized a special committee with the scope of revising the Penal Code (*Comisión Especial Revisora del Código Penal*). This commission already drafted a proposal of revision of the Penal Code - *Consolidado de Propuestas*. This document is not finalized and it is still under discussion within the Government of Peru. It will add to Penal Code some very important new provisions and it will amend existing provisions: Article 202 (interference in the communications), Article 230 (child pornography), Article 261(computer intrusion) Article 262 (computer sabotage) Article 263 (sabotage to computer systems with security measures and special information), Article 264 (supply of devices with the scope of intrusion or sabotage) Article 265 (computer espionage), Article 266 (forgery of computer documents) and Article 268 (computer fraud).

24.

As a generic comment, it must be said that Penal Code of Peru has a very small and limited description of computer crimes. There are not any comprehensive definitions regarding cybercrime, in any legal instrument.

Only on regard of illegal access it can be said that national law fully complies with Budapest Convention. However, with the introduction in the Penal Code of a new Article 261, by *Consolidado de Propuestas*, it will be clarified the scope of the law and the legal interest beyond the legal provisions on regard illegal access.

Respecting child pornography, national law covers most of the provisions of Article 9 of Budapest Convention. *Consolidado de Propuestas* will also amend this part of the legislation and will cover gaps of current legislation: particularly it will cover the provisions of Article 9, nr 2, b and c, which are now uncovered by Penal Code.

On regard of illegal interception, national law does not comply completely with Budapest Convention, but *Consolidado de Propuestas* will introduce a new version of the law. This new version has a very broad approach and will cover Article 3 of Budapest Convention.

It can be said the same respecting data interference. Wording of Article 207-B of the Penal Code does not comply completely with Article 4 of the Convention. But *Consolidado de Propuestas* will revise the text and if this bill is adopted Penal Code will be closer to Article 4 of the Convention.

Concerning system interference, Article 207-A of the Penal Code is generic and comprehensive, but does not cover completely Article 5 of the Convention. *Consolidado de Propuestas* will introduce a new version of computer sabotage. This eventual new version of the Penal Code will comply with Article 5 of Budapest Convention.
Respecting Article 6 of Budapest Convention, current legislation of Peru does not incriminate any of the factual situations described under that provision. Nevertheless, *Consolidado de Propuestas* provides a new Article 262 incriminating, among other situations, the creation, introduction or transmission, by any means, of a virus or similar software, able to expand to other computer systems. Besides, also provides a new Article 264, incriminating whoever imports, produces, detains, distributes, sells or uses devices with the purpose of violating or suppress the security of a computer system. These provisions will partly cover Article 6 of Budapest Convention.
Current legislation of Peru does not incriminate specifically computer forgery and computer-related fraud. However, *Consolidado de Propuestas* provides a new Article 266, according to which it will be punished the forgery of a computer document. This provision will comply with Article 7 of Budapest Convention. On the other hand, it will introduce in the Penal Code a new Article 268, describing exactly computer fraud. This provision has a broad approach, but will comply with Article 8 of Budapest Convention.

25.
TABLE 7 – PERU

Convention of Budapest	**National Law**	**Comments**
Article 1 – Definitions For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c) "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a		There are not any comprehensive definitions regarding cybercrime, in any legal instrument.

computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.		
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**CODIGO PENAL** **Artículo 207-A** **Delito Informático** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas. **Artículo 207-C**	On Article 207-A it is described a so called computer crime. According to it, it will be punished whoever unduly accesses a data base, or a computer system, or any part of it. However, the law requires that the agent of the crime has the aim of draft, execute or alter a schema or similar, within that computer system. In other words, the mere access is not incriminated. This kind of requirement is allowed in the final part of Article 2. Thus, Article 207-A complies with Budapest Convention, regarding illegal access. *Consolidado de Propuestas* will introduce in the Penal Code a new Article 261, incriminating "computer intrusion". According to this provision, it will be punished whoever unduly, accedes, intercepts or interferes a computer system. Besides, this bill will also add to Penal Code a new Article 265. According to its provisions, it will be punished whoever obtains or discloses data stores in an information system. These new Articles will clarify the scope of the law and the legal interest beyond the legal provisions on regard illegal access.

	Delito informático agravado En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.	
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CODIGO PENAL** **Artículo 207-A** **Delito Informático** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas. **Artículo 207-C** **Delito informático agravado** En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:	On Article 207-A it is described a so called computer crime. According to it, it will be punished whoever unduly accesses a data base, or a computer system, or any part of it to interfere, intercept, accede, or copy information being transferred or stored in a data base. As illegal interception, this provision has a very narrow scope, and does not comply completely with Budapest Convention, because leaves outside the incrimination all kind of illegal accesses not referring to a data base. *Consolidado de Propuestas* will introduce a new version to Article 202 of the Penal Code, which provides a new crime of interference in communications. According to it, it will be punished whoever, unduly and unauthorised, interferes, intercepts or listen other communications, making use of the telephone, email, or other means of communication. This draft law has a very broad approach and will cover Article 3 of Budapest Convention.

