COMMENTS BY THE ARGENTINE REPUBLIC FOR THE SECOND SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

For the purpose of encouraging and facilitating an effective debate during the Second Session of the Ad Hoc Group, the Argentine Republic is pleased to present its views on the following aspects of the Convention which are under negotiation: General provisions, Criminalization, and Procedural measures and law enforcement.

A. GENERAL PROVISIONS

1. **Purpose**. The purpose of this convention is to promote cooperation to prevent and combat "cybercrime" more effectively.

2. **Definitions.** In principle, it is necessary to define:

-"computer system": any isolated device or set of interconnected or interrelated devices, the function of which, or that of any of its elements, is the automatic processing of data in the execution of a program;

-"service provider": shall mean: (i) any public or private entity that provides to the users of its services the ability to communicate by means of computer systems, and (ii) any other entity that processes or stores computer data on behalf of such communication service or the users of that service;

-"computer data": any representation of facts, information or concepts expressed in any form that is suitable for computer processing, including programs designed for a computer system to perform a function;

-"traffic data": any computer data relating to a communication carried out by means of a computer system, generated by the latter as an element of the chain of communication, and indicating the origin, destination, route, time, date, size and duration of the communication and the type of underlying service.[1]

"Content data": any data relating to a communication carried out by means of a computer system, available or stored in the computer system; and which are not covered by the definitions of traffic data or basic subscriber data.

[1] The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services.
The "destination" refers to comparable indication of a communications facility to which communications are transmitted.
The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, e-mail or instant messaging.

"Basic subscriber information": any information, in the form of computer data or otherwise, held by a service provider, relating to the subscribers of its services and which may enable to establish: (i) the type of service, the technical provisions adopted thereto and the period of service; (ii) the subscriber's identity –postal or geographical address, telephone and other access number, billing and payment information, available under a contract or service provision agreement-; (iii) and/or any information relating to the location of communication equipment, available under a contract or a service provision agreement[2].

-"child sexual abuse material": Any representation of a minor under eighteen (18) years of age engaged in sexually explicit activities or any representation of his or her genitals for predominantly sexual purposes.

-"property": assets of any type, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets;

-"proceeds of crime": any property of whatever type derived from or obtained, directly or indirectly, through the commission of an offence;

-"freezing" or "seizure": temporarily prohibiting the transfer, conversion, disposition or moving of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

-"confiscation": permanent deprivation of property by order of a court or other competent authority;

-"predicate offence": any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article XXX of this Convention.

3. **Scope of Application**.

1. This Convention shall apply, unless otherwise provided for herein, to the prevention, investigation and prosecution of the offences established in accordance with articles [number] of this Convention.

2. Subject to such exceptions as may be established for reasons of public policy of each State and Human Rights rules, the (section, title, chapter] relating to "Procedural Measures and law enforcement" of this Convention shall apply to:

i. any criminal offence committed through a computer system; and

ii. the collection of electronic evidence of a criminal offence.

[2] For some Parties, it may include certain traffic data necessary to identify a subscriber to a service, for example, the IP address used at the time the account was created, the most recent login IP address or the log.

3. Subject to such exceptions as may be established for reasons of public policy of each State and Human Rights rules, the (section, title, chapter] relating to "International Cooperation" of this Convention shall apply to:

i. any other criminal offence committed through a computer system; and

ii. the collection of electronic evidence of any offence.

4. **Respect of Sovereignty**. 1. State Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and integrity of the States, as well as that of non-intervention in the domestic affairs of other States.

2. Nothing in this Convention shall entitle a State Party to exercise in the territory of another State jurisdiction or functions that are reserved exclusively for the authorities of that other State by its domestic law.

B. CRIMINALIZATION

1. The following criminal offences and their definitions are encouraged to be incorporated into the Convention:

-"**Illegal access"**: Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the intentional and unlawful access to the whole or any part of a computer system. The Parties may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other criminal intent, or in relation to a computer system that is connected to another computer system.

-"Illegal interception": Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the intentional and unlawful interception through technical means of non-public transmissions of computer data to, from or within a computer system, including the electromagnetic emissions transporting such computer data. Parties may require that the offence be committed with criminal intent or in connection with a computer system connected to another computer system.

