Philippines

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 25 March 2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	
Ratification/accession:	28/03/2018

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": 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	**R.A. No. 10175** SEC. 3. Definition of Terms. For purposes of this Act, the following terms are hereby defined as follows: (a) Access refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network. (b) Alteration refers to the modification or change, in form or substance, of an existing computer data or program. (c) Communication refers to the transmission of information through ICT media, including voice, video and other forms of data. (d) Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet. (e) Computer data refers to 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 and includes electronic documents and/or electronic data messages whether stored in local computer systems or online. (f) Computer program refers to a set of instructions executed by the computer to achieve intended results. (g) Computer system refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media. (h) Without right refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law. (i) Cyber refers to a computer or a computer network, the electronic medium in which online communication takes place. (j) Critical infrastructure refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	security, national or economic security, national public health and safety, or any combination of those matters. (k) Cybersecurity refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (l) Database refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system. (m) Interception refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring. (n) Service provider refers to: (1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service. (o) Subscriber's information refers to 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 identity can be established: (1) The type of communication service used, the technical provisions taken thereto and the period of service;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	(2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and (3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. (p) Traffic data or non-content data refers to any computer data other than the content of the communication including, but not limited to, 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.	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: (a) Offenses against the confidentiality, integrity and availability of computer data and systems: (1) Illegal Access. – The access to the whole or any part of a computer system without right.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: (a) Offenses against the confidentiality, integrity and availability of computer data and systems: […] (2) Illegal Interception. – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.
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.	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: (a) Offenses against the confidentiality, integrity and availability of computer data and systems: […] (3) Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: (a) Offenses against the confidentiality, integrity and availability of computer data and systems: […] (4) System Interference. — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.
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,	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses.** The following acts constitute the offense of cybercrime punishable under this Act: (a) Offenses against the confidentiality, integrity and availability of computer data and systems: […] (5)Misuse of Devices. (i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or (bb) 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 offenses under this Act. (ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.
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.	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: […] (b) Computer-related Offenses: (1) Computer-related Forgery. — (i) The input, alteration, or deletion of any computer data without right 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; or (ii) The act of knowingly using computer data which is the product of computer-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.
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.	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses.** The following acts constitute the offense of cybercrime punishable under this Act: […] (b) Computer-related Offenses: […] (2) Computer-related Fraud. — The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.
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;	**R.A. No. 10175** **SEC. 4. Cybercrime Offenses** The following acts constitute the offense of cybercrime punishable under this Act: […] (c) Content-related Offenses: […] (2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	**R.A. No. 9775** Section 3. Definition of Terms. (b) "Child pornography" refers to any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities
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	**R.A. No. 8293** CHAPTER XVII INFRINGEMENT Section 216. Remedies for Infringement. - 216.1. Any person infringing a right protected under this law shall be liable: (a) To an injunction restraining such infringement. The court may also order the defendant to desist from an infringement, among others, to prevent the entry into the channels of commerce of imported goods that involve an infringement,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	immediately after customs clearance of such goods. (b) Pay to the copyright proprietor or his assigns or heirs such actual damages, including legal costs and other expenses, as he may have incurred due to the infringement as well as the profits the infringer may have made due to such infringement, and in proving profits the plaintiff shall be required to prove sales only and the defendant shall be required to prove every element of cost which he claims, or, in lieu of actual damages and profits, such damages which to the court shall appear to be just and shall not be regarded as penalty. (c) Deliver under oath, for impounding during the pendency of the action, upon such terms and conditions as the court may prescribe, sales invoices and other documents evidencing sales, all articles and their packaging alleged to infringe a copyright and implements for making them. (d) Deliver under oath for destruction without any compensation all infringing copies or devices, as well as all plates, molds, or other means for making such infringing copies as the court may order. (e) Such other terms and conditions, including the payment of moral and exemplary damages, which the court may deem proper, wise and equitable and the destruction of infringing copies of the work even in the event of acquittal in a criminal case. 216.2. In an infringement action, the court shall also have the power to order the seizure and impounding of any article which may serve as evidence in the court proceedings. (Sec. 28, P.D. No. 49a) Section 217. Criminal Penalties. - 217.1. Any person infringing any right secured by provisions of Part IV of this Act or aiding or abetting such infringement shall

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	be guilty of a crime punishable by: (a) Imprisonment of one (1) year to three (3) years plus a fine ranging from Fifty thousand pesos (P50,000) to One hundred fifty thousand pesos (P150,000) for the first offense. (b) Imprisonment of three (3) years and one (1) day to six (6) years plus a fine ranging from One hundred fifty thousand pesos (P150,000) to Five hundred thousand pesos (P500,000) for the second offense. (c) Imprisonment of six (6) years and one (1) day to nine (9) years plus a fine ranging from five hundred thousand pesos (P500,000) to One million five hundred thousand pesos (P1,500,000) for the third and subsequent offenses. (d) In all cases, subsidiary imprisonment in cases of insolvency. 217.2. In determining the number of years of imprisonment and the amount of fine, the court shall consider the value of the infringing materials that the defendant has produced or manufactured and the damage that the copyright owner has suffered by reason of the infringement. 217.3. Any person who at the time when copyright subsists in a work has in his possession an article which he knows, or ought to know, to be an infringing copy of the work for the purpose of: (a) Selling, letting for hire, or by way of trade offering or exposing for sale, or hire, the article; (b) Distributing the article for purpose of trade, or for any other purpose to an extent that will prejudice the rights of the copyright owner in the work; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	(c) Trade exhibit of the article in public, shall be guilty of an offense and shall be liable on conviction to imprisonment and fine as above mentioned. (Sec. 29, P.D. No. 49a)
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 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**R.A. No. 10175** **SEC. 5. Other Offenses** The following acts shall also constitute an offense: (a) Aiding or Abetting in the Commission of Cybercrime. – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable. (b) Attempt in the Commission of Cybercrime. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.
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	**R.A. No. 10175** **SEC. 9. Corporate Liability** When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: Provided, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00). If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00). The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.
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.	**R.A. No. 10175** **SEC. 6.** All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be. **SEC. 8. Penalties** Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of prison mayor or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both. Any person found guilty of the punishable act under Section 4(a)(5) shall be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	punished with imprisonment of prison mayor or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both. If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of reclusion temporal or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed. Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of prison mayor or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both. Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system. Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of arrest mayor or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both. Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and 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	**R.A. No. 10175** **SEC. 10. Law Enforcement Authorities** The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act. **SEC. 11. Duties of Law Enforcement Authorities** To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	**The Constitution of the Republic of the Philippines** **ARTICLE III** **Bill of Rights** SECTION 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws. SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized. SECTION 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law. (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding. SECTION 4. No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances. SECTION 5. No law shall be made respecting an establishment of religion, or prohibiting the free exercise thereof. The free exercise and enjoyment of religious profession and worship, without discrimination or preference, shall forever be allowed. No religious test shall be required for the exercise of civil or political rights. […]
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	**R.A. No. 10175** **SEC. 13. Preservation of Computer Data.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation. Law enforcement authorities may order a one-time extension for another six (6) months: Provided, that once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case. The service provider ordered to preserve computer data shall keep confidential the order and its compliance.
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	**R.A. No. 10175** **SEC. 14. Disclosure of Computer Data** Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation. *See Section 25 of the Rules and Regulations Implementing Republic Act No.*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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.	*10175, Otherwise Known as the "Cybercrime Prevention Act of 2012" below.* **Section 4, Rule on Cybercrime Warrants (A.M. No. 17-11-03-SC)** **Section 4. *Disclosure of Computer Data*[1]** **Section 4.1. *Disclosure of Computer Data.*** — Pursuant to Section 14, Chapter IV of RA 10175, law enforcement authorities, upon securing a Warrant to Disclose Computer Data (WDCD) under this Rule, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/her or its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation. **Section 4.2. *Warrant to Disclose Computer Data (WDCD).*** — A WDCD is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to issue an order to disclose and accordingly, require any person or service provider to disclose or submit subscriber's information, traffic data, or relevant data in his/her or its possession or control. **Section 4.3. *Contents of Application for a WDCD.*** — The verified application for a WDCD, as well as the supporting affidavits, shall state the following essential facts: 1. The probable offense involved; 2. Relevance and necessity of the computer data or subscriber's information sought to be disclosed for the purpose of the

[1] RA 10175, Chapter IV, Section 14.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	investigation; 3. Names of the individuals or entities whose computer data or subscriber's information are sought to be disclosed, including the names of the individuals or entities who have control, possession or access thereto, if available; 4. Particular description of the computer data or subscriber's information sought to be disclosed;[2] 5. Place where the disclosure of computer data or subscriber's information is to be enforced, if available; 6. Manner or method by which the disclosure of the computer data or subscriber's information is to be carried out, if available;[3] and 7. Other relevant information that will persuade the court that there is a probable cause to issue a WDCD. **Section 4.4.** ***Issuance and Form of WDCD.*** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WDCD exists, he/she shall issue the WDCD, which must be substantially in the form prescribed in "Annex A" of this Rule. **Section 4.5.** ***Return on the WDCD; Retained Copy.*** — Within forty-eight (48) hours from implementation or after the expiration of the effectivity of the WDCD, whichever comes first, the authorized law enforcement officer shall

[2] Ephemeral data: phone calls, short messaging service (SMS), social media internet relay chat (IRC); e-mail or the content data.

[3] E.g., by hard copies or soft copies, by photograph or video, mirror imaging or bit streaming. Bit streaming – refers to making a clone copy of a computer drive. It copies virtually everything included in the drive, including sectors and clusters, which makes it possible to retrieve files that were deleted from the drive. Bit stream images are usually used when conducting digital forensic investigations in a bid to avoid tampering with digital evidence such that it is not lost or corrupted (See http://www.igi-global.com/book/handbook-research-digital-crime-cyberspace/104750), image capture, etc.) [Visited June 3, 2018].

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	submit a return on the WDCD to the court that issued it and simultaneously turn over the custody of the disclosed computer data or subscriber's information thereto as provided under Section 7.1[4] of this Rule. It is the duty of the issuing judge to ascertain if the return has been made, and if none, to summon the law enforcement officer to whom the WDCD was issued

[4] **Section 7.1.** ***Deposit and Custody of Seized Computer Data***.[4] — Upon the filing of the return for a WDCD or WICD, or the final return for a WSSECD or WECD, all computer data subject thereof shall be simultaneously deposited in a sealed package with the same court that issued the warrant. It shall be accompanied by a complete and verified inventory of all the other items seized in relation thereto, and by the affidavit of the duly authorized law enforcement officer containing:

1. The date and time of the disclosure, interception, search, seizure, and/or examination of the computer data, as the case may be. If the examiner or analyst has recorded his/her examination, the recording shall also be deposited with the court in a sealed package and stated in the affidavit;

2. The particulars of the subject computer data, including its hash value;

3. The manner by which the computer data was obtained;

4. Detailed identification of all items seized in relation to the subject computer data, including the computer device containing such data and/or other parts of the computer system seized, indicating the name, make, brand, serial numbers, or any other mode of identification, if available;

5. The names and positions of the law enforcement authorities who had access to the computer data from the time of its seizure until the termination of the examination but prior to depositing it with the court,[4] and the names of officers who will be delivering the seized items to the court;[4]

6. The name of the law enforcement officer who may be allowed access to the deposited data. When the said officer dies, resigns of severs tie with the office, his/her successor may, upon motion, be granted access to the deposit; and

7. A certification that no duplicates or copies of the whole or any part thereof have been made, or if made, all such duplicates or copies are included in the sealed package deposited, except for the copy retained by law enforcement authorities pursuant to paragraph 3 of Section 4.5 of this Rule.