	1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.	
Article 4 – Data interference 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 - A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CODIGO PENAL** **Artículo 207-A** **Delito Informático** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas. **Artículo 207-B** **Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras** El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no	On Article 207-A it is described a so called computer crime. According to it, it will be punished whoever unduly accesses a data base, or a computer system, or any part of it with the aim of draft, execute or alter a schema or similar, within that computer system. On Article 207-B it is described alteration, damage and destruction of a data base, a system, a network or software. According to this provision, it will be incriminated whoever uses, introduces or interferes unduly a data base, a system or software with the scope of alter, damage or destroy them. It is clear that it is purpose of this article to incriminate computer damage, or data interference. However, its wording does not comply completely with Article 4 of the Convention. *Consolidado de Propuestas* will introduce a new Article 262, incriminating computer sabotage. Its provisions state, besides other, that it will be punished whoever destroys, damages, alters or makes unusable data or information stored in a computer system. This Article also covers the creation, introduction or transmission, by any means, of a virus or similar software, able to expand to other computer systems. After this bill, if it is adopted, Penal Code will be closer to Article 4 of the Convention.

	menor de tres ni mayor de cinco años y con setenta a noventa días multa. **Artículo 207-C** **Delito informático agravado** En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.	
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**CODIGO PENAL** **Artículo 207-B** **Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras** El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa. **Artículo 207-C** **Delito informático agravado** En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de	On Article 207-B of the Penal Code it is described alteration, damage and destruction of a data base, a system, a network or software. According to this provision, it will be incriminated whoever uses, introduces or interferes unduly a data base, a system or software with the scope of alter, damage or destroy them. One of the purposes of this article is to incriminate system interference. Its wording is generic and comprehensive, but does not cover completely with Article 5 of the Convention. *Consolidado de Propuestas* will introduce a new Article 262, incriminating computer sabotage. This new provision will punish whoever destroys, damages, alters or practices any other act able to alter the normal functioning, or makes unusable a computer system. This eventual new version of the Penal Code will comply with Article 5 of Budapest Convention. It was also introduced, in *Consolidado de Propuestas,* a new Article 263, specifically incriminating the same kind of acts, but when their target are computer systems protected by security measures or storing special

	información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.	information.
Article 6 – Misuse of devices 1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed		Current legislation of Peru does not incriminate the factual situations described under Article 6 of the Convention. *Consolidado de Propuestas* provides a new Article 262 incriminating, among other situations, computer sabotage. This Article also covers the creation, introduction or transmission, by any means, of a virus or similar software, able to expand to other computer systems. Besides, *Consolidado de Propuestas* also provides a new Article 264, incriminating whoever imports, produces, detains, distributes, sells or uses devices with the purpose of violating or suppress the security of a computer system. These provisions will partly cover Article 6 of Budapest Convention, but some of the incriminated facts, under this article, remain uncovered by this bill.

before criminal liability attaches. 2 - This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 - Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an		Current legislation of Peru does not incriminate computer forgery, as described under Article 7 of the Convention. However, *Consolidado de Propuestas* provides a new Article 266, according to which it will be punished the forgery of a computer document. It will consider forgery of a document, to alter or eliminate a document stored in a computer system, create, modify or eliminate data from a document or input to a computer system a non existent document. This provision will comply with Article 7 of Budapest Convention.

intent to defraud, or similar dishonest intent, before criminal liability attaches.		
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CODIGO PENAL** **Artículo 207-A – Delito Informático** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas. **Artículo 207-C** **Delito informático agravado** En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.	Current legislation of Peru does not incriminate specifically computer-related fraud. Though, *Consolidado de Propuestas* introduces in the Penal Code a new Article 268, describing exactly computer fraud. According to it, it will be punished whoever, with aim of profit, obtains values or goods of other, by the means of access, interception, interference or by the use by any other mode of information technology or a communication system. This provision has a broad approach and will fully comply with Article 8 of Budapest Convention.
Article 9 – Offences related to child pornography	**CODIGO PENAL**	Child pornography is incriminated by Article 183-A of the Penal Code. Under this provision it will be punished

1 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2 - For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3 - For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A	**Artículo 183-A** **Pornografía infantil** El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a menores de catorce a dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ciento veinte a trescientos sesenta y cinco días multa. Cuando el menor tenga menos de catorce años de edad la pena será no menor de cuatro ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa. Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del Artículo 173, la pena privativa de libertad será no menor de ocho ni mayor de doce años.	whoever possess, promotes, produces, distributes, exhibits, offers, sells or publishes imports or exports objects, books or pictures using minors of less than eighteen years old. This provision covers most of the provisions of Article 9 of Budapest Convention. *Consolidado de Propuestas* will amend this Article (which will be renumbered as Article 230) to introduce two alterations. From one side, it will be specified that all the facts can be practiced by any means, including Internet. This is not a big change. The current version does not specify and so Internet is already a possible medium to commit this kind of crime. But on the other side, it is also added that the pornographic material, besides use minors of less than eighteen years old, can also just regard or represent minors of less than eighteen years old. This is a big change, because if this bill is adopted it will cover also some of the gaps of current legislation: particularly it will cover the provisions of Article 9, nr 2, b and c, which are now uncovered by Penal Code.

Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 - Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.		

9 Appendix A - Argentina

LEY 11.179
CODIGO PENAL DE LA NACION ARGENTINA

ARTICULO 128 — Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 129 — Será reprimido con multa de mil a quince mil pesos el que ejecutare o hiciese ejecutar por otros actos de exhibiciones obscenas expuestas a ser vistas involuntariamente por terceros.
Si los afectados fueren menores de dieciocho años la pena será de prisión de seis meses a cuatro años. Lo mismo valdrá, con independencia de la voluntad del afectado, cuando se tratare de un menor de trece años.

ARTICULO 153. - Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 153 BIS. - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 154. - Será reprimido con prisión de uno a cuatro años, el empleado de correos o telégrafos que, abusando de su empleo, se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia, se impusiere de su contenido, la entregare o comunicare a otro que no sea el destinatario, la suprimiere, la ocultare o cambiare su texto.

ARTICULO 155. - Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 156. - Será reprimido con multa de pesos mil quinientos a pesos noventa mil e inhabilitación especial, en su caso, por seis meses a tres años, el que teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.

ARTICULO 157. - Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 157 bis. -Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 172. - Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

ARTICULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
(…)
16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 183. - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 184. - La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:
1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 197. - Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 292.- El que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio, será reprimido con reclusión o prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado.
Si el documento falsificado o adulterado fuere de los destinados a acreditar la identidad de las personas o la titularidad del dominio o habilitación para circular de vehículos automotores, la pena será de tres a ocho años.
Para los efectos del párrafo anterior están equiparados a los documentos destinados a acreditar la identidad de las personas, aquellos que a tal fin se dieren a los integrantes de las fuerzas armadas, de seguridad, policiales o penitenciarias, las cédulas de identidad expedidas por autoridad pública competente, las libretas cívicas o de enrolamiento, y los pasaportes, así como también los certificados de parto y de nacimiento.

ARTICULO 293.- Será reprimido con reclusión o prisión de uno a seis años, el que insertare o hiciere insertar en un instrumento público declaraciones falsas, concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio.
Si se tratase de los documentos o certificados mencionados en el último párrafo del artículo anterior, la pena será de 3 a 8 años.

ARTICULO 298. - Cuando alguno de los delitos previstos en este Capítulo, fuere ejecutado por un funcionario público con abuso de sus funciones, el culpable sufrirá, además, inhabilitación absoluta por doble tiempo del de la condena.

10 Appendix B – CHILE

CODIGO PENAL
Lei Nr. 18742, de 12-11-1874, actualizada en 18-03-2010

Artículo 366 quinquies

El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo.
Para los efectos de este artículo y del artículo 374 bis, se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de estos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente seuales.

Artículo 374 bis

El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado medio a máximo.
El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio.

Artículo 374 ter

Las conductas de comercialización, distribución y exhibición señaladas en el artículo anterior, se entenderán cometidas en Chile cuando se realicen a través de un sistema de telecomunicaciones al que se tenga acceso desde territorio nacional.

Ley 19223, de 07-06-1993
TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente
Proyecto de Ley:

Artículo 1°

El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°

El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°

El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°

El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.
Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la
República.- Francisco Cumplido Cereceda, Ministro de Justicia.
Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Martita
Worner Tapia, Subsecretario de Justicia.

11 Appendix C - COLOMBIA

CÓDIGO PENAL

Artigo 218 - Pornografía con personas menores de 18 años
El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión 10 a 20 años y multa de 150 a 1500 salarios mínimos legales mensuales vigentes.
Igual pena se aplicará a quién alimente con pornografía infantil bases de dados de Internet, con o sin fines de lucro.
La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la victima.

Artículo 269 A - Acceso abusivo a un sistema informático.
El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 B - Obstaculización ilegítima de sistema informático o red de telecomunicación.
El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269 C - Interceptación de datos informáticos.
El que, sin orden judicial previa intercepte datos informáticos en su origen, desti-no o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los tras-porte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269 D - Daño informático.
El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 E - Uso de software malicioso.

El que, sin estar faculta-do para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 F - Violación de datos personales.
El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 G - Suplantación de sitios web para capturar datos personales.
El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269 H. - Circunstancias de agravación punitiva.
Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la in-formación o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269 I - Hurto por medios informáticos y semejantes.
El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269 J - Transferencia no consentida de activos.
El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cual-quier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

12 Appendix D – COSTA RICA

Código de Normas y Procedimientos Tributarios
Ley No. 4755, de 3 de mayo de 1971
(reformada por la Ley No.7900, de 3 de agosto de 1999)

Artículo 94 - Acceso desautorizado a la información
Será sancionado con prisión de uno a tres años quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente.

Artículo 95 - Manejo indebido de programas de cómputo
Será sancionado con pena de tres a diez años de prisión, quien sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

Ley General de Aduanas
Ley No. 7557, de 20 de octubre de 1995

Artículo 221 – Delitos informáticos
Será reprimido con prisión de uno a tres años quien:
a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.
b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.
c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.
d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

Ley de Administración Financiera de la República y Presupuestos Públicos
Ley No 8131, de 18 de setiembre de 2001

Artículo 111
Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la administración financiera y de proveeduría, alguna de las siguientes acciones:
a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.
b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.
c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.
d) Utilizar las facilidades del sistema para beneficio propio o de terceros.

Código Penal

Artículo 167 - Corrupción de menores
Será sancionado con pena de prisión de tres a ocho años, siempre que no constituya un delito más grave, quien promueva o mantenga la corrupción de una persona menor de edad o incapaz, ejecutando o haciendo ejecutar a otro u otros, actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta en participar en ellos o en verlos ejecutar.
La misma pena se impondrá a quien utilice a personas menores de edad o incapaces con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos, públicos o privados, de tal índole, aunque las personas menores de edad lo consientan.

Artículo 173 - Fabricación, producción o reproducción de pornografía
Será sancionado con pena de prisión de tres a ocho años, quien fabrique, produzca o reproduzca material pornográfico, utilizando a personas menores de edad, su imagen y/o su voz.
Será sancionado con pena de prisión de uno a cuatro años, quien transporte o ingrese en el país este tipo de material con fines comerciales.

Artículo 173 bis - Tenencia de material pornográfico
Será sancionado con pena de prisión de seis meses a dos años, quien posea material pornográfico en el que aparezcan personas menores de edad, ya sea utilizando su imagen y/o su voz.”

Artículo 174 - Difusión de pornografía

Quien comercie, difunda o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de uno a cuatro años. La misma pena se impondrá a quien exhiba, difunda, distribuya o comercie, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o donde se utilice su imagen, o lo posea para estos fines.

Artículo 196 bis - Violación de comunicaciones electrónicas
Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

Artículo 217 bis - Fraude informático
Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Artículo 229 bis - Alteración de datos y sabotaje informático
Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.
Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

Proyecto de Ley nº 17613 of the *Asamblea Legislativa de Costa Rica*

(reforma a varios artículos del Código Penal y adición de una nueva sección viii denominada "delitos informáticos y conexos" al titulo VII del Código Penal)

ARTÍCULO 1
Refórmense los artículos 167, 196, 196 bis, 209, 214, 217 bis, 229 bis y 288 del Código Penal, Ley N.° 4573, del 4 de mayo de 1970 y sus reformas, y se lean como sigue:

Artículo 167 - Corrupción
Será sancionado con pena de prisión de tres a ocho años, quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta.

La pena será de cuatro a diez años de prisión si el actor utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación busca encuentros de carácter sexual para sí o para otro, o para grupos, con una persona menor de edad o incapaz, o utiliza a estas personas para promover la corrupción, o los obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.

Artículo 196 - Violación de correspondencia o comunicaciones
Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidas a otra persona.
La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones; o

b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 Bis - Violación de datos personales
Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, y con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de cuatro a ocho años de prisión, cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) Cuando las datos sean de carácter público o estén contenidas en bases de datos públicas.

c) Si la información vulnerada corresponde a un menor de edad o incapaz.

d) Cuando las conductas afecten datos que revelen la ideología, religión, creencias, salud, origen racial, preferencia o vida sexual de una persona.

Artículo 209 - Hurto agravado
Se aplicará prisión de uno a nueve años, si el valor de lo sustraído no excede de cinco veces el salario base, y de cinco a diez años, si fuere mayor de esa suma, en los siguientes casos:

a) Cuando el hurto fuere sobre cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para la explotación agropecuaria.

b) Si fuera cometido aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado;

c) Si se hiciere uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida, claves de acceso, tarjetas magnéticas o dispositivos electrónicos.

d) Si fuere de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes;
e) Si fuere de vehículos dejados en la vía pública o en lugares de acceso público;
f) Si fuere de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o libradas a la confianza pública; y
g) Si fuere cometido por dos o más personas.

Artículo 214 - Extorsión
Será reprimido con pena de prisión de cuatro a ocho años, al que para procurar un lucro obligare a otro con intimidación o con amenazas graves a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.
La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.

Artículo 217 Bis - Fraude informático
Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, uso indebido de datos, programación, valiéndose de alguna operación informática, o artificio tecnológico, o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión si las conductas son cometidas contra sistemas de información públicos, sistema de información bancarios, de entidades financieras o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 229 Bis - Daño informático
Se impondrá pena de prisión de uno a tres años, al que sin autorización del titular, o excediendo la que se le hubiere concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 288 - Espionaje
Será reprimido con prisión de cuatro a ocho años, el que procurare u obtuviere indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales, o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación, o afecte la lucha contra el narcotráfico o el crimen organizado.
La pena será de cinco a diez años de prisión, cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

ARTÍCULO 2
Adiciónese un nuevo inciso 6) al artículo 229 y un artículo 229 ter al Código Penal, Ley N.° 4573, del 4 de mayo de 1970 y sus reformas, los cuales se leerán como sigue:

ARTÍCULO 229 - Daño agravado
Se impondrá prisión de seis meses a cuatro años:
[…]
6) Cuando el daño recayere sobre redes, sistemas o equipos informáticos, telemáticas o electrónicos, o sus componentes físicos, lógicos o periféricos.

ARTICULO 229 Ter - Sabotaje informático
Se impondrá pena de de prisión de tres a seis años, al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o impida, altere, obstaculice o modifique sin autorización, el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.
La pena será de cuatro a ocho años de prisión, cuando:

a) Como consecuencia de la conducta del autor sobreviniere peligro colectivo o daño social.
b) La conducta se realizare por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
c) El sistema informático sea de carácter público o la información está contenida en bases de datos públicas.
d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

ARTÍCULO 3
Modifíquese la Sección VIII del Título VII del Código Penal, Ley N.° 4573, del 4 de mayo de 1970 y sus reformas y se corra la numeración de los artículos subsiguientes, para que se lea como sigue:

Sección VIII
DELITOS INFORMÁTICOS Y CONEXOS

Artículo 230 - Suplantación de identidad
Será sancionado con pena de prisión de tres a seis años, quien suplante la identidad de una persona en cualquier red social, sitio de internet, medio electrónico o tecnológico de información. En la misma pena incurrirá quien utilizando una identidad falsa o inexistente cause perjuicio a un tercero.
La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.

Artículo 231 - Espionaje informático

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle, información de valor para el tráfico económico de la industria y el comercio.

Artículo 232 - Instalación o propagación de Programas informáticos maliciosos

Será sancionado con prisión de uno a seis años, quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.

b) A quien, sin autorización instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como Sitios de Internet Atacantes.

c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de internet que permita la instalación de programas informáticos maliciosos.

d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i. Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii. Afecte el funcionamiento de servicios públicos.

iii. Obtenga el control a distancia de un sistema o de una red informática, para formar parte de una red de ordenadores zombi.

iv. Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v. Afecte sistemas informáticos de la salud y la afectación de los mismos pueda poner en peligro la salud o vida de las personas.

vi. Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 233 - Suplantación de páginas electrónicas

Se impondrá pena de prisión de uno a tres años, a quien en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando como consecuencia de la suplantación del sitio legítimo de Internet, y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

12.1.1.1 **Artículo 234 - Facilitación del delito informático**

12.1.1.2 Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

12.1.1.3 **Articulo 235 - Narcotráfico y crimen organizado**

12.1.1.4 La pena se duplicará cuando cualquiera de los delitos cometidos por medio un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

Artículo 236 - Difusión de Información Falsa

Será sancionado con pena de tres a seis años de prisión quien a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones propague o difunda noticias, o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

Rige a partir de su publicación.

