Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version January 2010

Cybercrime legislation – country profile

MALAYSIA

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Malaysia**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
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;	**Section 2 (Interpretation) of Computer Crimes Act 1997 (CCA):-** **Computer** means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in

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	conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility. **Computer network** means the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers. **Computer output or output** means a statement or a representation whether in written, printed, pictorial, film, graphical, acoustic or other form- (a) Produced by a computer (b) Displayed on the screen of a computer (c) Accurately translated from a statement or representation so produced **Data** means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer. **Section 6 (1) of the Communications and Multimedia Act 1998(CMA):-** Communications means any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms – **wide enough to cover both traffic data and content data.**
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.	**Section 3 of Computer Crimes Act 1997-** (1) A person shall be guilty of an offence if- (a) He causes a computer to perform any function with intent to secure access to any program or data held in any computer (b) The access he intends to secure is unauthorised; and (c) He knows at the time when he causes the computer to perform the

	function that is the case **Section 2 of the CCA 1997 – Interpretation** Function includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer.
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.	**Section 234 of CMA 1998 – Interception and disclosure of communications prohibited** (1) A person who, without lawful authority under this Act or any other written law- (a) Intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any communications; (b) Discloses, or attempts to disclose, to any other person the contents, of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or (c) Uses, or attempts to use, the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section Commits an offence. (2) A person authorised under this Act who intentionally discloses, attempts to disclose, to any other person the contents of any communications, intercepted by means authorised by this Act- (a) Knowingly or having reason to believe that the information was obtained thorough the interception of such communications in connection with criminal investigation (b) Having obtained or received the information in connection with a criminal investigation; or (c) To improperly obstruct, impede or interfere with a duly authorised criminal investigation

	commits an offence (3) A person who commits an offence under subsection (1) or (2) shall on conviction be liable to a fine not exceeding RM50, 000.00 or to imprisonment for a term not exceeding 1 year or both. (4) It shall be lawful under this Chapter for an officer, employee or agent of any network facilities provider, network service provider, applications service provider or content applications service provider whose facilities or services are used in communications to intercept, disclose or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his facilities or services or to the protection of the rights or property of the provider of the facilities or services, but the provider shall not utilise the facilities or services for observing or random monitoring unless it is for mechanical or service quality control checks. **Section 252 (1) of CMA 1998 – Power to intercept communications (safeguards for interception)**
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.	**Section 5 of Computer Crimes Act 1997- Unauthorised modification of the contents of any computer-** (1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorised modification of the contents of any computer (2) For the purposes of this section, it is immaterial that the act in question is not directed at- (a) Any particular program or data (b) A program or data of any kind or (c) A program or data held in any particular computer (3) For the purposes of this section, it is immaterial whether an unauthorised modification is or is intended to be permanent or merely temporary (4) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM100,000.00 or to imprisonment for a term not

	exceeding 7 years or both or be liable to a fine not exceeding RM150,000.00 or to imprisonment for a term not exceeding 10 years or to both, if the act is done with the intention of causing injury as defined in Penal Code.
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	**Section 5 of the CCA – Unauthorised modification of the contents of any computer** Section 2 (7) Interpretation of CCA 1997 – for the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer- (a) Any program or data held in the computer concerned is altered or erased; (b) Any program or data is introduced or added to its content; **(c) Any event occurs which impairs the normal operation of any computer (interpreted to cover DDos attacks/Botnet attacks)** And any act that contributes towards causing such a modification shall be regarded as causing it. **Section 2 (8) Interpretation of CCA 1997 – Any modification referred to subsection (7) above is unauthorised if-** (a) The person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) He does not have consent to the modification from any person who is so entitled. **Section 235 of CMA - Damage to network facilities** A person who by any wilful, dishonest or negligent act or omission, extends, tampers with, adjusts, alters, removes, destroys or damages any network facilities or any part of them commits an offence and shall, on conviction, be liable to a fine not exceeding RM300,000.00 or to imprisonment for a term not exceeding 3 years or both.
Article 6 – Misuse of devices	**Section 236 CMA – Fraud and related activity in connection with access**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**devices etc** (1) A person who knowingly or with intention to defraud- (a) Produce, assembles, uses, imports, sells, supplies or lets for hire any counterfeit access devices (b) Possesses any counterfeit access device or unauthorised access device (c) Produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses any device-making equipment; or (d) Produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses- (i) Any equipment, device or apparatus that has been modified or altered to obtain unauthorised use of any network service applications service or content applications services or (ii) Hardware or software used for altering or modifying any equipment, device or apparatus to obtain unauthorised access to any network service, applications services or content applications services. Commits an offence. (2) A person who without the authorisation of the issuer of an access device, solicits a person for the purpose of- (a) Offering an access device; or (b) Selling information regarding, or an application to obtain an access device Commits an offence. (3) A person who commits an offence under subsection (1) or (2) shall on conviction, be liable to a fine not exceeding RM500,00.00 or to imprisonment for a term not exceeding 5 years or to both (4) For the purposes of this section- **Counterfeit access device means** any access device that is counterfeit, fictitious, altered or forged or an identifiable component of an access device or a counterfeit access device

	Device –making equipment means any equipment, mechanism or impression designed or primarily used for making an access device or a counterfeit access device **Unauthorised access device** means any access device that is lost, stolen, expired, revoked, cancelled or obtained with intent to defraud Access device is defined as any card, plate, code, account number, electronic serial number, mobile identification number, or other network service, applications service or content applications service, equipment, or facility identifier, or other means of access that can be used, alone or in conjunction with another access device, for the purposes of any communications. **Section 6 of the CCA 1997 (wrongful communications)** (1) A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate (2) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM25,000.00 or to imprisonment for a term not exceeding 3 years or both.
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.	**Section 463 – Forgery – Penal Code** Section 4 of CCA 1997 – Unauthorised access with intent to commit or facilitate commission of further offence (1) A person shall be guilty of an offence under this section if he commits an offence referred to in Section 3 of CCA 1997 with intent- (a) To commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or (b) To facilitate the commission of such an offence whether by himself or by any other person

	(2) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorised access is secured or any future occasions. (3) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM150,000.00 or to imprisonment for a term not exceeding 10 years or both.
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.	**Section 415 of Penal Code (covers both conventional and cyber fraud)-** **Cheating.** Whoever by deceiving any person, whether or not such deception was the sole or main inducement: *(a)* **fraudulently or dishonestly induces the person so deceived to deliver any property** to any person, or to consent that any person shall retain any property; or *(b)* **intentionally induces the person so deceived to do or omit to do anything** which he would not do or omit to do if he were not so deceived and which act or omission causes or is **likely to cause damage or harm to any person in body, mind, reputation, or property** is said to "**cheat**". **Section 3 of CCA 1997 – Unauthorized access to computer material** **Section 4 of CCA 1997 – Unauthorized access with intent to commit or facilitate commission of further offence** **Section 8 of CCA 1997 –** **Presumption** A person who has in his custody or control any program, data or other information which is held in any computer or retrieved from any computer which he is not authorized to have in his custody or control shall be deemed to have obtained unauthorized access to such program, data or information unless the contrary is proved.

	Section 233 of CMA 1998 – Improper use of network facilities or network service etc (1) A person who- (a) By means of any network facilities or network service or applications service knowingly- (i) Makes, creates or solicits and (ii) Initiates the transmission of Any comment, request, suggestion or other communication which is obscene, indecent, **false,** menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or (b) Initiates a communications using any application service, whether continuously , repeatedly or otherwise during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address Commits an offence
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall	Malaysia does not have specific legislation against child pornography. Such offences are dealt with under the following provisions:- **Section 292 of Penal Code – Sale etc of obscene books etc** **Section 293- Sale of obscene objects to young persons** **Section 372, Section 372A, Section 372B of Penal Code** **Child Act 2001 – Section 31, 32 and 43** **Section 211 of the CMA 1998 – Prohibition on provision of offensive content** (1) No content applications service provider or other person using a content applications service shall provide content which is indecent, obscene, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass any person

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.	**Section 233 of the CMA 1998 (Improper use of network facilities or network service)**
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial	**Section 7, 8 and 41 of Copyright Act 1987 (reprint- 2001) (Act 332)**

scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 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.	**Section 4(1/b,3) and Section 7(1) of CCA – Abetments and attempts punishable as offences** **Section 34 and 511 of the Penal Code**

Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Section 244 of the CMA (Offences by body corporate)**
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.	Sufficient sanctions and measures provided in the following legislations:- **Computer Crimes Act 1997;** **Communications and Multimedia Act 1998;** **Penal Code** **Child Act 2001** **Copyright Act 1987**
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	**Section 10 of CCA – Powers of search, seizure and arrest** **Part X Chapter 3 of the CMA – Powers of entry, investigation into offences and prosecution** **Section 50 of Copyright Act** **Criminal Procedure Code (Section 16, 17, 20, 20A and 62)**

to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
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	**Federal Constitution of Malaysia Part II – Fundamental Liberties (supreme law of the country)** Examples of safeguards in substantive law Section 252 of CMA 1998 – Power to intercept Requirement to make application and obtain authorisation from Public

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.	Prosecutor prior to conducting interception.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 263 of the CMA – General duty of the licensees (limited to telecommunications sector service providers)** (2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia including but not limited to the protection of the public revenue and preservation of national security. **Section 51 (1) of CPC** Summons to produce document or other things. **Section 268 in CMA –** The Minister may make rules, to be published in the *Gazette*, to provide for record-keeping and to require one or more licensees or persons to keep and retain records. Draft rules have been developed

Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 263 of the CMA – General duty of the licensees** (2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia including but not limited to the protection of the public revenue and preservation of national security. **Section 51 (1) of the Criminal Procedure Code**: Summons to produce document or other things. **Section 268 in CMA** – The Minister may make rules, to be published in the *Gazette*, to provide for record-keeping and to require one or more licensees or persons to keep and retain records. Draft rules have been developed
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;	**Specific provisons in relation with the handling and producing of evidence:-** **Section 10 of the CCA:- Powers of search, seizure and arrest** **Chapter 3 of the CMA :- Powers of entry, investigation into offences and prosecution (Section 245 to Section 262)** **Section 51 of the Criminal Procedure Code (summons to produce document or other things)** **Section 23 Mutual Assistance in Criminal Matters 2002 (production order for criminal matters)** **Section 90A of the Evidence Act 1950** **Admissibility of documents produced by computers and of statements, contained therein.** (1) In any criminal or civil proceeding a document produced by a computer or a statement contained in such document, shall be

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.	admissible as evidence of any fact stated therein if the document was **produced by the computer in the course of its ordinary use**, **whether or not the person tendering the same is the maker** of such document or statement. **Provisioning of subscribers information** Service Providers are obliged to share subscriber's information to the Regulator and relevant authorities' for investigation of offences through the General Consumer Code, application of which is mandated through the Service Providers' standard licence condition. The above requirement is also duplicated in the terms and conditions of the contractual agreement for subscription of service between the Service Providers and their customers.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a	**Section 10 of the CCA 1997 – Powers of search, seizure and arrest** (1) Whenever it appears to any Magistrate upon information and after such inquiry as he thinks necessary that there is reasonable cause to believe that in any premises there is evidence of the commission of an offence under this Act, he may, by warrant directed to any police officer of or above the rank of Inspector, empower the officer to enter the premises, by force if necessary, and there to search for, **seize and detain any such evidence** and he shall be entitled- (a) – "have access to any program or data held in any computer, or have access to, inspect or check the operation of, **any computer and any associated apparatus or material** which he has reasonable cause to suspect is or has been use in connection with any offence under this Act" (b) Require- (i) The person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or (ii) Any person having charge of or otherwise concerned with the operation of, the computer, apparatus or material

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.	To provide him with such reasonable assistance as he may require for the purposes of paragraph (a); and (c) Require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible. Part X Chapter 3 of CMA 1998 – Powers of Entry, Investigation into Offences and Prosecution Section 249 of the CMA 1998 - access to computerised data **(1)** A police officer conducting a search under Section 247 (search under warrant) or 248 (search and seizure without warrant) or an authorised officer conducting a search under section 247 shall be given access to computerised data **whether stored in a computer or otherwise.** (2) For the purpose of this section, "access" includes- (a) Being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data; and (b) The meaning assigned to it by subsection 2(2) and (5) of the CCA 1997
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	**Section 268 of CMA 1998 – Minister may make rules on record keeping** The Minister may make rules, to be published in the Gazette to provide for record-keeping and to require one or more licensees or persons to keep and retain records Draft rules have been developed. **Section 252 of CMA 1998 – Power to intercept communications (includes both traffic and content data)**

communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.	**Section 252 of the CMA 1998 – Power to intercept communications** (1) Notwithstanding the provisions of any other written law, the Public Prosecutor, if he considers that any communications is likely to contain any information which is relevant for the purpose of any investigation into an offence under this Act or its subsidiary legislation may on the application of an authorised officer or a police officer or above the rank of Superintendent, authorise the officer to intercept or to listen to any communication transmitted or received by any communication. (includes both traffic and content data) **Section 211 – Prohibition on provision of offensive content** **Section 233 – Improper use of network facilities and network services** General provisions for interception are also provided for the following offences:- (a) Kidnapping Act (b) Dangerous Drug Act (c) Anti Terrorism provisions under Criminal Procedure Code (Section 106C)

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 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.	**Section 9 of the CCA – Territorial scope of offences under this Act** **Section 4 of the CMA – Territorial and extra-territorial application** **Section 4 of the Penal Code – Extension of the Code to extra territorial** offences
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	**Section 6 of the Extradition Act 1992** **Section 9(3) of the CCA 1997** Specific Extradition Treaties with Thailand, Indonesia, Hong Kong, Australia and

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

provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
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 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	**Section 3, 7, 19 and 20 of the Mutual Assistance in Criminal Matters Act 2002.**

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.	**Section 4 of the Mutual Assistance in Criminal Matters Act 2002** **Section 269 of the CMA 1998 (Interworking with other authorities)-** (1) The Minister may direct the Commission regarding the interworking arrangements between the Commission and any other authority in Malaysia or in a foreign jurisdiction or any international organisation (2) The Minister may make rules to be published in the Gazette and/or determine arrangements for interworking with or membership of international organisations regarding the interworking arrangements between licensees under this Act and international organisation (3) The Commission may direct a licensee to comply with the rules made and/or arrangements determined under subsection (2)
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 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	**Section 19, Section 20-42 of the Mutual Assistance in Criminal Matters Act 2002 + numerous treaties with ASEAN and non-ASEAN members.**

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 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.	
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.	**Section 19 (c) (vii) of the Mutual Assistance in Criminal Matters Act 2002.**
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,	**Section 263 of CMA 1998 – General duty of licensees** **Section 51 (1) of CPC- Summons to produce documents and other things** **Section 268 of CMA – Minister may make rules on record-keeping**

located within the territory of that other Party and in respect of which the 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 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.	**Section 263 of CMA 1998 – General duty of licensees** **Section 51 (1) of CPC- Summons to produce documents and other things** **Section 268 of CMA – Minister may make rules on record-keeping**
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 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	**S3 of MACMA 2002 – provide and obtain international assistance in criminal matters** **Section 35 of the Mutual Assistance in Criminal Matters Act 2002 – Request for search and seizure**

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.	**Section 4 of the Mutual Assistance in Criminal Matters Act 2002.**
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.	**Section 3 and 4 of the Mutual Assistance in Criminal Matters Act 2002** **Section 265 and 269 of the CMA 1998**
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.	Section 3 and 4 of the Mutual Assistance in Criminal Matters Act 2002 Section 265 and 269 of the CMA 1998
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	**Malaysian Control Centre – MCC under the Royal Malaysian Police**

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.	
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.	