-"Attack on data integrity". 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law any intentional and unlawful act that damages, deletes, deteriorates, alters or suppresses computer data. 2. The Parties may reserve the right to require that the acts defined in paragraph 1 result in serious damage.

- "**Attack on system integrity"**. Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the serious, intentional and unlawful hindering of the functioning of a computer system by means of inputting, transmitting, damaging, deleting, altering or suppressing computer data.

- "**Misuse of equipment and technical devices"**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offences in its domestic law the intentional and unlawful commission of the following acts:

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 criminal offences established in accordance with articles xx to xx of this Convention. ii. a computer password, access code or similar computer data which may enable access to the whole or part of a computer system, with intent that it be used for the purpose of committing any of the criminal offences contemplated in articles xx to xx.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available referred to in paragraph 1 of this article is not for the purpose of committing of one of the criminal offences provided for in accordance with articles xx to xx of this Convention, as in the case of the authorized testing or the protection of a computer system.

3. The Parties may reserve the right not to apply paragraph 1 of this article, provided that such reservation does not affect the sale, distribution or any other form of making available of the items referred to in subparagraph 1 a) ii) of this article.

- "Computer-related fraud": The Parties shall adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law the intentional and unlawful acts that cause damage to the property of another person by means of:

a. the 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, unlawfully, an economic benefit for oneself or for another person.

- **"Offences related to child sexual abuse material"**. 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law the intentional and unlawful commission of the following acts:

a. producing child pornography with 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. possessing child pornography in a computer system or on a computer-data storage device.

2. For the purpose of paragraph 1 above, the term "child pornography" shall mean any pornographic material containing a visual representation of a minor engaged in sexually explicit behavior.

3. For the purposes of paragraph 2 above, the term “minor” shall mean any person under the age of 18 years. The parties may, however, require a lower age limit, which shall be at least 16 years of age.

- **“Offences related to infringements of copyright and related rights”**.

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences in their domestic law the infringements of copyright as may be defined by the legislation of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971, revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by said conventions, where such acts are committed deliberately, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences in their domestic law the infringements of related rights, as defined by the legislation of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by said conventions, where such acts are committed deliberately, on a commercial scale and by means of a computer system.

3. In well-delimited circumstances, a Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article, provided that other effective remedies are available and that such reservation does not violate that Party´s international obligations under the international instruments referred to in paragraphs 1 and 2 of this article.

2. Other criminal offences. In the exchanges held among delegations during the First Session, no consensus was reached on the final list of criminal offences to be incorporated and described by the Convention. While there was consensus on a set of offences, the so-called “cyber-dependent” and a reduced number of “cyber-assisted” offences, some delegations supported narrowing the list to those offences, while other delegations advocated for incorporating more offences.

Agreeing on a broader list of criminal offences seems “a priori” likely to present a number of difficulties and delays in the negotiation. On the other hand, it seems that many of the positions in favor of expanding the number of incorporated criminal offences were based on the need to count on tools to obtain digital evidence in the investigation of crimes. In this sense, a compromise solution could be that the section on “Procedural measures and law enforcement” and the section on “International cooperation” could be applied to other criminal offences, provided that this is possible as long as the States understand that it does not infringe their respective human rights norms or their public order. In other words, in case of international cooperation, it should be optional for a State, which receives a request for cooperation under this Convention regarding

offences which were not the subject of consensus, to determine whether such a request is appropriate, in the light of the aforementioned parameters.

As a guideline, without prejudice to the relevant regulations in every section relating to "Procedural measures and law enforcement" and the section relating to "International cooperation", the clause in relation with the scope of the Convention should read as drafted in point A. 3. of this document.

3. Participation and attempt.

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, under its domestic law, any form of participation, whether as an accomplice, assistant or instigator, in a criminal offence established in accordance with this Convention.

2. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, any attempt to commit a criminal offence established in accordance with this Convention.

3. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, the preparation for the commission of an offence established in accordance with this Convention.

4. **Liability of legal persons**.

1. Each State Party shall adopt such measures as may be necessary, in accordance with its legal principles, to establish the liability of legal persons for participation in criminal offences established in accordance with this Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are imposed effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

5. **Prosecution, adjudications and sanctions**.

1. Each State Party shall make the commission of the offences established in accordance with articles x of this Convention liable to sanctions that take into account the gravity of such offences.

2. Each State Party shall ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this Convention are exercised to maximize

the effectiveness of law enforcement measures in respect of such offences, with due regard to the need to prevent the commission of such offences.

3. In the case of offences established in accordance with articles x of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with a decision to grant release pending trial or appeal take into account the need to ensure the presence of the defendant at any subsequent criminal proceedings.

4. Each State Party shall ensure that its courts or other competent authorities bear in mind the serious nature of the offences covered by this Convention when considering the eventuality of granting early release or parole to persons convicted of such offences.

5. Each State Party shall, where appropriate, establish under its domestic law, a [reasonable/adequate/long] statute of limitations period in which to commence a proceeding for any of the offences covered by this Convention and a longer period where the alleged defendant has evaded the administration of justice.

6. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles underlying the legality of a conduct is reserved to the domestic law of the State Parties and that such offences are to be prosecuted and punished in accordance with that law.

6. **Criminalization of the laundering of proceeds of criminal offences listed in the Convention**.

1. Each State Party shall adopt, in accordance with the fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as an offence, when committed intentionally:

a) i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person involved in the commission of the predicate offence to evade the legal consequences of his or her action;

ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or of the legitimate rights in respect to property, knowing that such property is the proceeds of crime;

b) Subject to the basic concepts of its legal system:

i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

2. For purposes of implementing or applying paragraph 1 of this article:

a) Each State Party shall endeavor to apply paragraph 1 of this article to the offences established in this Convention

b) Each State Party shall include as predicate offences those criminal offences established in accordance with articles xx of this Convention

c) For the purposes of subparagraph b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party concerned. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences, provided that the relevant act is a criminal offence under the domestic law of the State where it was committed and would also constitute a criminal offence under the domestic law of the State Party implementing of applying this article if the offence had been committed there;

d) Each State Party shall provide the Secretary-General of the United Nations with a copy of its laws giving effect to this article and of any subsequent amendments made to such laws or a description thereof;

e) If so required by the fundamental principles of the domestic law of a State Party, it may be provided that the offences established in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

f) Knowledge, intent or purpose required as an element of an offence established in paragraph 1 of this article may be inferred from objective factual circumstances.

7. **Criminalization of obstruction of justice**.

Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, when committed intentionally:

a) The use of physical force, threats or intimidation, or the promise, the offering or giving of an undue benefit to induce false testimony or to interfere in the giving of testimony or the production of evidence in a proceeding in relation to the commission of offences covered by this Convention;

b) The use of physical force, threats or intimidation to interfere with the exercise of the official duties of a justice or law enforcement official in relation to the commission of offences covered by this Convention. Nothing in this subparagraph shall prejudice the right of the State Parties to have legislation that protects other categories of public officials.

8. **Jurisdiction**.

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with articles x of this Convention when:

a) The offence is committed in its territory; or

b) The offence is committed on board of a vessel flying its flag or an aircraft registered under its laws at the time of the commission of the offence.

2. Subject to the provisions of article x of this Convention, a State Party may also establish its jurisdiction over any such offence when:

a) The offence is committed against a national of that State Party;

b) The offence is committed by a national of that State Party or by a stateless person who has his or her habitual residence in its territory; or

c) The offence is:

i) One of those established by article xx of this Convention and is committed outside its territory with a view to the commission of an offence provided for in its territory.

ii) One of those established in accordance with article xx, paragraph 1 b) ii) *[on criminalization of laundering of proceeds of crime]* of this Convention and is committed outside its territory with a view to the commission, within its territory, of an offence established in accordance with article x, paragraph 1 a) i) or ii) or b) i) *[on criminalization of laundering of proceeds of crime]* of this Convention.

3. For purposes of paragraph 10 of article x *[extradition]* of this Convention, each State Party shall adopt such measures as may be necessary to establish its jurisdiction in relation to the offences covered by this Convention when the alleged offender is present in its territory and the State Party does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and the State Party does not extradite him or her.

5. If a State Party exercising its jurisdiction in accordance with paragraphs 1 or 2 of this article has been notified, or otherwise learned that one or more other State Parties are conducting an investigation, prosecution or legal proceeding in respect of the same facts, the competent authorities of those State Parties shall, as appropriate, consult one another with a view to coordinating their [measures].

6. Without prejudice to the norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by the State Parties in accordance with their domestic law.

C. PROCEDURAL MEASURES AND LAW ENFORCEMENT

1. **Scope and procedural provisions**.

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

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

a. the criminal offences established in accordance with [articles x to x] of this Convention;

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

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

2. **Conditions and safeguards**.

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall ensure adequate protection of human rights and freedoms, and in particular the rights derived from obligations assumed by each Party under the United Nations International Covenant on Civil and Political Rights (1966) or other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Where appropriate, having regard to the nature of the procedure or the power concerned, such conditions and safeguards shall include judicial or other independent supervision, the grounds justifying its application, as well as the limitation of the scope and duration of such power or procedure.

3. To the extent that it is consistent with the public interest and in particular with the sound administration of justice, each Party shall consider the impact of the powers and procedures in this [Section /Chapter] on the rights, responsibilities and [legitimate interest of third parties].

3. **Expedited preservation of stored computer data**.

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that such computer data is particularly vulnerable to loss or modification.

2. Where a Party implements the provisions of paragraph 1 above by ordering a person to retain certain stored data in the possession or under the control of that person, the Party shall take such legislative and other measures as may be necessary to compel that person to retain and protect the integrity of the data for as long as necessary, up to a [maximum of ninety days], to enable the competent authorities to obtain its disclosure. The Parties may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or such other person who is to preserve the computer data to keep confidential the undertaking of such procedures for a period of time as provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to the provisions of articles X and X *(equivalent to articles 14.1. , 14.2. and 15 of the Budapest Conv.).*

4. **Expedited preservation and disclosure of traffic data**.

1. In order to ensure the preservation of traffic data, in accordance with "article 16" (particular article number must be specified), each Party shall adopt such legislative and other measures as may be necessary to:

a. ensure the expeditious preservation of the traffic data, regardless of whether one or more service providers were involved in the transmission of such communication; and

b. ensure the expeditious disclosure to the Party´s competent authority, or to a person designated by that authority, of a sufficient amount of traffic data to enable such Party to identify both the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to the provisions of articles x and x (equivalent to articles 14.1, 14.2. and 15 of the Budapest Conv.)

5. **Production order**.

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its authorities to order:

a. a person in its territory to provide specified computer data in its possession or under its control, stored in a computer system or on a computer storage device; and

b. a service provider offering its services in the territory of that Party, to submit subscribers' information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to the provisions of articles x and x (equivalent to articles 14.1, 14.2. and 15 of the Budapest Conv.)

3. For the purpose of this article, "subscriber information" shall mean any information contained in the form of computer data or otherwise, held by a service provider, which relates to

subscribers of its services, other than traffic or content data and which makes it possible to determine:

a. the type of communication service used, the technical provisions adopted thereto and the period of service;

b. the subscriber's identity, postal address or geographical location, telephone number as well as any other access number and the billing and payment information available under a service agreement or arrangement.

c. any other information relating to the location of the communication equipment available under a service agreement or arrangement.

6. **Search and seizure of stored computer data**.

1. Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. any computer system or part of it, as well as the computer data stored therein; and

b. any computer-data storage device in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1. a), and have ground to believe that the data sought is stored in another computer system or part of it in its territory, and that such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed in application of paragraphs 1 or 2. Such measures shall include the following prerogatives:

a. to seize or similarly secure a computer system or part of it, or a computer-data storage device;

b. to make and retain a copy of such computer data;

c. to maintain the integrity of the relevant stored computer data; and

d. to render inaccessible or to delete such computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has the knowledge about the operation of a computer system or the measures implemented to protect the computer data therein to provide all information, as may reasonably be necessary, to enable the application of the measures provided for in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to the provisions of articles x and x (equivalent to articles 14.1, 14.2 and 15 of the Budapest Conv.)

7. **Real-time collection of traffic data**.

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. obtain or record with existing technical means on the territory of that Party, and

b. compel any service provider, within its existing technical capability:

i. to obtain or record with existing technical means on the territory of that Party, or

ii. to offer the competent authorities its cooperation and assistance in obtaining or recording, in real-time, traffic data associated with specific communications transmitted in its territory by means of a computer system.

2. Where a Party is unable to adopt the measures set forth in paragraph 1.a) by reason of compliance with the principles established in its domestic legal system, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specific communications transmitted in its territory through the application of technical means available in its territory.

3. Each Party shall adopt such legislative or other measures as may be necessary to compel a service provider to keep secret the fact that any of the powers provided for in this article have been exercised, as well as any information relating thereto.

4. The powers and procedures referred to in this article shall be subject to the provisions of articles x and x (equivalent to articles 14 and 15 of the Budapest Conv.)

8. **Interception of content data**.

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by its domestic law, to empower its competent authorities to:

a. obtain or record with existing technical means on the territory of that Party, and

b. compel any service provider, within its existing technical capability:

i. to obtain or record with existing technical means on the territory of that Party, or

ii. to offer the competent authorities its cooperation and assistance in obtaining or recording, in real-time, content data associated with specific communications transmitted in its territory by means of a computer system.

2. Where a Party is unable to adopt the measures set forth in paragraph 1.a) by reason of compliance with the principles established in its domestic legal system, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of content data associated with specific communications transmitted in its territory through the application of technical means available in its territory.

3. Each Party shall adopt such legislative or other measures as may be necessary to compel a service provider to keep secret the fact that any of the powers provided for in this article have been exercised, as well as any information relating thereto.

4. The powers and procedures referred to in this article shall be subject to the provisions of articles x and x (equivalent to articles 14.1, 14.2 and 15 of the Budapest Conv.)

9. **Confiscation and seizure**.

1. State Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

b) Property, equipment or other instrumentalities used or destined for use in the commission of offences covered by this Convention.

2. State Parties shall adopt such measures as may be necessary to enable the identification, localization, freezing or seizure of any item referred to in paragraph 1 of this article with a view to its eventual confiscation.

3. Where the proceeds of crime have been transformed or converted, in part or in full, into other property, such property, instead of the proceeds, may be liable to the measures referred to in this article.

4. Where the proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, notwithstanding any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

5. Income or other benefits derived from the proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

6. For the purposes of this article [and article 13 UNDOT of this] Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. State Parties may not refuse to apply the provisions of this article on the ground of bank secrecy.

7. State Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such requirement is consistent with the principles of their domestic law and with the nature of the judicial or other [related] proceedings.

8. The provisions of this article shall not be construed to prejudice the rights of bona fide third parties.

9. Nothing contained in this article shall affect the principle that the measures provided for therein shall be defined and implemented in accordance with and subject to the provisions of the domestic law of the State Parties.

10. **Disposal of confiscated proceeds of crime or property**.

1. State Parties shall dispose of proceeds of crime or of property confiscated pursuant to article x or paragraph 1 of article x of this Convention *(corresponding to articles 12 and 13 of UNDOT, respectively)* in accordance with their domestic law and administrative procedures.

2. When executing a request submitted by another State Party in accordance with article x of this Convention *(article 13 UNDOT)*, State Parties shall, to the extent permitted by their domestic law and if so requested, give priority consideration to returning proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of crime or return such proceeds of crime or property to their legitimate owners.

3. When executing a request submitted by another State Party pursuant to articles x and x of this Convention *(articles 12 and 13 UNDOT)*, State Parties may give special consideration to celebrating agreements or arrangements on:

a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with the provisions of article x, paragraph 2, subparagraph c) of this Convention *(article 30 UNDOT)* and to intergovernmental bodies specializing in the fight against organized crime;

b) Sharing with other State Parties, on a general or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with their domestic law or administrative procedures.

11. **Establishment of criminal record**.

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction, in another State, of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence covered by this Convention.

12. **Protection of witnesses**.

1. Each State Party shall adopt appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings who give testimony concerning offences covered by this Convention, and, as appropriate, for their relatives and other persons close to them.

2. The provisions of this article shall also apply to victims in the event that they act as witnesses.

13. **Assistance to and protection of victims**.

1. Each State Party shall adopt appropriate measures within its means to provide assistance and protection to victims of offences covered by this Convention, in particular in cases of threat of retaliation or intimidation.

2. Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of the offences covered by this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders without prejudice to the rights of the defence.