13 Appendix E – MÉXICO

CÓDIGO PENAL FEDERAL
(publicado en el Diario Oficial de la Federación el 14 de agosto de 1931 - última reforma publicada en el 19 de Agosto de 2010)

Artículo 173 - Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad:
I.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y
II.- Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.

Artículo 177 - A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Artículo 202 - Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.
A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.
La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 bis - Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

Artículo 211 bis 1 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3 - Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5 - Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6 - Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7 - Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Ley General del Sistema Nacional de Seguridad Pública.

Artículo 139
Se sancionará con dos a ocho años de prisión y de quinientos a mil días multa, a quien:
I. Ingrese dolosamente a las bases de datos del Sistema Nacional de Seguridad Pública previstos en esta Ley, sin tener derecho a ello o, teniéndolo, ingrese a sabiendas información errónea, que dañe o que pretenda dañar en cualquier forma la información, las bases de datos o los equipos o sistemas que las contengan;
(…)

Ley de Instituciones de Crédito.

Artículo 112 Bis
Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:

I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada.

14 Appendix F – PARAGUAY

CODIGO PENAL DE PARAGUAY
LEY Nº 1160/97

Articulo 140
Pornografía relativa a niños y adolescentes
1º El que:

1. por cualquier medio produjere publicaciones, que contengan como temática actos sexuales con participación de personas menores de dieciocho años de edad y que busquen excitar el apetito sexual,
2. organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales.
3. distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del inciso 1°, será castigado con pena privativa de libertad de hasta cinco años.

2º El que reprodujera publicaciones según el numeral 1. del inciso 1º, será castigado con pena privativa de libertad de hasta tres años o multa.
3° La pena de los incisos anteriores podrá ser aumentada hasta diez años, cuando:

1. las publicaciones y espectáculos en el sentido de los incisos 1º y 2º se refieran a menores de catorce años
2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
3. el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie;

4° El que con la intención prevista en el numeral 1. del inciso 1º obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3º, será castigado con pena privativa de libertad de hasta tres años o con multa.
5° Se aplicará, en lo pertinente, también lo dispuesto en los artículos 57 y 94.
6° Los condenados por la comisión de hechos punibles descriptos en este artículo, generalmente no podrán ser beneficiados con el régimen de libertad condicional.

Artículo 143
Lesión de la intimidad de la persona
1º. El que, ante una multitud o mediante publicación en los términos del artículo 14, inciso 3º, expusiera la intimidad de otro, entendiéndose como tal la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud, será castigado con pena de multa.
2º. Cuando por su forma o contenido, la declaración no exceda los límites de una crítica racional, ella quedará exenta de pena.

3º. Cuando la declaración, sopesando los intereses involucrados y el deber de comprobación que según las circunstancias incumba al autor, sea un medio adecuado para la persecución de legítimos intereses públicos o privados, ella quedará exenta de pena.
4º. La prueba de la verdad de la declaración será admitida sólo cuando de ella dependiera la aplicación de los incisos 2º y 3º.

Artículo 144
Lesión del derecho a la comunicación y a la imagen
1º El que sin consentimiento del afectado:
1. escuchara mediante instrumentos técnicos;
2. grabara o almacenara técnicamente; o
3. hiciera, mediante instalaciones técnicas, inmediatamente accesible a un tercero, la palabra de otro, no destinada al conocimiento del autor y no públicamente dicha, será castigado con pena privativa de libertad de hasta dos años o con multa.
2º La misma pena se aplicará a quien, sin consentimiento del afectado, produjera o transmitiera imágenes:
1. de otra persona dentro de su recinto privado;
2. del recinto privado ajeno;
3. de otra persona fuera de su recinto, violando su derecho al respeto del ámbito de su vida íntima.
3º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme a los incisos 1º y 2º.
4º En los casos señalados en los incisos 1º y 2º será castigada también la tentativa.
5º La persecución penal del hecho dependerá de la instancia de la víctima, salvo que el interés público requiera una persecución de oficio. Si la víctima muriera antes del vencimiento del plazo para la instancia sin haber renunciado a su derecho de interponerla, éste pasará a sus parientes.

Artículo 146
Violación del secreto de la comunicación
1º El que, sin consentimiento del titular:
1. abriera una carta cerrada no destinada a su conocimiento;
2. abriera una publicación, en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación;
3. lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero,
será castigado con pena privativa de libertad de hasta un año o con multa.
2º La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte.

Artículo 174
Alteración de datos
1º El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º En estos casos, será castigada también la tentativa.
3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

Artículo 175
Sabotaje de computadoras
1º El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante:

1. un hecho punible según el artículo 174, inciso 1º, o
2. la destrucción, inutilización sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital,

será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos, será castigada también la tentativa.

Artículo 187
Estafa
1º El que con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, y mediante declaración falsa sobre un hecho, produjera en otro un error que le indujera a disponer de todo o parte de su patrimonio o el de un tercero a quien represente, y con ello causara un perjuicio patrimonial para sí mismo o para éste, será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos, será castigada también la tentativa.
3º En los casos especialmente graves, la pena privativa de libertad podrá ser aumentada hasta ocho años.
4º En lo pertinente se aplicará también lo dispuesto en los artículos 171 y 172.

Artículo 188
Operaciones fraudulentas por computadora
1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. programación falsa;
2. utilización de datos falsos o incompletos;
3. utilización indebida de datos; o
4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el patrimonio de otro,

será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.

Artículo 248

Alteración de datos relevantes para la prueba
1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos será castigada también la tentativa.
3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º.

Artículo 249
Equiparación para el procesamiento de datos
La manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3º, será equiparada a la inducción al error en las relaciones jurídicas.

Artículo 253
Destrucción o daño a documentos o señales
1º El que con la intención de perjudicar a otro:

1. destruyera, dañara, ocultara o de otra forma suprimiera un documento o una graficación técnica, en contra del derecho de otro a usarlo como prueba.
2. borrara, suprimiera, inutilizara o alterara, en contra del derecho de disposición de otro, datos conforme al artículo 174, inciso 3º, con relevancia para la prueba, o
3. destruyera o de otra forma suprimiera mojones u otras señales destinadas a indicar un límite o la altura de las aguas,

será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos, será castigada también la tentativa.

Proyecto de Ley 3221
(que modifica el Código Penal - delitos informáticos)

EL CONGRESO DE LA NACION PARAGUAYA SANCIONA CON FUERZA DE LEY:

Artículo 1º.- Modificase los artículos 140, 175, y 188 de la Ley Nº 1160 "CODIGO PENAL", de fecha 26 de noviembre de 1997, e introdúzcanse en la misma los artículos 146º B, 146º C, 146º D, 174º B, 175º B, y 248º B, los cuales quedan redactados de la siguiente manera:

Artículo 140
Pornografía relativa a niños y adolescentes

1º.- El que:

1. Produjere publicaciones (Art. 14, inc. 3º), que representan actos sexuales con participación de personas menores de dieciocho años de edad,
2. Organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales; o
3. Distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.

2º.- El que reprodujera publicaciones según el numeral 1 del inciso 1º, será castigado con pena privativa de libertad de hasta tres años o multa.

3º- La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:

1. Las publicaciones y espectáculos en el sentido de los incisos 1º y 2º se refieran a menores de catorce años; o se dé acceso a publicaciones y espectáculos en sentido de los incisos 1º y 2º a menores de catorce años;
2. El autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
3. El autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
4. El autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o
5. El autor actuará comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.

4º.- El que con la intención prevista en el numeral 1 del inciso 1º obtuviera la posesión de publicaciones en el sentido de los incisos 1º y 3º, será castigado con pena privativa de libertada de hasta tres años o con multa.

5.- Se aplicará, en lo pertinente, también lo dispuesto en los artículos 57 y 94.

Artículo 146 B

Acceso indebido a datos

1º. El que sin autorización y violando medidas de seguridad obtuviere para sí o para terceros acceso a datos no destinados a él, será castigado con pena privativa de libertad de hasta tres años o multa.

2º. Como datos en sentido del inciso 1º se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible.

Artículo 146 C

Intercepción de datos

El que sin autorización, utilizando medios técnicos obtuviere para si o para un tercero datos en sentido del Artículo 146 bis, inciso 2º no destinados para él.

3. De una transferencia no pública de datos o

4. De la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor.

Artículo 146 D
Preparación de acceso indebido e interceptación de datos
1º. El que prepare un hecho punible según Artículo 146 B o Artículo 146 C produciendo, difundiendo o haciendo accesible de otra manera a terceros.
1. Clave de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 B, inciso 2, o
2. Programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa.

2º. Se aplicará, en lo pertinente, lo previsto en el Artículo 266, inciso 2º.

Artículo 174 B
Acceso indebido a sistemas informáticos
1º. El que accediere a un sistema informático, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de hasta tres años o multa.
2º. Se entenderá como sistema informático a todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento automatizado de datos por medio de un programa informático.

Artículo 175
Sabotaje de sistemas informáticos
1º. El que obstaculizara un procesamiento de datos de un particular, de una empresa o de una entidad de la administración pública mediante:
1. Un hecho punible según el artículo 174, inciso 1º;o
2. La destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte componente indispensable, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º. En estos casos será castigada también la tentativa.

Artículo 175 bis
Instancia
En los casos de los artículos 174 y 175, la persecución penal dependerá de la instancia de la víctima, salvo que, a criterio del Ministerio Público, un interés público especial requiera una persecución pública.

Artículo 188
Estafa mediante sistemas informáticos
1º. El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante.
1. Una programación incorrecta,
2. El uso de datos falsos o incompletos,
3. El uso indebido de datos u

4. Otra maniobra no autorizada, y con ello causara un perjuicio al patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º. Se aplicará también lo dispuesto en el Artículo 187, incisos 2º al 4º.

3º. El que preparare un hecho punible señalado en el inciso 1º de manera tal que produjera, obtuviera para sí u otro, tenga en venta, almacenara o proporcionara a terceros programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

4º. En los casos señalados en el inciso 3º se aplicará lo dispuesto en el Artículo 266, incisos 2º y 3º.

Artículo 248 B

Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago

1º. El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error

1. Falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago, o
2. Adquiera para si o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º. Se castigará también la tentativa.

3º. Cuando el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados, la pena será privativa de libertad de hasta diez años.

4º. Tarjetas de crédito en sentido del inciso 1º son aquellas:

1. Que han sido emitido por una entidad de crédito o de servicios financieros, y
2. Que por su configuración o codificación son especialmente protegidas contra su falsificación.

5º. Medios electrónicos de pago en el sentido del inciso 1º, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, en el cual se almacenan digitalmente unidades de valor recargable, ya sea este, un medio físico o una memoria de un sistema digital y pueden permitir al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta.

15 Appendix G – PERU

CODIGO PENAL
DECRETO LEGISLATIVO Nº 635, publicado: 08.04.91

Artículo 183-A
Pornografía infantil
El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a menores de catorce a dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ciento veinte a trescientos sesenta y cinco días multa.
Cuando el menor tenga menos de catorce años de edad la pena será no menor de cuatro ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa.
Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del Artículo 173, la pena privativa de libertad será no menor de ocho ni mayor de doce años.

Artículo 207-A
Delito Informático
El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207-B
Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras
El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207-C
Delito informático agravado

En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:
1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

Comisión Especial Revisora del Código Penal
CONSOLIDADO DE PROPUESTAS

CAPITULO IV
VIOLACION DEL SECRETO DE LAS COMUNICACIONES

Artículo 202
Interferencia en las comunicaciones
El que indebidamente interfiere, intercepta o escuche comunicaciones de cualquier persona, sin autorización, utilizando servicio telefónico, de cualquier modalidad de teleservicio, del correo electrónico u otra modalidad del servicio de valor añadido, o cualquier otra forma de comunicación será reprimida con pena privativa de libertad no menor de tres ni mayor de cinco.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de seis e inhabilitación conforme al Artículo 35 inciso 1, 2 y 4
Será reprimido con pena privativa de libertad no menor tres ni mayor de seis el que en perjuicio de tercero, comercializa, trasfiere, reproduce o adquiere en forma directa o indirecta, en provecho propio o de tercera persona, los registros de la información obtenida indebidamente descrita en el primer párrafo.

Artículo 203
Venta, compra o comercialización de equipos electrónicos para la interceptación de comunicación privada entre personas
El que venda, compre o comercialice equipos electrónicos para la interceptación de comunicación privada entre personas será reprimido con pena privativa de la libertad no menor de cuatro ni mayor de ocho años.

Artículo 204
Supresión o extravío indebido de correspondencia
El que indebidamente, suprime o extravía de su destino una correspondencia epistolar o telegráfica, aunque no la haya violado, será reprimido con prestación de servicio comunitario de veinte a cincuenta y dos jornadas.

Artículo 205

Publicación indebida de correspondencia
El que publica, indebidamente, una correspondencia epistolar o telegráfica, no destinada a la publicidad, aunque le haya sido dirigida, será reprimido, si el hecho causa algún perjuicio a otro, con limitación de días libres de veinte a cincuenta y dos jornadas.

CAPITULO XI
OFENSAS AL PUDOR PÚBLICO

Artículo 228
Publicación en los medios de comunicación sobre delitos de libertad sexual a menores
Los gerentes, los responsables y los que intervienen en la elaboración de las publicaciones o ediciones a transmitirse a través de los medios de comunicación masivos que publiciten la explotación sexual, turismo sexual o la trata de menores de dieciocho años de edad serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de seis años.

Artículo 229
Exhibiciones y publicaciones obscenas
El que realiza exhibiciones, gestos, tocamientos u otra conducta de índole obscena será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años.
Será reprimido con pena privativa de libertad no menor de seis ni mayor de diez años:
1. El que muestra, vende o entrega a un menor de dieciocho años, por cualquier medio, objetos, libros, escritos, imágenes, visuales o auditivas que por su carácter obsceno puedan afectar gravemente el pudor, excitar prematuramente o pervertir su desarrollo sexual.
2. El que incita a un menor de dieciocho años a la práctica de un acto obsceno o le facilita la entrada a los prostíbulos u otros lugares de corrupción.
3. El administrador, vigilante o persona autorizada para controlar un cine u otro espectáculo donde se exhiban representaciones obscenas que permita el ingreso a estos lugares de un menor de dieciocho años.

Artículo 230
Pornografía infantil
El que posee, promueve, fábrica, distribuye, exhibe, ofrece, comercializa o pública, importa o exporta por cualquier medio incluido la Internet objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice, refiere o represente a personas menores de dieciocho años de edad será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con doscientos a trescientos sesenta y cinco días-multa y con la consecuencia accesoria prevista en el artículo 109 inciso 1.
Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 215, o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de diez ni mayor de quince años.

CAPITULO XII
DISPOSICION COMUN

Artículo 231
Disposición Común
1. Los ascendientes, descendientes, afines en línea recta, hermanos y cualquier persona que, con abuso de autoridad, encargo o confianza, cooperen a la perpetración de los delitos comprendidos en los Capítulos IX, X y XI de este Título actuando en la forma señalada por el artículo 25 primer párrafo serán reprimidos con la pena de los autores.
2. El Juez impondrá la pena de inhabilitación al autor o cómplice de los delitos comprendidos en los Capítulos IX, X y XI de este Título, de conformidad con el artículo 35 del Código Penal.
Nota. Consideramos que la pena de Inhabilitación debe elevarse hasta diez años como lo señala el Proyecto del Código Penal; asimismo, debe de considerarse la inhabilitación con carácter indefinido en el caso que las víctimas sean menores de edad.

CAPÍTULO X
DELITOS INFORMÁTICOS

SECCIÓN I
DELITOS CONTRA LOS SISTEMAS DE INFORMACIÓN, TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACION

Artículo 261
Intrusismo informático
El que sin la debida autorización acceda, intercepte o interfiera un sistema de información o una tecnología de información será reprimido con una pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 262
Sabotaje informático
El que destruya, dañe, modifique o realice cualquier acto que altere el normal funcionamiento o inutilice un sistema de información o una tecnología de información o de comunicación o cualquiera de los componentes que los conforman será reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.
Se le impondrá la misma pena a quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema de información o tecnología de información o de comunicación en cualquiera de sus componentes.
La pena privativa de la libertad será no menor de tres ni mayor de seis años si la alteración o inutilización se llevase a cabo mediante la creación, introducción o transmisión, por cualquier medio, de un virus informático o programa análogo capaz de extenderse a otros sistemas de información de comunicación o sus componentes.

Artículo 263
Intrusismo o sabotaje de sistemas o tecnologías de información con medidas de seguridad o información especial

La pena será privativa de libertad no menor de cuatro ni mayor de siete años si los delitos previstos en los artículos precedentes recaen sobre cualquiera de los componentes de un sistema de información o de una tecnología de información o de comunicación protegidos por medidas de seguridad que estén destinados a funciones públicas o a servicios privados y que contengan información personal o patrimonial reservada sobre personas naturales o jurídicas.

Artículo 264
Prestación de equipos y servicios con fines de intrusismo y/o sabotaje
El que importe, fabrique, posea, distribuya, venda o utilice equipos o dispositivos con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema de información o de una tecnología de información o de comunicación, o el que ofrezca o preste servicios que contribuyan a ese propósito será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 265
Espionaje informático
El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema de información o en una tecnología de información o de comunicación en cualquiera de sus componentes será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.
La pena privativa de la libertad será no menor de tres ni mayor de siete años si el delito se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.
La pena privativa de la libertad será no menor de cuatro ni mayor de diez si como consecuencia de dicho acto se pusiere en peligro la seguridad del Estado, la confiabilidad general de las operaciones financieras o administrativas de las instituciones públicas o privadas afectadas o resultare algún daño para las personas naturales o jurídicas.

Artículo 266
Falsificación de documento informático
Será reprimido con una pena privativa de libertad no menor de dos ni mayor de seis años el que a través de cualquier medio realiza, de manera que pueda perjudicar a otro, cualquiera de las siguientes conductas:
1. Modifique o elimine un documento que se encuentre incorporado en un sistema de información o en una tecnología de información o de comunicación.
2. Cree, modifique o elimine datos de un documento que se encuentre incorporado en un sistema de información o en una tecnología de información o de comunicación.
3. Incorpore a un sistema de información o a una tecnología de información o de comunicación un documento inexistente.
Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio o hubiere producido un perjuicio efectivo a otro, la pena será privativa de libertad no menor de tres ni mayor de siete años.

Artículo 267
Falsificación de tarjetas inteligentes

El que sin autorización, cree, capture, grabe, copie o duplique la data o información contenidas en una tarjeta inteligente para usarla como si fuese verdadera será reprimido con una pena privativa de libertad de tres a cinco años.
La misma pena se le impondrá al que use la data, o una tarjeta inteligente conteniendo esta data, obtenida por otro mediante la conducta del párrafo precedente.

Artículo 268
Fraude Informático
El que, para obtener provecho para sí o para otro, se apodere de bienes o valores tangibles o intangibles de carácter patrimonial, sustrayéndolos a su tenedor mediante el acceso, interceptación, interferencia o uso de cualquier forma de una tecnología de información o un sistema de comunicación será reprimido con una pena privativa de libertad no menor cuatro, ni mayor de ocho años cuando el valor del bien o el valor en sí mismo sea superior a una remuneración mínima vital.

Artículo 269
Agravante
La pena correspondiente a los delitos previstos en el presente capítulo e inclusive a sus agravantes se incrementará en un tercio por encima del marco penal máximo en los siguientes casos:
1. Si el agente comete el delito en calidad de integrante de una organización delictiva.
2. Si el delito es cometido mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 270
Obtención indebida de bienes o servicios
El que utilice sin autorización un medio electrónico de pago ajeno o el que utilice tecnologías de información o de comunicación para obtener indebidamente cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años.

Artículo 271
Manejo fraudulento de medios electrónicos de pago
Será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años, el que sin autorización realice cualquiera de las siguientes conductas:
1. Cree, capture, grabe, copie, altere, duplique o elimine por cualquier medio la data o información contenidas en un medio electrónico de pago.
2. Cree, duplique o altere mediante el uso de tecnologías de información o de comunicación, la data o información en un sistema de información con el objeto de incorporar usuarios, cuentas, registros, o consumos inexistentes o modifique la cuantía de éstos.
3. Adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de medios electrónicos de pago, o de la data o información contenidos en ellos o en un sistema de información o de comunicación.

Artículo 272
Apropiación de medios electrónicos de pago
El que se apropie de medio electrónico de pago que se haya perdido, extraviado o le haya sido entregado por equivocación con el fin de usarlo, venderlo, o transferirlo a persona distinta del usuario autorizado o entidad emisora será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. La misma pena se impondrá a quien adquiera o reciba el medio electrónico de pago a que se refiere el párrafo anterior.

Artículo 273
Provisión indebida de bienes o servicios
El que provea a otro de dinero, efectos, bienes, servicios o cualquier otra cosa de valor económico con la presentación de un medio electrónico de pago que ha sido falsificado o alterado o que se encuentre revocado o que ha sido indebidamente obtenido o retenido será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años.

Artículo 274
Posesión de equipo informático para falsificación de medios electrónicos de pago
El que sin estar debidamente autorizado para fabricar, emitir o distribuir medios electrónicos de pago reciba, adquiera, posea, custodie, distribuya, transfiera, comercialice o venda cualquier equipo de fabricación de estos medios de pago o cualquier equipo o componente que capture, grabe o copie o transmita la data o información de dichos medios de pago será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 275
Excusa absolutoria. Exención de Pena
No son reprimibles, sin perjuicio de la reparación civil, los hurtos, apropiaciones, defraudaciones o daños que se causen:
1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.
2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.
3. Los hermanos y cuñados, si viviesen juntos.

Artículo 276
Circunstancia agravante por el empleo de las Tecnologías de la Información y de las Comunicaciones
Si para la perpetración de un hecho punible contemplado en el Código Penal el agente utiliza o emplea tecnología de la información o de las comunicaciones, tal uso constituirá circunstancia agravante; el Juez elevará la pena hasta la mitad por encima del máximo legal fijado para el delito cometido, no siendo de aplicación si esta circunstancia se encuentra prevista en el tipo penal.