The return on the warrant shall be filed and kept by the custodian of the log book on search warrants who shall enter therein the date of the return, the description of the sealed package deposited, the name of the affiant, and other actions of the judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	and require him to explain why no return was made, without prejudice to any action for contempt as provided under Section 2.6[5] of this Rule. Law enforcement authorities are allowed to retain a copy of the disclosed computer data or subscriber's information subject of the WDCD which may be utilized for case build-up or preliminary investigation purposes, without the need of any court intervention; *Provided,* that the details thereof are kept strictly confidential and that the retained copy shall be labelled as such. The retained copy shall be turned over upon the filing of a criminal action involving the disclosed computer data or subscriber's information to the court where such action has been instituted, or if no criminal action has been filed, upon order of the issuing court under the procedure set forth in paragraph 3 of Section 8.2[6] of this Rule. Upon its turn-over, the retained copy shall always be kept, destroyed, and/or returned together with the computer data or subscriber's information that was originally turned over to the issuing court under the first paragraph of this

[5] **Section 2.6.** ***Contempt*****.** – Failure to timely file the returns for any of the issued warrants under this Rule or to duly turn-over to the court's custody any of the items disclosed, intercepted, searched, seized, and/or examined as prescribed hereunder, shall subject the responsible law enforcement authorities to an action for contempt, which procedures shall be governed by Rule 71 of the Rules of Civil Procedure, insofar as they are applicable.

[6] **Section 8.2.** ***Destruction and Return of Computer Data in the Custody of the Court.*** — Upon motion and due hearing, the court may, for justifiable reasons, order the complete or partial destruction, or the return to its lawful owner or possessor, of the computer data or any of the related items turned over to its custody.

Likewise, the court may, *motu proprio,* and upon written notice to all the parties concerned, order the complete or partial destruction, or return to its lawful owner or possessor, of the computer data or any of the related items turned over to its custody if no preliminary investigation or case[6] involving these items has been instituted after thirty-one (31) days from their deposit, or if preliminary investigation has been so instituted within this period, upon finality of the prosecutor's resolution finding lack of probable cause. In its sound discretion, the court may conduct a clarificatory hearing to further determine if there is no reasonable opposition to the items' destruction or return.

If the court finds the destruction or return of disclosed computer data or subscriber's information subject of a WDCD to be justified under this Section, it shall first issue an order directing the law enforcement authorities to turn-over the retained copy thereof as described in paragraph 3 of Section 4.5 of this Rule. Upon its turn-over, the retained copy shall be simultaneously destroyed or returned to its lawful owner or possessor together with the computer data or subscriber's information that was originally turned over to the issuing court.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	Section. **Section 4.6. *Contempt.*** — Non-compliance with the order to disclose issued by law enforcement authorities shall be deemed non-compliance with the WDCD on which the said order is based, and shall likewise give rise to an action for contempt under Section 2.6 of this Rule.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**R.A. No. 10175** **SEC. 14. Disclosure of Computer Data** Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation. Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012" Section 28. *Department of Justice (DOJ); Functions and Duties.* The DOJ-Office of Cybercrime (OOC), designated as the central authority in all matters related to international mutual assistance and extradition, and the Cybercrime Operations Center of the CICC, shall have the following functions and duties: a. Act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	b. Act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the Act; c. Issue preservation orders addressed to service providers; d. Administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime; e. Require the submission of timely and regular reports including pre-operation, post-operation and investigation results, and such other documents from the PNP and NBI for monitoring and review; f. Monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof; g. Facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution; h. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices; i. Prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination: j. Undertake the specific roles and responsibilities of the DOJ related to cybercrime under the Implementing Rules and Regulation of Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009"; and k. Perform such other acts necessary for the implementation of the Act. *See Section 25 of the Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012" below.*
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:	**R.A. No. 10175** **SEC. 15. Search, Seizure and Examination of Computer Data.** Where a search and seizure warrant is properly issued, the law enforcement

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	authorities shall likewise have the following powers and duties. Within the time period specified in the warrant, to conduct interception, as defined in this Act, and: (a) To secure a computer system or a computer data storage medium; (b) To make and retain a copy of those computer data secured; (c) To maintain the integrity of the relevant stored computer data (d) To conduct forensic analysis or examination of the computer data storage medium; and (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network. Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination. Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court. **Sections 6, Rule on Cybercrime Warrants (A.M. No. 17-11-03-SC)** **Section 6*. Search, Seizure and Examination of Computer Data*[7]** **Section 6.1. *Warrant to Search, Seize and Examine Computer Data (WSSECD)*.** — A Warrant to Search, Seize and Examine Computer Data

[7] RA 10175, Chapter IV, Section 15.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	(WSSECD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to search the particular place for items to be seized and/or examined. **Section 6.2. *Contents of Application for a WSSECD*.** — The verified application for a WSSECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be searched, seized, and examined, and all other items related thereto. In addition, the application shall contain an explanation of the search and seizure strategy to be implemented, including a projection of whether or not an off-site or on-site search will be conducted, taking into account the nature of the computer data involved, the computer or computer system's security features, and/or other relevant circumstances, if such information is available. **Section 6.3. *Issuance and Form of WSSECD.*** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WSSECD exists, he shall issue the WSSECD, which must be substantially in the form prescribed under "Annex C" of this Rule. **Section 6.4. *Off-site and On-site Principle; Return of Items Seized Off-site.*** —Law enforcement authorities shall, if the circumstances so allow, endeavor to first make a forensic image of the computer data on-site as well as limit their search to the place specified in the warrant. Otherwise, an off-site search may be conducted, provided that a forensic image is, nevertheless, made, and that the reasons for the said search are stated in the initial return. A person whose computer devices or computer system have been searched and seized off-site may, upon motion, seek the return of the said items from the court issuing the WSSECD: *Provided*, that a forensic image of the computer data subject of the WSSECD has already been made. The court may grant the motion upon its determination that no lawful ground exists to otherwise withhold the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	return of such items to him. **Section 6.5.** ***Allowable Activities During the Implementation of the WSSECD*****.** – Pursuant to Section 15, Chapter IV of RA 10175, the interception of communications and computer data may be conducted during the implementation of the WSSECD: *Provided*, that the interception activities shall only be limited to communications and computer data that are reasonably related to the subject matter of the WSSECD; and that the said activities are fully disclosed, and the foregoing relation duly explained in the initial return. Likewise, law enforcement authorities may order any person, who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the search, seizure and examination.[8] **Section 6.6.** ***Initial Return.*** — Within ten (10) days from the issuance of the WSSECD, the authorized law enforcement officers shall submit an initial return that contains the following information: 1. A list of all the items that were seized, with a detailed identification of: (a) the devices of the computer system seized, including the name, make, brand, serial numbers, or any other mode of identification, if available; and (b) the hash value of the computer data and/or the seized computer device or computer system containing such data; 2. A statement on whether a forensic image of the computer data was made on-site, and if not, the reasons for making the forensic image off-site; 3. A statement on whether the search was conducted on-site, and

[8] RA 10175, Chapter IV, Section 15.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	if not, the reasons for conducting the search and seizure off-site; 4. A statement on whether interception was conducted during the implementation of the WSSECD, together with (a) a detailed identification of all the interception activities that were conducted; (b) the hash value/s of the communications or computer data intercepted; and (c) an explanation of the said items' reasonable relation to the computer data subject of the WSSECD; 5. List of all the actions taken to enforce the WSSECD, from the time the law enforcement officers reached the place to be seized until they left the premises with the seized items and reached the place where the items seized were stored and secured for examination; and 6. A reasonable estimation of how long the examination of the items seized will be concluded and the justification therefor. It is the duty of the issuing judge to ascertain if the initial return has been made, and if none, to summon the law enforcement authority to whom the WSSECD was issued and require him to explain why no initial return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule. **Section 6.7.** ***Period to Examine and Order to Return.*** **–** After the initial return is submitted to the court pursuant to the WSSECD, the court shall issue an order fixing the period to conclude the examination of all the items seized, which period may be extended not exceeding thirty (30) days, upon motion, for justifiable reasons. **Section 6.8.** ***Final Return on the WSSECD.*** — Within forty-eight (48) hours after the expiration of the period to examine as provided under Section 6.7 of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	this Rule, the authorized law enforcement officers shall submit a final return on the WSSECD to the court that issued it, and simultaneously turn-over the custody of the seized computer data, as well as all other items seized and/or the communications or computer data intercepted in relation thereto, following the procedure under Section 7.1 of this Rule. It is the duty of the issuing judge to ascertain if the final return has been made, and if none, to summon the law enforcement officer to whom the WSSECD was issued and require him to explain why no final return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule. **Section 6.9. *Examination where lawful possession of device is obtained; Warrant to Examine Computer Data (WECD).*** – Upon acquiring possession of a computer device or computer system via a lawful warrantless arrest, or by any other lawful method,[9] law enforcement authorities shall first apply for a warrant before searching the said computer device or computer system for the purpose of obtaining for forensic examination the computer data contained therein. The warrant therefor shall be denominated as a Warrant to Examine Computer Data (WECD). The verified application for a WECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be examined. In addition, the application shall disclose the circumstances surrounding the lawful acquisition of the computer device or computer system containing the said computer data. If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WECD exists, he shall issue the WECD, which must be substantially in the form prescribed under "Annex D" of this Rule. The initial and final returns, as well as the period to examine under a WECD, shall be similarly governed by the procedures set forth in Sections 6.6 to 6.8 of

