

SEVENTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
Second Regular Session)

SENATE

COMMITTEE REPORT NO. 238

18 FEB -7 11:03

Submitted by the Committee on Foreign Relations on FEB - 7 2018.

Re: P.S. Res. No. 616, prepared by the Committee

RECORDED

Recommending its approval without amendment.

Sponsor: Sen. Loren Legarda

MR. PRESIDENT:

The Committee on Foreign Relations, to which was referred the Agreement, entitled:

CONVENTION ON CYBERCRIME

has considered the same and has the honor to report it back to the Senate with the recommendation that Proposed Senate Resolution No. 616, prepared by the Committee, entitled:

**RESOLUTION
CONCURRING IN THE ACCESSION TO THE
CONVENTION ON CYBERCRIME**

be approved without amendment.

Respectfully submitted:




LOREN LEGARDA

Chair

Committee on Foreign Relations

Vice Chairs:


EMMANUEL "MANNY" D. PACQUIAO


JOEL VILLANUEVA


CYNTHIA A. VILLAR


Members:


SONNY ANGAÑA


GREGORIO B. HONASAN


RICHARD J. GORDON


JOSEPH VICTOR G. EJERCITO


JUAN MIGUEL F. ZUBIRI


MARIA LOURDES NANCY S. BINAY

FRANCIS G. ESCUDERO

ANTONIO "SONNY" F. TRILLANES IV

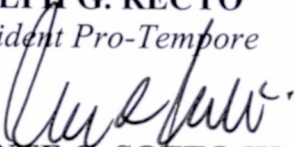
FRANCIS N. PANGILINAN


RISA HONTIVEROS

PAOLO BENIGNO "BAM" AQUINO IV

Ex-Officio Members:

RALPH G. RECTO
President Pro-Tempore


VICENTE C. SOTTO III
Majority Leader


FRANKLIN M. DRILON
Minority Leader

AQUILINO "KOKO" PIMENTEL III

President
Senate of the Philippines

SEVENTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
Second Regular Session)

SENATE

P.S. RES. NO. 616

OFFICE OF THE CLERK
SENATE
ROOM 1000, MALACANANG

REC-1000 FEB -7 AM-03

Prepared by the Committee on Foreign Relations

RECEIVED



RESOLUTION
CONCURRING IN THE ACCESSION TO THE
CONVENTION ON CYBERCRIME

WHEREAS, the Constitution, Article 7, Section 21, states: "No treaty or international agreement shall be valid and effective unless concurred in by at least two-thirds of all the members of the Senate";

WHEREAS, the *Convention on Cybercrime* (Convention) was signed on 23 November 2001 in Budapest, Hungary;

WHEREAS, to date, the Convention on Cybercrime remains the sole binding international legal mechanism adopted by countries to address the threats posed by cybercrime;

WHEREAS, the Convention takes into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe Member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective, as well as to enable the more efficient collection of evidence in electronic form of a criminal offense;

WHEREAS, Article 37 (2) of Chapter IV of the Convention provides that, "In respect of any State acceding to the Convention under paragraph 1, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe;

WHEREAS, the President of the Philippines ratified the Agreement on 9 December 2016 and submitted it to the Senate for concurrence, in accordance with the Constitution;

WHEREAS, in the hearing conducted by the Senate Committee on Foreign Relations on 6 February 2018, the following government agencies endorsed the concurrence to the accession of the Convention:

1. Department of Foreign Affairs

2. Department of Justice
3. Department of Information and Communication Technology
4. National Bureau of Investigation
5. Philippine National Police

WHEREFORE, BE IT HEREBY RESOLVED, that the Philippine Senate concur, as it hereby concurs, in the Philippine accession to the Convention on Cybercrime.

Adopted,



LOREN LEGARDA

Chair

Committee on Foreign Relations

0577102845 11/1

DB#29959/05

Office of the President
of the Philippines
Malacañang

OFFICE OF THE SENATE PRESIDENT	
AQUILINO "KOKO" PIMENTEL III	
TEL.NO: 5526601 loc.5548 FAX: 5526813	
Date: <u>DEC 12, 2016</u>	Time: <u>3:22</u>
Received by: <u>KIM</u>	

09 December 2016

Senator AQUILINO PIMENTEL III
Senate President
Senate of the Philippines
Pasay City

Sir:

May we respectfully transmit the herein attached letter to the Senate President signed by President Rodrigo Roa Duterte, submitting the Instrument of Accession to the "Convention on Cybercrime" for the Senate's consideration and concurrence.

For your information and appropriate action.

Very truly yours,



SALVADOR C. MEDIALDEA
Executive Secretary

Encl.: a/s

cc.: Office of Legal Affairs
Department of Foreign Affairs
Pasay City

GGAO/RE1636825/RE1641073
MPO/LD/AMG/jddt





MALACAÑAN PALACE
MANILA

09 December 2016

The Honorable Senate President
and Members of the Senate
Senate of the Philippines
Pasay City

Gentlemen and Ladies of the Senate:

I have the honor to submit, for the Senate's consideration, the *Convention on Cybercrime* which was signed on 23 November 2001 in Budapest, Hungary.

The Convention takes into account the existing Council of Europe conventions on cooperation in the penal field, as well as similar treaties which exist between the Council of Europe Member-States and other States. It is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offenses related to computer systems and data more effective, as well as to facilitate the more efficient collection of evidence in electronic form.

The Department of Justice, the Department of Information and Communications Technology and the Department of the Interior and Local Government have been consulted and have concurred with the proposed accession.

After examining the text thereof, I find it advisable to accede to the *Convention on Cybercrime* and seek the Senate's concurrence thereto.


RODRIGO ROA DUTERTE



THE PRESIDENT OF THE PHILIPPINES

MALACAÑANG
MANILA

INSTRUMENT OF ACCESSION

TO WHOM THESE PRESENTS SHALL COME, GREETINGS:

KNOW YE, that whereas, the *Convention on Cybercrime* was signed on 23 November 2001 at Budapest, Hungary;

WHEREAS, the Convention takes into account the existing Council of Europe conventions on cooperation in the penal field, as well as similar treaties which exist between the Council of Europe Member States and other States, and is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offenses related to computer systems and data more effective, as well as to enable the more efficient collection of evidence in electronic form;

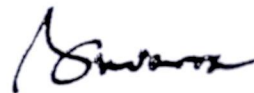
NOW, THEREFORE, be it known that I, RODRIGO ROA DUTERTE, President of the Republic of the Philippines, after having seen and considered the *Convention on Cybercrime*, do hereby accede and confirm the same and each and every article and clause thereof.

IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the seal of the Republic of the Philippines to be affixed.

GIVEN under my hand at the City of Manila, this 9th day of December in the year of Our Lord two thousand and sixteen.



By the President:


for - SALVADOR C. MEDIALDEA
Executive Secretary



CERTIFICATION

I **HEREBY CERTIFY** that the attached documents are true and correct copies of the official text of the *Budapest Convention on Cybercrime*.

IN WITNESS WHEREOF, I, LINGLINGAY F. LACANLALE, Acting Secretary of Foreign Affairs, have caused the seal of the Department of Foreign Affairs to be affixed and my name subscribed to before the Acting Assistant Secretary for Legal Affairs of the Department, in Pasay City this ___ day of _____ 2016.


LINGLINGAY F. LACANLALE
Acting Secretary of Foreign Affairs

SUBSCRIBED AND SWORN to before me this ___ day of _____ 2016 by the Honorable **LINGLINGAY F. LACANLALE**, Acting Secretary of Foreign Affairs.


LEO TITO L. AUSAN, JR.
Acting Assistant Secretary



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

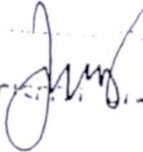
European Treaty Series - No. 185

CONVENTION
ON CYBERCRIME

Budapest, 23.XI.2001

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2011


DAMIANOS KIKELI

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

DEPARTMENT OF FOREIGN AFFAIRS
Information Technology Communications
Division

09 FEB 2011

FOR THE DIRECTOR
FRANCISCA ALBA

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2017

FOR THE DIRECTOR OF ITC&C:

FRANCIS COLLAZAO

Chapter I – Use of terms

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.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

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.

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.

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2017

FOR THE DIRECTOR OF THE DIVISION

FRANCISCO L. ALBA()

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.

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.

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 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.

CERTIFIED TRUE COPY
 DEPARTMENT OF FOREIGN AFFAIRS
 Information Technology, Communications
 Division

09 FEB 2017

FOR THE DIRECTOR OF ITCSD:

FRANCISCO L. ALBAO

*Title 2 – Computer-related offences***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.

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.

*Title 3 – Content-related offences***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;

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2017

FOR THE DIRECTOR OF AFD:

FRANCISCO L. ALBAO

- 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.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – 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 under its domestic law the infringement of copyright, as defined under the law 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 such conventions, where such acts are committed wilfully, 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 under its domestic law the infringement of related rights, as defined under the law 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 Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
- 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

- 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, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
- 2 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, an attempt to commit any of the offences established in accordance with Articles 2 through 5, 7, 8, and 9.1.a and c. of this Convention.

ARTICLES 7 THROUGH
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology Communications
Division

09 FEB 2017

FOR THE DIRECTOR GENERAL

FRANCISCOL AIRAC

- 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 - Corporate liability

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
- a a power of representation of the legal person;
 - b an authority to take decisions on behalf of the legal person;
 - c an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 - Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 - Procedural law

Title 1 - Common provisions

Article 14 - Scope of procedural provisions

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

ESTRADO ISSUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology Communication
Division

09 FEB 2017

FOR THE SECRETARY OF DEFENCE
FRANCIS (JOE) STRAIN

- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
 - b other criminal offences committed by means of a computer system; and
 - c the collection of evidence in electronic form of a criminal offence.
- 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
- b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
- i is being operated for the benefit of a closed group of users, and
 - ii does not employ public communications networks and is not connected with another computer system, whether public or private,
- that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
- 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
and Security Division

09 FEB 2017

FOR THE DIRECTOR GENERAL

FRANCISCOLI AIRAO

*Title 2 – Expedited preservation of stored computer data***Article 16 – Expedited preservation of stored computer data**

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

Article 17 – Expedited preservation and partial disclosure of traffic data

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
- a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
 - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

*Title 3 – Production order***Article 18 – Production order**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
- a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology Communications
Division

09 FEB 2017

FOR THE SECRETARY

FRANCISOL AIRAO

- b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
- a the type of communication service used, the technical provisions taken thereto and the period of service;
- b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
- a a computer system or part of it and computer data stored therein; and
- b a computer-data storage medium in which computer data may be stored in its territory.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
- b make and retain a copy of those computer data;

CERTIFIED TRUE COPY
 DEPARTMENT OF FOREIGN AFFAIRS
 Information Technology & Communications
 Division

09 FEB 2017

FOR THE DIRECTOR GENERAL:

FRANCISCO AIRAOL

- c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

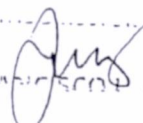
- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
- a collect or record through the application of technical means on the territory of that Party, and
 - b compel a service provider, within its existing technical capability:
 -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

Article 21 – Interception of content data

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

LAW TO EMPOWER COMPETENT
 DEPARTMENT OF FOREIGN AFFAIRS
 Information Technology, Communications
 Division

09 FEB 2017

FOR THE DIRECTOR

 COORDINATOR AIRAC

- a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party, or
 - ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - a in its territory; or
 - b on board a ship flying the flag of that Party; or
 - c on board an aircraft registered under the laws of that Party; or
 - d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
- 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2017

FOR THE DIRECTOR OF TRADE:

SPANICSO L. AURAO

- 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
- 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

- 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
- b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
- 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
- 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
Division

09 FEB 2017

FOR THE SECRETARY OF STATE

CRIMINAL AIRAC

Article 44 - Amendments

- 1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
- 2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
- 3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
- 4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
- 5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 - Settlement of disputes

- 1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
- 2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 - Consultations of the Parties

The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

- 2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

CERTIFIED TRUE COPY
 DEPARTMENT OF FOREIGN AFFAIRS
 International Technology Crime Center
 # Division

09 FEB 2017 a

FOR INFORMATION RECORD:

MANUSCO L AIRAO

- 3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
- 4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
- 5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

- 1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
- 2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d any declaration made under Article 40 or reservation made in accordance with Article 42;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

CERTIFIED TRUE COPY
DEPARTMENT OF FOREIGN AFFAIRS
Information Technology, Communications
and Security Division

09 FEB 2017

FOR THE DIRECTOR OF ICED:

FOR THE SECRETARY GENERAL: