Project on Cybercrime
www.coe.int/cybercrime

COUNCIL CONSEIL
OF EUROPE DE L'EUROPE

Version 30 May 2007
[Reformat in March 2011]

Cybercrime legislation – country profile

DOMINICAN REPUBLIC

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:

Country:	Dominican Republic
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	**Computer system:** Any electronic device, regardless of its form, size, capacity or technology used, capable of processing data and/or signals and performing logical, arithmetical and memory functions by manipulating electronic, optical, magnetic, electro-chemical or any other type of impulses, including all input,

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	output, processing, storage, programme, communication or other facilities connected or linked to or integrated with the system. **Computer data:** Any information transmitted, saved, recorded, processed, copied or stored in any type of information system or in any of its component parts, such as those geared to the transmission, emission, storage, processing and reception of electro-magnetic signals, signs, signals, writing, still or moving images, videos, voice, sounds, data transmitted by optical, cellular or radio-electrical means, electro-magnetic systems or through any other channel suited to the purpose.

Chapter II – Measures to be taken at the national level
Section 1 – Substantive criminal law

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

Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Article 6.- Illegal access.** The fact of acceding to an electronic, computing, telematics or telecommunications system, or its component parts, whether or not by usurping an identity or exceeding authorisation, shall be punished with a prison sentence of between three months and one year and a fine of up to two hundred times the minimum wage.
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.	**Article 9.- Interception and tapping of data or signals.** The fact of intercepting, tapping, interfering with, blocking, spying and listening in on, diverting, recording and observing, in any way, an item or set of data, a signal or transmission of data or signals belonging to another person on one's own or someone else's behalf, without prior authorisation from a competent judge, from, through or towards an electronic, computing, telematics or telecommunications system, or information transmitted by the latter, deliberately and intentionally violating the secrecy, confidentiality and privacy of

	natural or legal persons, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage, without prejudice to any administrative sanctions imposed under separate laws and regulations.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Article 10.- Damaging and altering computer data.** The fact of deleting, damaging, introducing, copying, deforming, editing, altering or eliminating data and component parts of electronic, computing, telematics or telecommunications systems, or transmitted through one of the latter, for fraudulent purposes, shall be punished with a prison sentence of between three months and one year and a fine of between three and five hundred times the minimum wage.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Article 11.- Sabotage.** The fact of altering, deforming, impeding, disabling, causing to malfunction, damaging or destroying an electronic, computing, telematics or telecommunications system or the programmes and logical operations run by such system shall be punished with a prison sentence of between three months and two years and a fine of between three and five hundred times the minimum wage.
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	**Article 8.- Fraudulent devices.** The fact of producing, using, possessing, trafficking in or distributing, without authorisation or legitimate cause, computer programmes, hardware, equipment or devices whose sole or primary use is to commit high-technology crimes and offences, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage.

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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Article 18.- Forged documents and signatures.** Anyone forging, decoding or in any way deciphering, disclosing or trafficking in digital or electronic documents, signatures, certificates, shall be punished with a prison sentence of between one and three years and a fine of between fifty and two hundred times the minimum wage.
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;	**Article 13.- High-technology theft.** Where theft is committed by using electronic, computing, telematics or telecommunications systems or devices to disable or inhibit alarm, protection or other similar mechanisms; or in cases where, in order to gain access to houses or other premises or to movables, recourse is had to the same means or means different from those intended by their owner for such purposes; or by using magnetic or perforated cards, controls or instruments for remote opening or any

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.	other high-technology mechanism or device, shall be punished with a prison sentence of between two and five years and a fine of between twenty and five hundred times the minimum salary. **Article 14.- Illegal obtainment of funds.** The fact of obtaining funds, appropriations or assets by coercing the legitimate user of a computing, electronic, telematics or telecommunications financial service shall be punished with a prison sentence of between three and ten years and a fine of between one hundred and five hundred times the minimum wage. **Paragraph.- Electronic transfers of funds.** The fact of effecting electronic transfers of funds through the illegal use of access codes or of any other similar mechanism, shall be punished with a prison sentence of between one and five years and a fine of between two and two hundred times the minimum wage. **Article 15.- Fraud.** Fraud committed through the use of electronic, computing, telematics or telecommunications facilities shall be punished with a prison sentence of between three months and seven years and a fine of between ten and five hundred times the minimum wage. **Article 16.- Blackmail**. Blackmail committed by means of electronic, computing, telematics or telecommunications systems or their component parts, and/or for the purpose of obtaining funds, assets, or the signature or handover of a document, whether digital or not, or an access code or any other component of a computer system, shall be punished with a prison sentence of between one and five years and a fine of between ten and two hundred times the minimum wage.
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	**Article 24.- Child pornography.** The production, circulation, sale and any form of marketing of images or

committed intentionally and without right, the following conduct:
 	
    a   producing child pornography for the purpose of its distribution through a computer system;
    b   offering or making available child pornography through a computer system;
    c   distributing or transmitting child pornography through a computer system;
    d   procuring child pornography through a computer system for oneself or for another person;
    e   possessing child pornography in a computer system or on a computer-data storage medium.
 	
2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
    a   a minor engaged in sexually explicit conduct;
    b   a person appearing to be a minor engaged in sexually explicit conduct;
    c   realistic images representing a minor engaged in sexually explicit conduct
 	
3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
 	
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.
	representations of a child or adolescent of a pornographic nature as defined in this law shall be punished with a prison sentence of between two and four years and a fine of between ten and five hundred times the minimum wage.
	
	Paragraph.- **Purchase and possession of child pornography**.
	The purchase of child pornography via an information system for oneself or another person, and the deliberate possession of child pornography in an information system or any of its component parts shall be punished with a prison sentence of between three months and one year and a fine of between two and two hundred times the minimum wage.

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	**Article 25.- Offences related to intellectual property and related subjects.** Where the offences set out in Law No.20-00 of 8 May 2000 on Industrial Property and Law No.65-00 of 21 August 2000 on Copyright are committed via electronic, computing, telematics or telecommunications systems or via any of their component parts, the culprit shall be liable to the penalties laid down in the relevant legislation on these illegal acts.

Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 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.	- Law 53-07 does not cover this aspect.-

Article 12 – Corporate liability	Article 60.- Civil and criminal responsibility of legal persons.

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.
	In addition to the sanctions set out below, legal persons bear civil responsibility for offences committed by their subordinate bodies or representatives. Criminal responsibility for the acts and offences set out in this law extends to the individuals ordering or arranging their commission and the legal representatives of the legal persons who, being apprised of the illegality of the act and empowered to prevent it, have permitted, taken part in, facilitated or concealed it. Criminal responsibility on the part of legal persons does not preclude that of any natural person who has perpetrated or aided the acts in question. Where the legal persons are used as a means or as cover for the commission of a crime or offence, or if they are used to commit an act of culpable negligence, they will be liable to one or more or all of the following penalties:
	
	a) A fine equal to or up to twice that imposed on the natural person for the illegal act as set out in this law;
	b) Liquidation, in cases of a crime or offence penalised, in the case of natural persons, with a prison sentence of more than five years;
	
	c) Prohibition, on a permanent basis or for a period of not more than five years, of direct or indirect exercise of specific professional or social activities;
	
	d) Subjection to court supervision for a period of not more than five years;
	
	e) Closing, on a permanent basis or for a period of not more than five years, of one or more of the company's branches which were used to commit the offences in question;
	
	f) Prohibition from taking part in public competitive bidding on a permanent basis or for a period of not more than five years;
	
	g) Prohibition, on a permanent basis or for a period of not more than five years, from participating in activities geared to obtaining assets from public savings;
	
	h) Confiscation of the item having served or been intended to commit the offence, or of the item constituting the proceeds of the offence;

	i) Publishing or disseminating the sentence pronounced, either in the press or via any other medium.
	Paragraph.- Negligence on the part of the legal person.
	Similarly, the legal person shall be considered civilly liable where a lack of supervision of the legal representative or employee has led to the commission of an illegal act as provided for in this law.
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.	- Each offence includes the corresponding sanction. -
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;	**Article 52.- Application of the Code of Criminal Procedure.** The rules on immediate verification and auxiliary resources set out in the Code of Criminal Procedure, Law No.76-02, apply to the obtaining and safeguarding of the data contained in an information system or its component parts, traffic, connection or access data or any other relevant information for investigating the offences covered by this law and for all the procedures set out in this chapter.

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

Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other	**Article 57.- Perverting the course of justice.** Attempts to hamper the investigations conducted by the competent authorities shall be punished with immediate dismissal, a prison sentence of between six months and five years and a fine of not less than ten times the minimum wage. Such attempts to pervert the course of justice include: a) Implementing or requesting measures for reasons other than that of the actual prosecution of one of the crimes or offences set out in this law; b) Trafficking in and marketing data obtained during the investigations; c) Disclosure of personal and commercial data on the defendant which

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.	are irrelevant to the investigations, as well as trafficking in or marketing such data.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 53.- Safeguarding the data.** The competent authorities must take prompt action to safeguard the data contained in an information system or its component parts, or the system traffic data, especially where the latter are exposed to loss or modification.
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:	**Article 56.- Service providers.** Without prejudice to the provisions of Article 47 b) of this law, service providers must store traffic, connection and access data and any other information which might be useful for investigations, for a minimum period of ninety (90) days. The Dominican Institute of Telecommunications (INDOTEL) will set out the

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.	regulations on procedure for obtaining and storing data and information on the part of service providers for a period of 6 months from publication of this law. These regulations should take account of the importance of preserving evidence, regardless of the number of service providers involved in the data transmission or communication.

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.
	Article 54.- Powers of the Public Prosecutor's Office.
	Subject to compliance with the formalities laid down in the Code of Criminal Procedure, the Public Prosecutor's Office, which may co-opt the services of one or more of the following: State investigating agencies such as the Investigation Department for High-Technology Crimes and Offences (DICAT) of the National Police Force, the Computer Crime Investigation Division (DIDI) of the National CID, experts, public or private institutions or other competent authorities, is empowered to:
	
	a) Order a natural or legal person to supply information stored in an information or system in any of its component parts;

Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be	**Article 54.- Powers of the Public Prosecutor's Office**. b) Accede to or order access to such information system or to any of its

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

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	**Article 54.- Powers of the Public Prosecutor's Office**. k) Invite the service provider to retrieve, extract or record data on a given user, as well as real-time traffic data, by technological means;

the territory of that Party, and
    b   compel a service provider, within its existing technical capability:
        i   to collect or record through the application of technical means on the territory of that Party; or
        ii   to co-operate and assist the competent authorities in the collection or recording of,
        traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2   Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
3   Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4   The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
	l) Intercept telecommunications in real time, in accordance with the procedure set out in Article 192 of the Code of Criminal Procedure for the investigation of all the offences punishable under this law;

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
	Article 54.- Powers of the Public Prosecutor's Office.
	    d) Order service providers, including Internet service providers, to supply information on any user data they may have in their possession or control;

the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

Section 3 – Jurisdiction

Article 22 – Jurisdiction 1　　Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: 　　a　　in its territory; or 　　b　　on board a ship flying the flag of that Party; or 　　c　　on board an aircraft registered under the laws of that Party; or 　　d　　by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2　　Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3　　Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 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.	**Article 65.- Competent court.** Cases of high-technology crimes and offences are brought before the relevant ordinary courts or the Youth Court, depending on the type of case. Judges may order the presentation of an expert report on the merits of the case.

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. 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 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 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 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 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.	

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 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.	
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 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.	
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.	
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.	
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.	
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.	