[9] Valid warrantless seizure, *en flagrante delicto*, or by voluntary surrender of the unit.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	this Rule. Interception of communications and computer data may be likewise conducted during the implementation of the WECD under the same conditions stated in Section 6.5 of this Rule.
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.	**Section 5, Rule on Cybercrime Warrants (A.M. No. 17-11-03-SC)** **Section 5*. Interception of Computer Data*[10]** **Section 5.1. *Interception of Computer Data.*** — Interception, as defined under Section 3 (m), Chapter I of RA 10175, may be carried out only by virtue of a court issued warrant, duly applied for by law enforcement authorities. **Section 5.2. *Warrant to Intercept Computer Data (WICD).*** — A WICD is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to carry out any or all of the following activities: (a) listening to, (b) recording, (c) monitoring, or (d) surveillance of the content of communications, including procuring of the content of computer data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring. **Section 5.3. *Contents of Application for WICD.*** — The verified application for a WICD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the communication or computer data sought to be intercepted. **Section 5.4. *Issuance and Form of WICD.*** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for

[10] RA 10175, Chapter IV, Section 15.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	WICD exists, he shall issue the WICD, which must be substantially in the form prescribed in "Annex B" of this Rule. **Section 5.5.** ***Return on the WICD.*** — Within forty-eight (48) hours from implementation or after the expiration of the effectivity of the WICD, whichever comes first, the authorized law enforcement officers shall submit a return on the WICD to the court that issued it and simultaneously turn-over the custody of the intercepted communication or computer data thereto as provided under Section 7.1 of this Rule. It is the duty of the issuing judge to ascertain if the return has been made, and if none, to summon the law enforcement officer to whom the WICD was issued and require him to explain why no return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule. **Section 5.6.** ***Notice after filing of Return.*** – Within thirty (30) days from the filing of the return, or, if no return is filed, from the lapse of the forty-eight (48) hour period to file the return, the authorized law enforcement officer has the duty to notify the person whose communications or computer data have been intercepted of the activities conducted pursuant to the WICD. If a return has been filed, a copy of the same shall be attached to the notice. On the other hand, if no return has been filed, the notice shall state the details of the interception activities, including the contents of the intercepted communication or computer data. Within ten (10) days from notice, the person whose communications or computer data have been intercepted may challenge, by motion, the legality of the interception before the issuing court.
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	**Also see Section 5, Rule on Cybercrime Warrants (A.M. No. 17-11-03-SC)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
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	**R.A. No. 10175** **SEC. 21. Jurisdiction** The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 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.	computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines. There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.
Chapter III – International co-operation	
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.	**R.A. No. 10175** **Sec. 22. General Principles Relating to International Cooperation** All relevant international instruments on international cooperation 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 offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal, offense shall be given full force and effect. **Implementing Rules and Regulations of R.A. No. 10175**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
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. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep	Rule 5 – International Cooperation **Section 25. *International Cooperation.*** – All relevant international instruments on international cooperation on criminal matters, and arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws shall be given full force and effect, to the widest extent possible for the purposes of investigations or proceedings concerning crimes related to computer systems and data, or for the collection of electronic evidence of crimes. The DOJ shall cooperate and render assistance to other contracting parties, as well as request assistance from foreign states, for purposes of detection, investigation and prosecution of offenses referred to in the Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069 and other pertinent laws, as well as existing extradition and mutual legal assistance treaties, shall apply. In this regard, the central authority shall: a. Provide assistance to a requesting State in the real-time collection of traffic data associated with specified communications in the country transmitted by means of a computer system, with respect to criminal offenses defined in the Act for which real-time collection of traffic data would be available, subject to the provisions of Section 13 hereof; b. Provide assistance to a requesting State in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system, subject to the provision of Section 13 hereof; c. Allow another State to: 1. Access publicly available stored computer data located in the country or elsewhere; or 2. Access or receive, through a computer system located in the country, stored computer data located in another country, if the other State

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
updated a register of authorities so designated by the Parties. Each Party shall ensure	obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to said other State through that computer system. d. Receive a request of another State for it to order or obtain the expeditious preservation of data stored by means of a computer system located within the country, relative to which the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data: *Provided*, That: 1. A request for preservation of data under this section shall specify: i. The authority seeking the preservation; ii. The offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; iii. The stored computer data to be preserved and its relationship to the offense; iv. The necessity of the preservation; and v. That the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 2. Upon receiving the request from another State, the DOJ and law enforcement agencies shall take all appropriate measures to expeditiously preserve the specified data, in accordance with the Act and other pertinent laws. For the purposes of responding to a request for preservation, dual criminality shall not be required as a condition; 3. A request for preservation may only be refused if: i. The request concerns an offense that the Philippine Government considers as a political offense or an offense connected with a political offense; or ii. The Philippine Government considers the execution of the request to be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	prejudicial to its sovereignty, security, public order or other national interest. 4. Where the Philippine Government believes that preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting State's investigation, it shall promptly so inform the requesting State. The requesting State will determine whether its request should be executed; and 5. Any preservation effected in response to the request referred to in paragraph (d) shall be for a period not less than sixty (60) days, in order to enable the requesting State to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request. e. Accommodate request from another State to search, access, seize, secure, or disclose data stored by means of a computer system located within the country, including data that has been preserved under the previous subsection. The Philippine Government shall respond to the request through the proper application of international instruments, arrangements and laws, and in accordance with the following rules: 1. The request shall be responded to on an expedited basis where: i. There are grounds to believe that relevant data is particularly vulnerable to loss or modification; or ii. The instruments, arrangements and laws referred to in paragraph (b) of this section otherwise provide for expedited cooperation. 2. The requesting State must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the requested information subject to the conditions specified in the grant. f. Make a request to any foreign state for assistance for purposes of detection,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	investigation and prosecution of offenses referred to in the Act; g. The criminal offenses described under Chapter II of the Act shall be deemed to be included as extraditable offenses in any extradition treaty where the Philippines is a party: *Provided*, That the offense is punishable under the laws of both Parties concerned by deprivation of liberty for a minimum period of at least one year or by a more severe penalty. The Secretary of Justice shall designate appropriate State Counsels to handle all matters of international cooperation as provided in this Rule.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose 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. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in	***Same with the immediately preceding section.***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and	**Implementing Rules and Regulations of R.A. No. 10175** Rule 5 – International Cooperation

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions	**Section 25. *International Cooperation.*** – All relevant international instruments on international cooperation on criminal matters, and arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws shall be given full force and effect, to the widest extent possible for the purposes of investigations or proceedings concerning crimes related to computer systems and data, or for the collection of electronic evidence of crimes. The DOJ shall cooperate and render assistance to other contracting parties, as well as request assistance from foreign states, for purposes of detection, investigation and prosecution of offenses referred to in the Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069 and other pertinent laws, as well as existing extradition and mutual legal assistance treaties, shall apply. In this regard, the central authority shall: a. Provide assistance to a requesting State in the real-time collection of traffic data associated with specified communications in the country transmitted by means of a computer system, with respect to criminal offenses defined in the Act for which real-time collection of traffic data would be available, subject to the provisions of Section 13 hereof; b. Provide assistance to a requesting State in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system, subject to the provision of Section 13 hereof; c. Allow another State to: 3. Access publicly available stored computer data located in the country or elsewhere; or 4. Access or receive, through a computer system located in the country, stored computer data located in another country, if the other State obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to said other State through that

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	computer system. d. Receive a request of another State for it to order or obtain the expeditious preservation of data stored by means of a computer system located within the country, relative to which the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data: *Provided*, That: 2. A request for preservation of data under this section shall specify: i. The authority seeking the preservation; ii. The offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; iii. The stored computer data to be preserved and its relationship to the offense; iv. The necessity of the preservation; and v. That the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 2. Upon receiving the request from another State, the DOJ and law enforcement agencies shall take all appropriate measures to expeditiously preserve the specified data, in accordance with the Act and other pertinent laws. For the purposes of responding to a request for preservation, dual criminality shall not be required as a condition; 3. A request for preservation may only be refused if: i. The request concerns an offense that the Philippine Government considers as a political offense or an offense connected with a political offense; or ii. The Philippine Government considers the execution of the request to be prejudicial to its sovereignty, security, public order or other national interest. 4. Where the Philippine Government believes that preservation will not ensure

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting State's investigation, it shall promptly so inform the requesting State. The requesting State will determine whether its request should be executed; and 5. Any preservation effected in response to the request referred to in paragraph (d) shall be for a period not less than sixty (60) days, in order to enable the requesting State to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request. e. Accommodate request from another State to search, access, seize, secure, or disclose data stored by means of a computer system located within the country, including data that has been preserved under the previous subsection. The Philippine Government shall respond to the request through the proper application of international instruments, arrangements and laws, and in accordance with the following rules: 1. The request shall be responded to on an expedited basis where: i. There are grounds to believe that relevant data is particularly vulnerable to loss or modification; or ii. The instruments, arrangements and laws referred to in paragraph (b) of this section otherwise provide for expedited cooperation. 2. The requesting State must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the requested information subject to the conditions specified in the grant. f. Make a request to any foreign state for assistance for purposes of detection, investigation and prosecution of offenses referred to in the Act; g. The criminal offenses described under Chapter II of the Act shall be deemed

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	to be included as extraditable offenses in any extradition treaty where the Philippines is a party: *Provided*, That the offense is punishable under the laws of both Parties concerned by deprivation of liberty for a minimum period of at least one year or by a more severe penalty. The Secretary of Justice shall designate appropriate State Counsels to handle all matters of international cooperation as provided in this Rule.
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	***Same with the immediately preceding section.***
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the	***Same with the immediately preceding section.***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	***Same with the immediately preceding section.***
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system	***Same with the immediately preceding section.***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	***Same with the immediately preceding section.***
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	***Same with the immediately preceding section.***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	***Same with the immediately preceding section.***
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose 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. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Implementing Rules and Regulations of R.A. No. 10175** Rule 6 – Competent Authorities **Section 28.** ***Department of Justice (DOJ); Functions and Duties.*** – The DOJ-Office of Cybercrime (OOC), designated as the central authority in all matters related to international mutual assistance and extradition, and the Cybercrime Operations Center of the CICC, shall have the following functions and duties: a. Act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects; b. Act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the Act; c. Issue preservation orders addressed to service providers; d. Administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime; e. Require the submission of timely and regular reports including pre-operation, post-operation and investigation results, and such other documents from the PNP and NBI for monitoring and review; f. Monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof; g. Facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity-building related to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 Implementing Rules and Regulations of R.A. No. 10175 A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants R.A. No. 9775 or the Anti-Child Pornography Act of 2009 R.A. No. 8293 or the Intellectual Property Code of the Philippines 1987 Philippine Constitution
	cybercrime prevention, suppression and prosecution; h. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices; i. Prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination; j. Undertake the specific roles and responsibilities of the DOJ related to cybercrime under the Implementing Rules and Regulation of Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009"; and k. Perform such other acts necessary for the implementation of the Act.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents