Version 18 August 2008

Workshop on Cybercrime Legislation

Bogotá, Colombia, 3-5 September 2008

Working document

The Convention on Cybercrime, explanatory report & examples of implementation

English – Spanish – Portuguese

Prepared by the Council of Europe

Contents

1 Article 1 – Use of terms

1.1 Text of the Convention

Article 1 Use terms

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Artículo 1 – Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c. por "proveedor de servicios" se entenderá:
   i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
   ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;
d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Artigo 1º - Definições

Para os fins da presente Convenção:

a) "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;

b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;
c) "Fornecedor de serviço" significa:
Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e
Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.
d) "Dados de tráfego" significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

1.2 Examples

DOMINICAN REPUBLIC

Article 4. Definitions
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, 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.

Artículo 4.- Definiciones
Computadora: Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma.
Datos: Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil a tales fines.

ROMANIA, ART. 35 of Romania Law no 161/2003

Art. 35 - (1) For the purpose of the present law, the terms and phrases below have the following meaning:

a) *„computer system*" means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program;

b) *„automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program;

c) *„computer program*" means a group of instructions that can be performed by a computer system in order to obtain a determined result;

d) *„computer data"* are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function;

e) *„a service provider"* is:

1. any natural or legal person offering the users the possibility to communicate by means of a computer system;

2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;

f) *„traffic data"* are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication

g*) "data on the users"* are represented by any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user;

h) *„security measures"* refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;

i) *„pornographic materials with minors"* refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual behaviour.

(2) For the purpose of this title, *a person acts without right* in the following situations:

a) is not authorised, in terms of the law or a contract;

b) exceeds the limits of the authorisation;

c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

Art.35 (1) de la Ley de Rumania núm. 161/2003

- por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos por medio de un programa informático

- por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático. Esta categoría incluye todo programa informático diseñado para que un sistema informático ejecute una función

BARBADOS

"computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function ;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function ;

"service provider" means

(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or those users;

"traffic data" means computer data that

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of a chain of communication; and

(c) shows the origin, destination, route, time, date, size, duration of the communication of the type of underlying services used to generate the data.

1.3 Explanatory report

Introduction to the definitions at Article 1

22. It was understood by the drafters that under this Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation.

Article 1 (a) - Computer system

23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

Article 1 (b) - Computer data

25. The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion " computer data" is

introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

Article 1 (c) - Service provider

26. The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems (cf. also comments on Section 2). Under (i) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

27. Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.

Article 1 (d) - Traffic data

28. For the purposes of this Convention traffic data as defined in article 1, under subparagraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.

29. In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

30. The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

31. The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. In this context, Article 15 obliges the Parties to provide for conditions and safeguards that are adequate for protection of human rights and liberties. This implies, *inter alia*, that the substantive criteria and the procedure to apply an investigative power may vary according to the sensitivity of the data.

2 Article 2 - Illegal Access

2.1 Convention

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.

Artículo 2 – Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artigo 2º - Acesso ilegítimo

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

2.2 Examples

DOMINICAN REPUBLIC,
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.

Art. 6 Sec.1 Derecho Penal Sustantivo : El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.

ROMANIA, Law 161/2003
Art. 42 – (1) The access without right to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine.
(2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment is imprisonment from 6 months to 5 years.

(3) Where the act provided in paragraphs 1-2 is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

Art.42 de la Ley de Rumania núm. 161/2003

1. El acceso, sin derecho, a un sistema informático.

Toda persona actuará sin derecho en las siguientes situaciones:
a) no está autorizada, en términos de la legislación o de un contrato;
b) supera los límites de la autorización;
c) no ha recibido la autorización de la persona cualificada para concederla, de conformidad con la legislación, para utilizar, administrar o controlar un sistema informático, o llevar a cabo investigaciones científicas en un sistema informático.

2. El acto se comete con el propósito de obtener datos informáticos.
3. El acto se comete infringiendo medidas de seguridad.

GERMANY, section 202a (1) StGB
(1) Whoever, without authorisation and by means of violating access security mechanisms, obtains for himself or another party access to data that are not intended for him and that are specially protected against unauthorised access, shall be punished with imprisonment for not more than three years or a fine.

2.3 Explanatory report

Illegal access (Article 2)
44. "Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.
45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.
46. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.
47. The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other

right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots' to locate and retrieve information on behalf of communication. The application of such tools *per se* is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it.

49. Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

3 Article 3 - Illegal interception

3.1 Convention

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.

Artículo 3 – Interceptación ilícita
Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artigo 3º - Intercepção ilegítima
Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

3.2 Examples

DOMINICAN REPUBLIC,
Article 9. *Law 53-07*
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.

Artículo 9.- Interceptación e Intervención de Datos o Señales. El hecho de interceptar,

intervenir, injerir, detener, espiar, escuchar desviar grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.

ROMANIA, ART.43 of Romania Law no 161/2003

Art. 43 – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

BARBADOS

7. A person who knowingly and without lawful excuse or justification intercepts by technical means

(a) any transmission to, from or within a computer system that is not available to the public; or

(b) electromagnetic emissions that are carrying computer data from a computer system

is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

3.3 Explanatory report

Illegal interception (Article 3)

51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

52. The text of the provision has been mainly taken from the offence of 'unauthorised interception' contained in Recommendation (89) 9. In the present Convention it has been made clear that the communications involved concern "transmissions of computer data" as well as electromagnetic radiation, under the circumstances as explained below.

53. Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

54. The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term 'non-public' does not *per se* exclude communications via public networks.

Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of 'computer system' may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though 'non-public', takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

57. The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision.

58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing 'cookies', is not intended to be criminalised as such, as not being an interception "without right". With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken "with right".

59. In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as "intentionally" and "without right".

4 Article 4 –Data interference

4.1 Text of the Convention

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.

Artículo 4 – Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.
2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.

4.2 Examples

DOMINICAN REPUBLIC, Law 53-07 against cybercrime
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.

Artículo 10.- Daño o Alteración de Datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo.

ROMANIA, ART.44 of Romania Law no 161/2003
Art. 44 – (1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years.
(2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years.

(3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium.

BARBADOS

5. (1) A person who knowingly or recklessly, and without lawful excuse or justification,
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data;
(d) obstructs, interrupts or interferes with any person in the lawful use of data; or
(e) denies access to data to any person entitled to the data;
is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

4.3 Explanatory report

Data interference (Article 4)

60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.
61. In paragraph 1, 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.
62. The above acts are only punishable if committed "without right". Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g., software permitting access to the Internet that disables similar, previously installed programs), are with right and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime.
63. In addition, the offender must have acted "intentionally".
64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

5 Article 5 – System interference

5.1 Text of the Convention

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.

Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

5.2 Examples

DOMINICAN REPUBLIC, Law 53-07 against cybercrime

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.

Artículo 11.- Sabotaje. El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.

ROMANIA, ART.45 of Romania Law no 161/2003

The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years.

Art.45 de la Ley de Rumania núm. 161/2003

Art. 45 – El acto consistente en obstaculizar seriamente, sin derecho, el funcionamiento de un sistema informático, mediante la introducción, transmisión, alteración, supresión o deterioro de datos informáticos, o mediante la restricción del acceso a dichos datos, constituye un delito penal y será castigado con una pena de prisión de tres a quince años.

BARBADOS

6. A person who knowingly or recklessly, and without lawful excuse or justification,
(a) hinders the functioning of a computer system by
(i) preventing the supply of electricity, permanently or
otherwise, to a computer system;
(ii) causing electromagnetic interference to a computer
system;
(iii) corrupting the computer system by any means;
(iv) adding, deleting or altering computer data; or
(b) interferes with the functioning of a computer system or with a person who is lawfully using or operating a computer system is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

6. Toda persona que, intencional o temerariamente, y sin una excusa o justificación legal,
a) obstaculice el funcionamiento de un sistema informático
i) impidiendo el suministro de electricidad, permanentemente o de otro modo, a un sistema informático;
ii) causando interferencias electromagnéticas en un sistema informático;
iii) corrompiendo el sistema informático a través de cualquier medio;
iv) añadiendo, suprimiendo o alterando datos informáticos, o

b) interfiera en el funcionamiento de un sistema informático o con
una persona que esté utilizando o ejecutando legalmente un sistema informático,
será culpable de un delito y será castigada en un proceso acusatorio a una multa de 50.000 dólares o a una pena de prisión de cinco años, o a ambas cosas.

5.3 Explanatory report

System interference (Article 5)

65. This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.
66. The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.
67. The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).
68. The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of

a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

6 Article 6 – Misuse of devices

6.1 Text of the Convention

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Artículo 6 – Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;

una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un

número determinado de dichos elementos para que se considere que existe responsabilidad penal.
2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.
3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

Artigo 6º - Uso abusivo de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;
ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e
b) A posse de um elemento referido nos alínea *a)*, *i.* ou *ii.*, com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.

2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, *a)*, *ii.*

6.2 Examples

DOMINICAN REPUBLIC,

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.

Artículo 8.- Dispositivos Fraudulentos. El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

ROMANIA, ART.46 of Romania Law no 161/2003

Art. 43 – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

BARBADOS

8. A person who knowingly or recklessly, and without lawful excuse or justification,

(a) supplies, distributes or otherwise makes available

(i) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence under section 4, 5, 6 or 7; or

(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 the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7; or

(b) has an item mentioned in paragraph *(a)*(i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7

is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

6.3 Explanatory report

Misuse of devices (Article 6)

71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access - ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries. A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. 'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

73. The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted, by the last phrase of paragraph 1(b), to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

76. The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent

that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'.

78. Due to different assessments of the need to apply the offence of "Misuse of Devices" to all of the different kinds of computer offences in Articles 2 – 5, paragraph 3 allows, on the basis of a reservation (cf. Article 42), to restrict the offence in domestic law. Each Party is, however, obliged to criminalise at least the sale, distribution or making available of a computer password or access data as described in paragraph 1 (a) 2.

Title 2 - Computer-related offences

79. Articles 7 - 10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones.

80. "Computer-related forgery" and "Computer-related fraud" deal with certain computer-related offences, i.e. computer-related forgery and computer-related fraud as two specific kinds of manipulation of computer systems or computer data. Their inclusion acknowledges the fact that in many countries certain traditional legal interests are not sufficiently protected against new forms of interference and attacks.

7 Article 7 – Computer-related forgery

7.1 Text of the Convention

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.

Artículo 7 – Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artigo 7º - Falsidade informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

7.2 Examples

DOMINICAN REPUBLIC,
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.

Artículo 18.- De la Falsedad de Documentos y Firmas. Todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a tres años de prisión y multa de cincuenta a doscientas veces el salario mínimo.

ROMANIA, ART.48 of Romania Law no 161/2003

Art. 48 – The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.

7.3 Explanatory report

81. The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

82. It should be noted that national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data.

83. This provision covers data which is the equivalent of a public or private document, which has legal effects. The unauthorised "input" of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document.

84. The term "for legal purposes" refers also to legal transactions and documents which are legally relevant.

85. The final sentence of the provision allows Parties, when implementing the offence in domestic law, to require in addition an intent to defraud, or similar dishonest intent, before criminal liability attaches.

8 Article 8 –Computer related fraud

8.1 Text of the Convention

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.

Artículo 8 – Fraude informático

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a la introducción, alteración, borrado o supresión de datos informáticos;

b cualquier interferencia en el funcionamiento de un sistema informático,

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Artigo 8º - Burla informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:

a Da introdução, da alteração, da eliminação ou da supressão de dados informáticos,

b De qualquer intervenção no funcionamento de um sistema informático,

com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.

8.2 Examples

DOMINICAN REPUBLIC

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 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.

Artículo 13.- Robo Mediante la Utilización de Alta Tecnología. El robo, cuando se comete por medio de la utilización de sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología, se sancionará con la pena de dos a cinco años de prisión y multa de veinte a quinientas veces el salario mínimo.

Artículo 14.- Obtención Ilícita de Fondos. El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo.

Párrafo.- Transferencias Electrónica de Fondos. La realización de transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo.

Artículo 15.- Estafa. La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.

Artículo 16.- Chantaje. El chantaje realizado a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, se sancionará con la pena de uno a cinco años de prisión y multa de diez a doscientas veces el salario mínimo.

ROMANIA, ART.49 of Romania Law no 161/2003

Art. 49 – The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be punished with imprisonment from 3 to 12 years.

8.3 Explanatory report

Computer-related fraud (Article 8)

86. With the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.

87. To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer programme or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles. Article 8(b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

88. The computer fraud manipulations are criminalised if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term 'loss of property', being a broad notion, includes loss of money, tangibles and intangibles with an economic value.

89. The offence must be committed "without right", and the economic benefit must be obtained without right. Of course, legitimate common commercial practices, which are intended to procure an economic benefit, are not meant to be included in the offence established by this article because they are conducted with right. For example, activities carried out pursuant to a valid contract between the affected persons are with right (e.g. disabling a web site as entitled pursuant to the terms of the contract).

90. The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet ("bots"), even if not authorised by a site visited by the "bot" is not intended to be criminalised.

9 Article 9 – Offences related to child pornography

9.1 Text of the Convention

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

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.

Artículo 9 – Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

la difusión o la transmisión de pornografía infantil a través de un sistema informático;

la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;

la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:

un menor adoptando un comportamiento sexualmente explícito;

una persona que parezca un menor adoptando un comportamiento sexualmente explícito;

imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

Artigo 9º - Infracções relacionadas com pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:

a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;
c) Difundir ou transmitir pornografia infantil através de um sistema informático;
d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:

a) Um menor envolvido num comportamento sexualmente explícito;
b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;
c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;

3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.

4.Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea *d)*, e., 2, alíneas *b)* e *c)*.

9.2 Examples

DOMINICAN REPUBLIC

Article 24.- Child pornography. The production, circulation, sale and any form of marketing of images or 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.

Artículo 24.- Pornografía Infantil. La producción, difusión, venta y cualquier tipo de comercialización de imágenes o representaciones de un niño, niña o adolescente con carácter pornográfico en los términos definidos en la presente ley, se sancionará con penas de dos a cuatro años de prisión y multa de diez a quinientas veces el salario mínimo.

Párrafo.- **Adquisición y Posesión de Pornografía Infantil**. La adquisición de pornografía infantil por medio de un sistema de información para uno mismo u otra persona, y la posesión intencional de pornografía infantil en un sistema de información o cualquiera de sus componentes, se sancionará con la pena de tres meses a un año de prisión y multa de dos a doscientas veces el salario mínimo.

ROMANIA, ART.51(1) of Romania Law no 161/2003

Art.51 – (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer system or computer data storage medium.

BARBARDOS

13. (1) A person who, knowingly,
(a) publishes child pornography through a computer system; or
(b) produces child pornography for the purpose of its publication through a computer system; or
(c) possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication
is guilty of an offence and is liable on conviction on indictment,
(i) in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or
(ii) in the case of a corporation, to a fine of $200 000.
(2) It is a defence to a charge of an offence under subsection (1)(i) or (ii) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose.
(3) For the purposes of subsection (1),
(a) "child pornography" includes material that visually depicts
(i) a minor engaged in sexually explicit conduct; or
(ii) a person who appears to be a minor engaged in sexually explicit conduct; or
(iii) realistic images representing a minor engaged in sexually

explicit conduct;
(b) "publish" includes
(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;
(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(a)*; or
(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(a)*.

9.3 Explanatory report

91. Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.
92. This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 - 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).
93. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.
94. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system. This provision was felt necessary to combat the dangers described above at their source.
95. Paragraph 1(b) criminalises the 'offering' of child pornography through a computer system. 'Offering' is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. 'Making available' is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography.
96. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system. 'Distribution' is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of 'transmitting' child pornography.
97. The term 'procuring for oneself or for another' in paragraph 1(d) means actively obtaining child pornography, e.g. by downloading it.
98. The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.
99. The term 'pornographic material' in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material

having an artistic, medical, scientific or similar merit may be considered not to be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which are capable of conversion into a visual image.

100. A 'sexually explicit conduct' covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

101. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.

102. In the three cases covered by paragraph 2, the protected legal interests are slightly different. Paragraph 2(a) focuses more directly on the protection against child abuse. Paragraphs 2(b) and 2(c) aim at providing protection against behaviour that, while not necessarily creating harm to the 'child' depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.

103. The term 'without right' does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, the term 'without right' allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a Party may provide a defence in respect of conduct related to "pornographic material" having an artistic, medical, scientific or similar merit. In relation to paragraph 2(b), the reference to 'without right' could also allow, for example, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a minor in the sense of this provision.

104. Paragraph 3 defines the term 'minor' in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a 'child' in the UN Convention on the Rights of the Child (Article 1). It was considered an important policy matter to set a uniform international standard regarding age. It should be noted that the age refers to the use of (real or fictitious) children as sexual objects, and is separate from the age of consent for sexual relations. Nevertheless, recognising that certain States require a lower age-limit in national legislation regarding child pornography, the last phrase of paragraph 3 allows Parties to require a different age-limit, provided it is not less than 16 years.

105. This article lists different types of illicit acts related to child pornography which, as in articles 2 - 8, Parties are obligated to criminalise if committed "intentionally." Under this standard, a person is not liable unless he has an intent to offer, make available, distribute, transmit, produce or possess child pornography. Parties may adopt a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is "knowledge and control" over the information which is transmitted or stored. It is not sufficient, for example, that a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

106. Paragraph 4 permits Parties to make reservations regarding paragraph 1(d) and (e), and paragraph 2(b) and (c). The right not to apply these sections of the provision may be made in part or in whole. Any such reservation should be declared to the Secretary General of the Council of Europe at the time of signature or when depositing the Party's instruments of ratification, acceptance, approval or accession, in accordance with Article 42.

10 Offences related to child pornography

10.1 Text of the Convention

Article 10 – Offences related to infringements of copyright and related rights

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

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

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se

disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Artigo 10º - Infracções relacionadas com a violação do direito de autor e dos direitos conexos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação do direito de autor definido pela legislação dessa Parte, em conformidade com as obrigações que a mesma assumiu em aplicação da Convenção Universal sobre o Direito de Autor, revista em Paris, em 24 de Julho de 1971, da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais conferidos por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.
2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de qualquer direito moral conferido por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.
3. Uma Parte pode, em circunstâncias bem delimitadas, reservar-se o direito de não determinar a responsabilidade penal nos termos dos n.ºs 1 e 2 do presente artigo, na condição de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo.

10.2 Examples

DOMINICAN REPUBLIC,
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.
Artículo 25.- Delitos Relacionados a la Propiedad Intelectual y Afines. Cuando las infracciones establecidas en la ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

ROMANIA, ART. 139[8] - 139 [9] and art. 143 of Law on copyright no.8/1996

ART. 139[8]

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the act of making available to the public, including through the Internet or other computer networks, without the consent of the owners of the copyright of protected works, neighbouring rights or sui generis rights of the manufacturers of databases or copies of such protected work, regardless of the form of storage thereof, in such a manner as to allow to the public to access it from anywhere or at anytime individually chosen.

ART. 139[9]

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the unauthorised reproduction in information systems of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission.

ART. 143

(1) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of manufacturing, import, distribution or rental, offer, by any means, for sale or rental or possession in view of selling without right devices or components that allow neutralisation of technical measures of protection or that perform services that lead to neutralisation of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment.

(2) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of person whom, without having the consent of the owners of the copyright, and while knowing or should have known that thus is allowing, facilitating, causing or concealing a violation of a right as set forth in this law:

a) removes or modifies from the protected works for commercial purposes any electronic information relating to the applicable regulations on copyright or neighbouring rights,

b) distributes, imports in view of distribution, broadcasts or publicly communicates or makes available to the public, so as to allow access from any place and at any time chosen individually, without right, through digital technology, works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights, have been removed or modified without authorisation.

10.3 Explanatory report

Offences related to infringements of copyright and related rights

107. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audio-visual and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international co-operation in this field.

108. Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale". Paragraph 1 provides for criminal sanctions against infringements of copyright by means of a computer system. Infringement of copyright is already an offence in almost all States. Paragraph 2 deals with the infringement of related rights by means of a computer system.

109. Infringement of both copyright and related rights is as defined under the law of each Party and pursuant to the obligations the Party has undertaken in respect of certain international instruments. While each Party is required to establish as criminal offences those infringements, the precise manner in which such infringements are defined under domestic law may vary from State to State. However, criminalisation obligations under the Convention do not cover intellectual property infringements other that those explictly addressed in Article 10 and thus exclude patent or trademark-related violations.

110. With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are 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 (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.

111. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty had not entered into force at the time of concluding the present Convention. These treaties are nevertheless important as they significantly update the international protection for intellectual property (especially with regard to the new right of 'making available' of protected material 'on demand' over the Internet) and improve the means to fight violations of intellectual property rights worldwide. However it is understood that the infringements of rights established by these treaties need not be criminalised under the present Convention until these treaties have entered into force with respect to a Party.

112. The obligation to criminalise infringements of copyright and related rights pursuant to obligations undertaken in international instruments does not extend to any moral rights conferred by the named instruments (such as in Article 6bis of the Bern Convention and in Article 5 of the WIPO Copyright Treaty).

113. Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations.

114. The provisions are intended to provide for criminal sanctions against infringements 'on a commercial scale' and by means of a computer system. This is in line with Article 61 of the TRIPS Agreement which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale". However, Parties may wish to go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.

115. The term "without right" has been omitted from the text of this article as redundant, since the term "infringement" already denotes use of the copyrighted material without authorisation. The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

116. Paragraph 3 allows Parties not to impose criminal liability under paragraphs 1 and 2 in "limited circumstances" (e.g. parallel imports, rental rights), as long as other effective remedies, including civil and/or administrative measures, are available. This provision essentially allows Parties a limited exemption from the obligation to impose criminal liability, provided that they do not derogate from obligations under Article 61 of the TRIPS Agreement, which is the minimum pre-existing criminalisation requirement.

117. This article shall in no way be interpreted to extend the protection granted to authors, film producers, performers, producers of phonograms, broadcasting organisations or other right holders to persons that do not meet the criteria for eligibility under domestic law or international agreement.

11 Article 11 – Attempt and aiding or abetting

11.1 Text of the Convention

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.

Artículo 11 – Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.
3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artigo 11º - Tentativa e cumplicidade

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infracções estabelecidas de acordo com os artigos 2º a 10º da presente Convenção, com a intenção de que essa infracção seja cometida.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a tentativa de cometer uma das infracções estabelecidas nos artigos 3º, 5º, 7º, 8º, 9º, 1., alínea *a)* e 9, 1. alínea *c)* da presente Convenção.

3. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

11.2 Explanatory report

Attempt and aiding or abetting (Article 11)

118. The purpose of this article is to establish additional offences related to attempt and aiding or abetting the commission of the offences defined in the Convention. As discussed further below, it is not required that a Party criminalise the attempt to commit each offence established in the Convention.

119. Paragraph 1 requires Parties to establish as criminal offences aiding or abetting the commission of any of the offences under Articles 2-10. Liability arises for aiding or abetting where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. For example, although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

120. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt (for example, the elements of offering or making available of child pornography). Moreover, some legal systems limit the offences for which the attempt is punished. Accordingly, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c).

121. As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

122. Paragraph 3 was added to address the difficulties Parties may have with paragraph 2, given the widely varying concepts in different legislations and despite the effort in paragraph 2 to exempt certain aspects from the provision on attempt. A Party may declare that it reserves the right not to apply paragraph 2 in part or in whole. This means that any Party making a reservation as to that provision will have no obligation to criminalise attempt at all, or may select the offences or parts of offences to which it will attach criminal sanctions in relation to attempt. The reservation aims at enabling the widest possible ratification of the Convention while permitting Parties to preserve some of their fundamental legal concepts.

12 Article 12 – Corporate liability

12.1. Text of the Convention

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.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

un poder de representación de la persona jurídica;

una autorización para tomar decisiones en nombre de la persona jurídica;

una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artigo 12º - Responsabilidade de pessoas colectivas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis por infracções estabelecidas de acordo com a presente Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa colectiva que exerça no seu seio uma posição de direcção, com base no seguinte:

a) Poder de representação da pessoa colectiva;

b) Autoridade para tomar decisões em nome da pessoa colectiva;

c) Autoridade para exercer controlo no seio da pessoa colectiva.

2. Além dos casos já previstos no n.º 1 deste artigo, cada Parte adoptará as medidas necessárias para assegurar que uma pessoa colectiva possa ser considerada responsável quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 tornou possível a prática de infracções previstas na presente Convenção, em benefício da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade.

3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa.

4. Essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção.

12.2. Explanatory report

Corporate liability (Article 12)

123. Article 12 deals with the liability of legal persons. It is consistent with the current legal trend to recognise corporate liability. It is intended to impose liability on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention.

124. Under paragraph 1, four conditions need to be met for liability to attach. First, one of the offences described in the Convention must have been committed. Second, the offence must have been committed for the benefit of the legal person. Third, a person who has a leading position must have committed the offence (including aiding and abetting). The term "person who has a leading position" refers to a natural person who has a high position in the organisation, such as a director. Fourth, the person who has a leading position must have acted on the basis of one of these powers – a power of representation or an authority to take decisions or to exercise control – which demonstrate that such a physical person acted within the scope of his or her authority to engage the liability of the legal person. In sum, paragraph 1 obligates Parties to have the ability to impose liability on the legal person only for offences committed by such leading persons.

125. In addition, Paragraph 2 obligates Parties to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by

another person acting under the legal person's authority, i.e., one of its employees or agents acting within the scope of their authority. The conditions that must be fulfilled before liability can attach are that (1) an offence has been committed by such an employee or agent of the legal person, (2) the offence has been committed for the benefit of the legal person; and (3) the commission of the offence has been made possible by the leading person having failed to supervise the employee or agent. In this context, failure to supervise should be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person. Such appropriate and reasonable measures could be determined by various factors, such as the type of the business, its size, the standards or the established business best practices, etc. This should not be interpreted as requiring a general surveillance regime over employee communications (see also paragraph 54). A service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person, because the term "acting under its authority" applies exclusively to employees and agents acting within the scope of their authority.

126. Liability under this Article may be criminal, civil or administrative. Each Party has the flexibility to choose to provide for any or all of these forms of liability, in accordance with the legal principles of each Party, as long as it meets the criteria of Article 13, paragraph 2, that the sanction or measure be "effective, proportionate and dissuasive" and includes monetary sanctions.

127. Paragraph 4 clarifies that corporate liability does not exclude individual liability.

13 Article 13 – Sanctions and measures

13.1 Text of the Convention

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.

Artículo 13 – Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.
2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Artigo 13º - Sanções e medidas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade.
2. Cada Parte assegurará que as pessoas colectivas consideradas responsáveis nos termos do artigo 12º, fiquem sujeitas à aplicação de sanções ou medidas, penais ou não penais eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.

13.2. Explanatory report

Sanctions and measures (Article 13)

128. This article is closely related to Articles 2-11, which define various computer- or computer-related crimes that should be made punishable under criminal law. In accordance with the obligations imposed by those articles, this provision obliges the Contracting Parties to draw consequences from the serious nature of these offences by providing for criminal sanctions that are 'effective, proportionate and dissuasive' and, in the case of natural persons, include the possibility of imposing prison sentences.
129. Legal persons whose liability is to be established in accordance with Article 12 shall also be subject to sanctions that are 'effective, proportionate and dissuasive', which can be criminal, administrative or civil in nature. Contracting Parties are compelled, under paragraph 2, to provide for the possibility of imposing monetary sanctions on legal persons.
130. The article leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences, for example, measures could include injunction or forfeiture. It leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems.

14 Article 14 – Scope of procedural provisions

14.1 Text of the Convention

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.
3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
i is being operated for the benefit of a closed group of users, and
ii does not employ public communications networks and is not connected with another computer system, whether public or private,
that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Artículo 14 – Ámbito de aplicación de las medidas de derecho procesal

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.
2. Salvo disposición en contrario, prevista en el artículo 21, las Partes podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:
a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;
b. a cualquier otra infracción penal cometida a través de un sistema informático; y
c. a la recogida de pruebas electrónicas de cualquier infracción penal.
3. a. Las Partes podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

i. es utilizado en beneficio de un grupo de usuarios cerrado, y

ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artigo 14º - Âmbito das disposições processuais

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento penal.

2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:

3. a) Às infracções penais em conformidade com o disposto nos artigos 2º a 11º da presente Convenção;

b) A outras infracções penais cometidas por meio de um sistema informático; e

c) À recolha de prova em suporte electrónico provas electrónicas de qualquer infracção penal.

a) Cada Parte pode reservar-se o direito de apenas aplicar as medidas referidas no artigo 20º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido do que o conjunto de infracções às quais aplica as medidas referidas no artigo 21º. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível da medida referida no Artigo 20º.

b) Nos casos em que uma Parte, devido a restrições impostas pela sua legislação em vigor no momento da adopção da presente Convenção, não puder aplicar as medidas referidas nos Artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que

i. Esteja em funcionamento para benefício de um grupo fechado de utilizadores, e

ii. Não utilize redes públicas de telecomunicações e não esteja em conexão com outro sistema informático, quer seja público ou privado,

essa Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível das medidas referidas nos Artigos 20º e 21º.

14.2 Explanatory report

Scope of procedural provisions (Article 14)

140. Each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal framework, to establish the powers and procedures described in this Section for the purpose of "specific criminal investigations or proceedings."

141. Subject to two exceptions, each Party shall apply the powers and procedures established in accordance with this Section to: (i) criminal offences established in accordance with Section 1 of the Convention; (ii) other criminal offences committed by means of a computer system; and (iii) the collection of evidence in electronic form of a criminal offence. Thus, for the purpose of specific criminal investigations or proceedings, the powers and procedures referred to in this Section shall be applied to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. This ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section. It ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data. The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.

142. There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Many States limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure. Likewise, this Convention only requires Parties to establish interception powers and procedures in relation to content data of specified computer communications in respect of a range of serious offences to be determined by domestic law.

143. Second, a Party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in Article 21. Some States consider the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness. The right of reservation would permit these States to limit the application of the measures to collect traffic data, in real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data. Many States, however, do not consider the interception of content data and the collection of traffic data to be equivalent in terms of privacy interests and degree of intrusiveness, as the collection of traffic data alone does not collect or disclose the content of the communication. As the real-time collection of traffic data can be very important in tracing the source or destination of computer communications (thus, assisting in identifying criminals), the Convention invites Parties that exercise the right of reservation to limit their reservation so as to enable the broadest application of the powers and procedures provided to collect, in real-time, traffic data.

144. Paragraph (b) provides a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention’s adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users and which do not use public communications networks nor are they connected with other computer systems. The term "closed group of users" refers, for example, to a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to

communicate amongst themselves using a computer network. The term "not connected with other computer systems" means that, at the time an order under Articles 20 or 21 would be issued, the system on which communications are being transmitted does not have a physical or logical connection to another computer network. The term "does not employ public communications networks" excludes systems that use public computer networks (including the Internet), public telephone networks or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users.

15 Article 15 – Conditions and safeguards

15.1 Text of the Convention

Article 15 – Conditions and safeguards

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

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.
2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.
3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Artigo 15º - Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações

Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros.

15.2 Explanatory report

Conditions and safeguards (Article 15)

145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005 [(4)], 009, 046, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.

146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that

the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.

147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation. Other safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

148. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.

16 Article 16 – Expedited preservation of stored computer data

16.1 Text of the Convention

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.

Artículo 16 – Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artigo 16º - Conservação expedita de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados

por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração.

2. Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controlo, esta Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

16.2 Examples

DOMINICAN REPUBLIC,
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.

Artículo 53.- Conservación de los Datos. Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

ROMANIA, ART.54 of Romania Law no 161/2003
(1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to

identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Art.54 de la Ley de Rumania núm. 161/2003

- En casos urgentes y debidamente justificados, si existen datos o indicaciones confirmadas relativas a la preparación o comisión de un delito penal por medio de sistemas informáticos, a efectos de obtener pruebas o de identificar a los delincuentes, puede ordenarse la conservación rápida de los datos informáticos o de los datos relativos al tráfico, que están en peligro de ser destruidos o alterados.
- La conservación será ordenada por el fiscal por conducto de una ordenanza motivada, a solicitud del órgano de investigación penal o *ex-officio* y, durante el juicio, por mandato judicial.
- La medida se ordena por un período que no excederá de 90 días y que podrá ser superado, sólo una vez, por un período que no excederá de 30 días.
- La ordenanza del fiscal o el mandato judicial se enviará, inmediatamente, a todo proveedor de servicios o toda otra persona que esté en posesión de los datos, y se obligará a la persona respectiva a conservar rápidamente los datos en condiciones de confidencialidad.

BARBADOS

20. (1) Where a police officer satisfies a Judge on the basis of an *ex parte* application that
(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk that the data may be destroyed or rendered inaccessible,
the Judge may make an order requiring the person in control of the computer system to ensure that the data specified in the order be preserved for a period of up to 14 days.
(2) The period may be extended beyond 14 days where, on an *ex parte* application, a Judge authorises an extension for a further specified period of time.

Barbados

20. 1) En los casos en que un agente de policía convenza a un Juez sobre la base de una solicitud ex parte acerca de que

a) los datos almacenados en un sistema informático serán solicitados razonablemente a los efectos de una investigación penal, y
b) existe el riesgo de que los datos sean destruidos o se hagan inaccesibles,

el Juez podrá emitir una orden que exija a la persona que controla el sistema informático conservar los datos especificados en la orden por un período de hasta 14 días.
2) El período podrá prolongarse más de 14 días, tras los cuales, sobre la base de una solicitud ex parte, el Juez autorizará una extensión por otro período específico de tiempo.

16.3 Explanatory report

Expedited preservation of stored computer data (Article 16)

158. Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceeding.

159. 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be 'frozen' (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data. The article does not specify how data should be preserved. It is left to each Party to determine the appropriate manner of preservation and whether, in some appropriate cases, preservation of the data should also entail its 'freezing'.

160. The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase 'or otherwise obtain' to permit these States to implement this article by the use of these means. However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases.

161. The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data. This can include any type of data that is specified in the order to be preserved. It can include, for example, business, health, personal or other records. The measures are to be established by Parties for use "in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." This can include situations where the data is subject to a short period of retention, such as where there is a business policy to delete the data after a certain period of time or the data is ordinarily deleted when the storage medium is used to record other data. It can also refer to the nature of the custodian of the data or the insecure manner in which the data is stored. However, if the custodian were untrustworthy, it would be more secure to effect preservation by means of search and seizure, rather than by means of an order that could be disobeyed. A specific reference to "traffic data" is made in paragraph 1 in order to signal the provisions particular applicability to this type of data, which if collected and retained by a service provider, is usually held for only a short period of time. The reference to "traffic data" also provides a link between the measures in Article 16 and 17.

162. Paragraph 2 specifies that where a Party gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person's possession or control". Thus, the stored data may actually be in the possession of the person or it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure." The domestic law of a Party should specify a maximum period of time for which data, subject to an order, must be preserved, and the order should specify the exact period of time that the specified data is to be preserved. The period of time should be as long as necessary, up to a maximum of 90 days, to permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or the issuance of a production order, to obtain the disclosure of the data.

A Party may provide for subsequent renewal of the production order. In this context, reference should be made to Article 29, which concerns a mutual assistance request to obtain the expeditious preservation of data stored by means of a computer system. That article specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 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."

163. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data.

164. In addition to the limitations set out above, the powers and procedures referred to in Article 16 are also subject to the conditions and safeguards provided in Articles 14 and 15.

17 Article 17 – Expedited preservation and partial disclosure of traffic data

17.1 Text of the Convention

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.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:
garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y
asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.
2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artigo 17º - Conservação expedita e divulgação parcial de dados de tráfego

1. A fim de assegurar a conservação de dados relativos ao trafego em aplicação do artigo 16º, cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para:
a) Assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços; e
b) Assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada.

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

17.2 Examples

DOMINICAN REPUBLIC,

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 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.

Artículo 56.- Proveedores de Servicios. Sin perjuicio de lo establecido en el literal b) del artículo 47 de la presente ley, los proveedores de servicio deberán conservar los datos de tráfico, conexión, acceso o cualquier otra información que pueda ser de utilidad a la investigación, por un período mínimo de noventa (90) días. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) creará un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en un plazo de 6 meses a partir de la promulgación de la presente ley. Dicha normativa deberá tomar en cuenta la importancia de preservación de la prueba, no obstante la cantidad de proveedores envueltos en la transmisión o comunicación.

ROMANIA, ART.54 of Romania Law no 161/2003

Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

BARBADOS

19. Where a Judge is satisfied on the basis of an *ex parte* application
by a police officer that specified data stored in a computer system

is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify
(a) the Internet service providers; and
(b) the path through which the communication was transmitted.

17.3 Explanatory report

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. The article does not specify the means by which this may be achieved, leaving it to domestic law to determine a means that is consistent with its legal and economic system. One means to achieve expeditious preservation would be for competent authorities to serve expeditiously a separate preservation order on each service provider. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other

service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.

18 Article 18 – Production order

18.1 Text of the Convention

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.

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y

a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;

cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Artigo 18º - Injunção

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:

a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

3. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

18.2 Examples

DOMINICAN REPUBLIC,

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:
Order a natural or legal person to supply information stored in an information or system in any of its component parts;

Artículo 54

Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las

siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de:
Ordenar a una persona física o moral la entrega de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;

ROMANIA, ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences

(2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1).

(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

BARBADOS

18. (1) Where a Judge is satisfied on the basis of an application
by a police officer that specified computer data or other information is
reasonably required for the purpose of a criminal investigation or
criminal proceedings, the Judge may order that
(a) a person in control of a computer system produce from the computer system specified computer data or other intelligible output of that data; and
(b) an Internet service provider in Barbados produce information
about persons who subscribe to or otherwise use the service.
(2) A person referred to in paragraph *(a)* or *(b)* of subsection (1)
who makes an unauthorised disclosure of any information under
his control is guilty of an offence and is liable on conviction on indictment,
(a) in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or
(b) in the case of a corporation, to a fine of $200 000.

18.3 Explanatory report

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control,

but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be

contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services.

19 Article 19 – Search and seizure of stored computer data

19.1 Text of the Convention

Article 19 – Search and seizure of stored computer data

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

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

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

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

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.

Artículo 19 – Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:
a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y
a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema

inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:
confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
realizar y conservar una copia de esos datos informáticos;
preservar la integridad de los datos informáticos almacenados pertinentes; y
hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.
4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.
5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artigo 19º - Busca e apreensão de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante:

a) A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e

A um suporte que permita armazenar dados informáticos.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que, nos casos em que as suas autoridades procedam a buscas ou acedam de forma semelhante a um sistema informático específico ou a uma parte do mesmo, em conformidade com o disposto no n.º 1, *a)*, e tenham razões para pensar que os dados procurados se encontram armazenados noutro sistema informático ou numa parte do mesmo situado no seu território, e que esses dados são legalmente acessíveis a partir do sistema inicial ou obteníveis a partir desse sistema inicial, as referidas autoridades estejam em condições de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relativamente aos quais o acesso foi realizado em aplicação dos n.ºs 1 ou 2. Essas medidas incluem as prerrogativas seguintes:

a) Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;
b) Realizar e conservar uma cópia desses dados informáticos;
c) Preservar a integridade dos dados informáticos pertinentes armazenados; e
d) Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.

4. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na medida do razoável as informações razoavelmente necessárias, para permitir a aplicação das medidas previstas nos n.ºs 1 e 2.

5. Os poderes e procedimentos referidos no presente artigos devem estar sujeitos aos artigos 14º e 15º.

19.2 Examples

DOMINICAN REPUBLIC,

Article 54.- Powers of the Public Prosecutor's Office.

b) Accede to or order access to such information system or to any of its 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;

Artículo 54.- Facultades del Ministerio Público.

a) Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;

b) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;

j) Recolectar o grabar los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;

ROMANIA LAW

Art.56 of Law 61/2003 – (1) Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.

(2) If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 55, paragraph (3).

(3) When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.

(4) The provisions of the Criminal Procedure Code regarding searches at home are applied accordingly.

508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences *(amended by Emergency Ordinance of Government no. 131/2006).*

ART. 16

(2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1).

(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

BARBADOS

15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

(2) A warrant issued under this section may authorise a police officer to *(a)* seize any computer, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed;

(b) inspect and check the operation of any computer referred to in paragraph *(a)*;

(c) use or cause to be used any computer referred to in paragraph *(a)* to search any programme or data held in or available to such computer;

(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer into readable and comprehensible format or text, for the purpose of investigating any offence under this Act;

(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;

(f) make and retain a copy of any programme or data held in the computer referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computers.

(3) A warrant issued under this section may authorise the rendering of assistance by an authorised person to the police officer in the execution of the warrant.

(4) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both.

(5) For the purposes of this section, "authorised person" means a person who has the relevant training and skill in computer systems and technology who is identified, in writing, by the Commissioner of Police or a gazetted officer designated by the Commissioner as authorised to assist the police; "encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data; "plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.

16. (1) A police officer executing a warrant in accordance with section 15 is entitled to require a person who is in possession or control of a computer data storage medium or computer system that is the subject of the search to assist him or an authorised person to *(a)* access and use a computer system or computer data storage medium to search any computer data available to or in the system;

(b) obtain and copy computer data referred to in paragraph *(a)*;
(c) use equipment to make copies;
(d) obtain access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence; and
(e) obtain an intelligible output from a computer system in a plain text format that can be read by a person.
(2) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both.
(3) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version.

17. (1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 15, the person who made the search shall, at the time of the search or as soon as practicable after the search,
(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and *(b)* give a copy of that list to
(i) the occupier of the premises; or
(ii) the person in control of the computer system.
(2) Subject to subsection (3), a police officer or authorised person shall, on request,
(a) permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or
(b) give the person referred to in paragraph *(a)*, a copy of the computer data.
(3) The police officer or authorised person may refuse to give access to or provide copies of computer data referred to in subsection
(2) if he has reasonable grounds for believing that giving the access or providing the copies
(a) would constitute a criminal offence; or
(b) would prejudice
(i) the investigation in connection with which the search was carried out; or
(ii) another investigation connected to the one in respect of which the search was carried out; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

19.3 Explanatory report

Search and seizure of stored computer data (Article 19)
184. This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.
185. In the traditional search environment concerning documents or records, a search involves gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and seize or physically take away the tangible record. The gathering of data takes place during the period of the search and in respect of

data that exists at that time. The precondition for obtaining legal authority to undertake a search is the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence of a specific criminal offence.

186. With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search are in respect of data that already exists and that will afford evidence of a specific offence.

187. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

188. Paragraph 1 requires Parties to empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette). As the definition of "computer system" in article 1 refers to "any device or a group of inter-connected or related devices", paragraph 1 concerns the search of a computer system and its related components that can be considered together as forming one distinct computer system (e.g., a PC together with a printer and related storage devices, or a local area network). Sometimes data that is physically stored in another system or storage device can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. This situation, involving linkages with other computer systems by means of telecommunication networks within the same territory (e.g., wide area network or Internet), is addressed at paragraph 2.

189. Although search and seizure of a "computer-data storage medium in which computer data may be stored" (paragraph 1 (b)) may be undertaken by use of traditional search powers, often the execution of a computer search requires both the search of the computer system and any related computer-data storage medium (e.g., diskettes) in the immediate vicinity of the computer system. Due to this relationship, a comprehensive legal authority is provided in paragraph 1 to encompass both situations.

190. Article 19 applies to stored computer data. In this respect, the question arises whether an unopened e-mail message waiting in the mailbox of an ISP until the addressee will download it to his or her computer system, has to be considered as stored computer data or as data in transfer. Under the law of some Parties, that e-mail message is part of a communication and therefore its content can only be obtained by applying the power of interception, whereas other legal systems consider such

message as stored data to which article 19 applies. Therefore, Parties should review their laws with respect to this issue to determine what is appropriate within their domestic legal systems.

191. Reference is made to the term 'search or similarly access'. The use of the traditional word 'search' conveys the idea of the exercise of coercive power by the State, and indicates that the power referred to in this article is analogous to traditional search. 'Search' means to seek, read, inspect or review data. It includes the notions of searching for data and searching of (examining) data. On the other hand, the word 'access' has a neutral meaning, but it reflects more accurately computer terminology. Both terms are used in order to marry the traditional concepts with modern terminology.

192. The reference to 'in its territory' is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level.

193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.

194. The Convention does not prescribe how an extension of a search is to be permitted or undertaken. This is left to domestic law. Some examples of possible conditions are: empowering the judicial or other authority which authorised the computer search of a specific computer system, to authorise the extension of the search or similar access to a connected system if he or she has grounds to believe (to the degree required by national law and human rights safeguards) that the connected computer system may contain the specific data that is being sought; empowering the investigative authorities to extend an authorised search or similar access of a specific computer system to a connected computer system where there are similar grounds to believe that the specific data being sought is stored in the other computer system; or exercising search or similar access powers at both locations in a co-ordinated and expeditious manner. In all cases the data to be searched must be lawfully accessible from or available to the initial computer system.

195. This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation.

196. Paragraph 3 addresses the issues of empowering competent authorities to seize or similarly secure computer data that has been searched or similarly accessed under paragraphs 1 or 2. This includes the power of seizure of computer hardware and computer-data storage media. In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier.

197. In this Convention, 'seize' means to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information. ‘Seize’ includes the use or seizure of programmes needed to access the data being seized. As well as using the traditional term 'seize', the term 'similarly secure' is included to reflect other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment. Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the ‘chain of custody’ of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data.

198. The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography. The term 'removal' is intended to express the idea that while the data is removed or rendered inaccessible, it is not

destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

199. Thus, seize or similarly secure data has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it. The seizure does not imply a final deletion of the seized data.

200. Paragraph 4 introduces a coercive measure to facilitate the search and seizure of computer data. It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

201. This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.

202. The information that can be ordered to be provided is that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

203. Under paragraph 5 of this article, the measures are subject to conditions and safeguards provided for under domestic law on the basis of Article 15 of this Convention. Such conditions may include provisions relating to the engagement and financial compensation of witnesses and experts.

204. The drafters discussed further in the frame of paragraph 5 if interested parties should be notified of the undertaking of a search procedure In the on-line world it may be less apparent that data has been searched and seized (copied) than that a seizure in the off-line world took place, where seized objects will be physically missing. The laws of some Parties do not provide for an obligation to notify in the case of a traditional search. For the Convention to require notification in respect of a computer search would create a discrepancy in the laws of these Parties. On the other hand, some Parties may consider notification as an essential feature of the measure, in order to maintain the distinction between computer search of stored data (which is generally not intended to be a surreptitious measure) and interception of flowing data (which is a surreptitious measure, see Articles 20 and 21). The issue of notification, therefore, is left to be determined by domestic law. If Parties consider a system of mandatory notification of persons concerned, it should be borne in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.

20 Article 20 – Real-time collection of traffic data

20.1 Text of the Convention

Article 20 – Real-time collection of traffic data

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

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

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

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:
a obtener o grabar con medios técnicos existentes en su territorio, y
a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:
a obtener o a grabar con medios técnicos existentes en su territorio, o
a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artigo 20º - Recolha em tempo real de dados relativos ao tráfego

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:

a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou

Prestar às autoridades competentes o seu apoio e assistência para recolher ou registar,

em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático.

2. Quando uma Parte, em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no nº 1, alínea *a)*, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo em tempo real dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

20.2 Examples

DOMINICAN REPUBLIC :
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;

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;

Artículo 54.- Facultades del Ministerio Público.

k) Solicitar al proveedor de servicios recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;

l) Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en el artículo 192 del Código Procesal Penal para la investigación de todos los hechos punibles en la presente ley;

ROMANIA

ART.54 of Romania Law no 161/2003
Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

20.3 Explanatory report

Real-time collection of traffic data
216. Often, historical traffic data may no longer be available or it may not be relevant as the intruder has changed the route of communication. Therefore, the real-time collection of traffic data is an important investigative measure. Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings.
217. Traditionally, the collection of traffic data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine the source or destination (e.g., telephone numbers) and related data (e.g., time, date and duration) of various types of illegal communications (e.g., criminal threats and harassment, criminal conspiracy, fraudulent misrepresentations) and of communications affording evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.).
218. Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text,

visual images and sound, it also has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Likewise, as computers can store vast quantities of data, often of a private nature, the potential for harm, whether economic, social or personal, can be significant if the integrity of this data is interfered with. Furthermore, as the science of computer technology is founded upon the processing of data, both as an end product and as part of its operational function (e.g., execution of computer programs), any interference with this data can have disastrous effects on the proper operation of computer systems. When an illegal distribution of child pornography, illegal access to a computer system or interference with the proper functioning of the computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, it is necessary and crucial to trace the route of the communications back from the victim to the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not more, important as it is in respect of purely traditional telecommunications. This investigative technique can correlate the time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.

219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified 'communications' are in the plural, as traffic data in respect of several communications may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The communications in respect of which the traffic data may be collected or recorded, however, must be specified. Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

220. Subject to paragraph 2, Parties are obliged, under paragraph 1(a) to ensure that their competent authorities have the capacity to collect or record traffic data by technical means. The article does not specify technologically how the collection is to be undertaken, and no obligations in technical terms are defined.

221. In addition, under paragraph 1(b), Parties are obliged to ensure that their competent authorities have the power to compel a service provider to collect or record traffic data or to co-operate and assist the competent authorities in the collection or recording of such data. This obligation regarding service providers is applicable only to the extent that the collection or recording, or co-operation and assistance, is within the existing technical capability of the service provider. The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems. However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability. For example, the system may be configured in such a manner, or computer programs may already be possessed by the service provider, which would permit such measures to be taken, but they are not ordinarily executed or used in the normal course of the service provider's operation. The article would require the service provider to engage or turn-on these features, as required by law.

222. As this is a measure to be carried out at national level, the measures are applied to the collection or recording of specified communications in the territory of the Party. Thus, in practical terms, the obligations are generally applicable where the service provider has some physical infrastructure or equipment on that territory capable of undertaking the measures, although this need not be the location of its main operations or headquarters. For the purposes of this Convention, it is understood that a communication is in a Party's territory if one of the communicating parties (human beings or computers) is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory.

223. In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a)). Likewise, an obligation under paragraph 1(b)(ii) to co-operate and assist the competent authorities in the collection or recording of traffic data is senseless if the competent authorities are not empowered to collect or record themselves the traffic data. Additionally, in the situation of some local area networks (LANs), where no service provider may be involved, the only way for collection or recording to be carried out would be for the investigating authorities to do it themselves. Both measures in paragraphs 1 (a) and (b) do not have to be used each time, but the availability of both methods is required by the article.

224. This dual obligation, however, posed difficulties for certain States in which the law enforcement authorities were only able to intercept data in telecommunication systems through the assistance of a service provider, or not surreptitiously without at least the knowledge of the service provider. For this reason, paragraph 2 accommodates such a situation. 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 a different approach, such as only compelling service providers to provide the necessary technical facilities, to ensure the real-time collection of traffic data by law enforcement authorities. In such case, all of the other limitations regarding territory, specificity of communications and use of technical means still apply.

225. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation. Service providers and their employees knowing about the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively.

226. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. This provision not only ensures the confidentiality of the investigation, but it also relieves the service provider of any contractual or other legal obligations to notify subscribers that data about them is being collected. Paragraph 3 may be effected by the creation of explicit obligations in the law. On the other hand, a Party may be able to ensure the confidentiality of the measure on the basis of other domestic legal provisions, such as the power to prosecute for obstruction of justice those persons who aid the criminals by telling them about the measure. Although a specific confidentiality requirement (with effective sanction in case of a breach) is a preferred procedure, the use of obstruction of justice offences can be an alternative means to prevent inappropriate disclosure and, therefore, also suffices to implement this paragraph. Where explicit obligations of confidentiality are created, these shall be subject to the conditions and safeguards as provided in Articles 14 and 15. These safeguards or conditions should impose reasonable time periods for the duration of the obligation, given the surreptitious nature of the investigative measure.

227. As noted above, the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15.

21 Article 21 – Interception of content data

21.1 Text of the Convention

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.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:

obtener o grabar con medios técnicos existentes en su territorio, y

obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:

obtener o grabar con medios técnicos existentes en su territorio, o

prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artigo 21º - Intercepção de dados relativos ao conteúdo

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes relativamente a um leque de infracções graves, a definir em direito interno, a:

a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

Recolher ou registar através da aplicação de meios técnicos no seu território, ou

Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar,

em tempo real, dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático.

2. Quando a Parte em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no n.º 1, alínea *a)*, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias, para assegurar a recolha ou o registo em tempo real dos dados relativos ao conteúdo associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

21.2 Examples

DOMINICAN REPUBLIC,
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 ;
Artículo 54.- Facultades del Ministerio Público.
d) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de Internet, a suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control ;

ROMANIA, ART.57 of Romania Law no 161/2003, ART. 91[1] (Section V[1]) of the Criminal Procedure Code on audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication
Art.57 – (1) The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find

the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence.
(2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.
(3) The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.
(4) Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.
(5) The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

ART. 91[1]

Conditions and cases of interception and recording of conversations or communications by telephone or by any other electronic means of communication

The interception and recording of conversations or communications by telephone or by any electronic means of communication are performed with the reasoned authorisation of a judge, at the request of the public prosecutor who is conducting or supervising criminal prosecution, under the law, in the event that solid data or clues indicate the preparation or perpetration of a criminal offence for which criminal prosecution is conducted ex officio, and interception and recording are required in order to establish the factual situation or because it would be impossible to identify or locate the participants by any other means or such means would cause much delay to the investigation.

Interception and recording of conversations or communications by telephone or by any electronic means of communication may be authorised for criminal offences against national security, as set forth in the Criminal Code and in other special laws, as well as for criminal offences of drug trafficking, weapons trafficking and trafficking in persons, terrorist acts, money laundering, counterfeiting of currency or other valuables, for the criminal offences set forth in Law No.78/2000 on the Prevention, Detection and Punishment of Acts of Corruption, as subsequently amended and supplemented, and for other serious criminal offences or criminal offences that are perpetrated through means of electronic communication. Para. 1 shall apply accordingly.

Authorisation shall be given for the period of time during which interception and recording is needed, however not for more than 30 days, in private by the president of the court that would be competent to try the case in first instance or of the court of the same rank that has jurisdiction over the prosecution office where the public prosecutor works who is conducting or supervising criminal prosecution. In the absence of the president of the court, the authorisation shall be given by a judge designated by the court president.

Such authorisation may be renewed, either before or after the previous one expires, but under the same conditions and for properly justified reasons. However, each extension may not exceed 30 days.

The total duration of authorised interception and recording, with regard to the same person and the same act may not exceed 120 days.

Recording of conversations between a lawyer and the party whom he is representing or assisting within the proceedings may not be used as evidence unless it contains or leads to the establishment of conclusive and useful data or information regarding the preparation or commission by the lawyer of a criminal offence of those provided in para. 1 and 2.

The public prosecutor ordains immediate cessation of interceptions and recordings before the expiry of the authorisation if the reasons that justified such measures no longer exist, and shall inform about this the law court that issued the authorisation.

At the reasoned request of the injured person, the public prosecutor may request authorisation from the judge to intercept and record conversations or communications by the injured person by telephone or by any electronic means of communication, whatever the nature of the criminal offence under investigation.

Interception and recording of conversations or communications shall be authorised by means of a reasoned order, which must include: the actual clues and facts that justify the measure; the reasons for which it would be impossible to determine the factual situation or to identify or locate the participants by other means or the reasons why the investigation would be very much delayed; the person, the means of communication or the place that is subject to recording; and the period for which interception and recording are authorised.

21.3 Explanatory report

Interception of content data

228. Traditionally, the collection of content data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or fraudulent misrepresentations) and to collect evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.). Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Many of the computer crimes involve the transmission or communication of data as part of their commission; for example, communications sent to effect an illegal access of a computer system or the distribution of computer viruses. It is not possible to determine in real-time the harmful and illegal nature of these communications without intercepting the content of the message. Without the ability to determine and prevent the occurrence of criminality in progress, law enforcement would merely be left with investigating past and completed crimes where the damage has already occurred. Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications.

229. 'Content data' refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything transmitted as part of the communication that is not traffic data.

230. Most of the elements of this article are identical to those of Article 20. Therefore, the comments, above, concerning the collection or recording of traffic data, obligations to co-operate and assist, and obligations of confidentiality apply equally to the interception of content data. Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'.

231. Also, as set forth in the comments above on Article 20, the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data.

Chapter III – International co-operation

29 Article 29 – Expedited preservation of stored computer data

29.1 Text of the Convention

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.

7 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.

Artículo 29 – Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

a. la autoridad que solicita la conservación;
b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
e. la necesidad de la medida de conservación; y
f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por

un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

Artigo 29º - Conservação expedita de dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte que ordene ou obtenha de outra forma a conservação rápida dos dados armazenados por meio de um sistema informático, que se encontre no território dessa outra Parte, e relativamente aos quais a Parte requerente pretenda apresentar um pedido de auxílio mútuo para fins de busca ou de acesso similar, apreensão ou obtenção por meio similar, ou divulgação dos dados.

2. Um pedido de conservação efectuado nos termos do n.º 1 deve especificar:

a) A autoridade que pede a conservação;

b) A infracção que é objecto de investigação criminal ou de procedimento e uma breve exposição dos factos relacionados;

c) Os dados informáticos armazenados a conservar e a sua relação com a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;

e) A necessidade da medida de conservação; e

f) Que a Parte tenciona apresentar um pedido de assistência mútua com vista à busca ou outra forma de acesso, apreensão ou obtenção semelhante, ou divulgação dos dados informáticos armazenados.

3. Após ter recebido o pedido de outra Parte, a Parte requerida deve tomar as medidas apropriadas a fim de proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para poder responder a esse pedido, a dupla incriminação não é exigida como condição prévia à conservação.

4. Uma Parte que exija a dupla incriminação como condição necessária para responder a um pedido de auxílio mútuo para fins de busca ou acesso semelhante, apreensão ou obtenção por meio semelhante, ou a divulgação dos dados, pode, no que diz respeito a outras infracções diferentes das estabelecidas em conformidade com os artigos 2º a 11º da presente Convenção, reservar-se o direito de recusar o pedido de conservação ao abrigo do presente artigo, se tiver razões para crer que no momento da divulgação, a condição de dupla incriminação não pode ser preenchida.

5. Além disso, um pedido de conservação só pode ser recusado se:

a) O pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou

b) A Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

6. Quando a Parte requerida considerar que a simples conservação não é suficiente para garantir a disponibilidade futura dos dados, e comprometerá a confidencialidade da investigação da Parte requerente, ou prejudica de outra forma a mesma, informará prontamente disso a Parte requerente que decidirá, então, se o pedido deve, ainda assim, ser executado.

7. Qualquer conservação efectuada em resposta a um pedido referido no n.º 1 será válida por um período não inferior a 60 dias, a fim de permitir à Parte requerente apresentar um pedido para fins de busca ou acesso semelhante, apreensão ou obtenção semelhante, ou divulgação dos dados. Após a recepção desse pedido, os dados devem continuar a ser conservados até à adopção de uma decisão respeitante ao pedido.

29.2 Examples

ROMANIA, ART.63 of Romania Law no 161/2003
Art. 63 - (1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters.
(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation;
b) a brief presentation of facts that are subject to the criminal investigation and their legal background;
c) computer data required to be preserved;
d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;
e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;
(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

29.3 Explanatory report

Expedited preservation of stored computer data
282. This article provides for a mechanism at the international level equivalent to that provided for in Article 16 for use at the domestic level. Paragraph 1 of this Article authorises a Party to make a request for, and paragraph 3 requires each Party to have the legal ability to obtain, the expeditious preservation of data stored in the territory of the requested Party by means of a computer system, in order that the data not be altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data. Preservation is a limited, provisional measure intended to take place much more rapidly than the execution of a traditional mutual assistance. As has been previously discussed, computer data is highly volatile. With a few keystrokes, or by operation of automatic programs, it may be deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. Thus, it was agreed that

a mechanism was required in order to ensure the availability of such data pending the lengthier and more involved process of executing a formal mutual assistance request, which may take weeks or months.

283. While much more rapid than ordinary mutual assistance practice, this measure is at the same time less intrusive. The mutual assistance officials of the requested Party are not required to obtain possession of the data from its custodian. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the issuance of process requiring it to be turned over to law enforcement officials at a later stage. This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. At the same time, a requested Party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost.

284. Paragraph 2 sets forth the contents of a request for preservation pursuant to this Article. Bearing in mind that this is a provisional measure and that a request will need to be prepared and transmitted rapidly, the information provided will be summary and include only the minimum information required to enable preservation of the data. In addition to specifying the authority that is seeking preservation and the offence for which the measure is sought, the request must provide a summary of the facts, information sufficient to identify the data to be preserved and its location, and a showing that the data is relevant to the investigation or prosecution of the offence concerned and that preservation is necessary. Finally, the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain production of the data.

285. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. In general, application of the principle of dual criminality is counterproductive in the context of preservation. First, as a matter of modern mutual assistance practice, there is a trend to eliminate the dual criminality requirement for all but the most intrusive procedural measures, such as search and seizure or interception. Preservation as foreseen by the drafters, however, is not particularly intrusive, since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed to or examined by officials of the requested Party until after execution of a formal mutual assistance request seeking disclosure of the data. Second, as a practical matter, it often takes so long to provide the clarifications necessary to conclusively establish the existence of dual criminality that the data would be deleted, removed or altered in the meantime. For example, at the early stages of an investigation, the requesting Party may be aware that there has been an intrusion into a computer in its territory, but may not until later have a good understanding of the nature and extent of damage. If the requested Party were to delay preserving traffic data that would trace the source of the intrusion pending conclusive establishment of dual criminality, the critical data would often be routinely deleted by service providers holding it for only hours or days after the transmission has been made. Even if thereafter the requesting Party were able to establish dual criminality, the crucial traffic data could not be recovered and the perpetrator of the crime would never be identified.

286. Accordingly, the general rule is that Parties must dispense with any dual criminality requirement for the purpose of preservation. However, a limited reservation is available under paragraph 4. If a Party requires dual criminality as a condition for responding to a request for mutual assistance for production of the data, and if it has reason to believe that, at the time of disclosure, dual criminality will not be satisfied, it may reserve the right to require dual criminality as a precondition to preservation. With respect to offences established in accordance with Articles 2 through 11, it is assumed that the condition of dual criminality is automatically met between the Parties, subject to any reservations they may have entered to these offences where permitted by the Convention. Therefore,

Parties may impose this requirement only in relation to offences other than those defined in the Convention.

287. Otherwise, under paragraph 5, the requested Party may only refuse a request for preservation where its execution will prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. Due to the centrality of this measure to the effective investigation and prosecution of computer- or computer-related crime, it was agreed that the assertion of any other basis for refusing a request for preservation is precluded.

288. At times, the requested Party will realise that the custodian of the data is likely to take action that will threaten the confidentiality of, or otherwise prejudice, the requesting Party's investigation (for example, where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of the investigation himself). In such situations, under paragraph 6, the requesting Party must be notified promptly, so that it may assess whether to take the risk posed by carrying through with the request for preservation, or to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.

289. Finally, paragraph 7 obliges each Party to ensure that data preserved pursuant to this Article will be held for at least 60 days pending receipt of a formal mutual assistance request seeking the disclosure of the data, and continue to be held following receipt of the request.

30 Article 30 – Expedited disclosure of preserved traffic data

30.1 Text of the Convention

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.

Artículo 30 – Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Artigo 30º - Divulgação expedita dos dados de tráfego conservados

1. Se ao executar um pedido de conservação de dados relativos ao tráfego relacionados com uma comunicação específica efectuada em aplicação do artigo 29º, a Parte requerida descobrir que um fornecedor de serviços noutro Estado participou na transmissão dessa comunicação, a Parte requerida divulgará rapidamente à Parte requerente uma quantidade suficiente de dados relativos ao tráfego que permita identificar esse fornecedor de serviços e a via através da qual a comunicação foi transmitida.

2. A divulgação de dados de tráfego nos termos do disposto no n.º 1 apenas pode ser recusada se:

a) Se o pedido respeitar a uma infracção considerada pela Parte requerida como infracção de natureza política ou com ela conexa; ou
b) Se a Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

30.2 Examples

ROMANIA, ART.64 of Romania Law no 161/2003
Art.64 - If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

30.3 Explanatory report

Expedited disclosure of preserved traffic data (Article 30)
290. This article provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting Party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.
291. Under Paragraph 2, the requested Party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 29 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.

31 Article 31 – Mutual assistance regarding accessing of stored computer data

31.1 Text of the Convention

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.

Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.

2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.

3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o

b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

Artigo 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29º.

2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, acordos e legislação referida no artigo 23º, e dando cumprimento às disposições pertinentes do presente Capítulo.

3. O pedido deve ser satisfeito o mais rapidamente possível nos casos em que:

a) Existam motivos para crer que os dados relevantes são especialmente vulneráveis à perda ou modificação; ou

b) Os instrumentos, acordos e legislação referida no n.º 2 prevejam uma cooperação rápida.

31.2 Examples

ROMANIA, ART. 60 of Romania Law no 161/2003
Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.
(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

24.3 Explanatory report

Mutual assistance regarding accessing of stored computer data (Article 31)
292. Each Party must have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory - just as under Article 19 (Search and seizure of stored computer data) it must have the ability to do so for domestic purposes. Paragraph 1 authorises a Party to request this type of mutual assistance, and paragraph 2 requires the requested Party to be able to provide it. Paragraph 2 also follows the principle that the terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters. Under paragraph 3, such a request must be responded to on an expedited basis where (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or (2) otherwise where such treaties, arrangements or laws so provide.

32 Article 32 – Trans-border access to stored computer data with consent or where publicly available

32.1 Text of the Convention

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.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o

b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artigo 32º - Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

32.2 Examples

ROMANIA, ART.65 of Romania Law no 161/2003
Art.65 - (1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities.
(2) A competent foreign authority can have access and can receive, by means of a computer system located on its territory, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law, to make them available by means of that computer system, without requesting the Romanian authorities.

32.3 Explanatory report

Transborder access to stored computer data with consent or where publicly available
293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.
294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person’s e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

33 Article 33 – Mutual assistance in the real-time collection of traffic data

33.1 Text of the Convention

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.

Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.

2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

Artigo 33º - Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real

1. As Partes concederão entre si o auxílio mútuo no que diz respeito à recolha, em tempo real, de dados de tráfego associados a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º2, esse auxílio regular-se-à pelas condições e procedimentos previstos em direito interno.

2. Cada Parte concederá o auxílio pelo menos no que diz respeito às infracções penais relativamente às quais seria possível a recolha ao nível interno a recolha em tempo real dos dados de tráfego em caso semelhante.

33.2 Examples

ROMANIA, ART. 60 of Romania Law no 161/2003

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.

(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

33.3 Explanatory report

Mutual assistance regarding the real-time collection of traffic data (Article 33)

295. In many cases, investigators cannot ensure that they are able to trace a communication to its source by following the trail through records of prior transmissions, as key traffic data may have been automatically deleted by a service provider in the chain of transmission before it could be preserved. It is therefore critical for investigators in each Party to have the ability to obtain traffic data in real time regarding communications passing through a computer system in other Parties. Accordingly, under Article 33 (Mutual assistance regarding the real-time collection of traffic data), each Party is under the obligation to collect traffic data in real time for another Party. While this Article requires the Parties to co-operate on these matters, here, as elsewhere, deference is given to existing modalities of mutual assistance. Thus, the terms and conditions by which such co-operation is to be provided are generally those set forth in applicable treaties, arrangements and laws governing mutual legal assistance in criminal matters.

296. In many countries, mutual assistance is provided broadly with respect to the real time collection of traffic data, because such collection is viewed as being less intrusive than either interception of content data, or search and seizure. However, a number of States take a narrower approach. Accordingly, in the same way as the Parties may enter a reservation under Article 14 (Scope of procedural provisions), paragraph 3, with respect to the scope of the equivalent domestic measure, paragraph 2 permits Parties to limit the scope of application of this measure to a more narrow range of offences than provided for in Article 23 (General principles relating to international co-operation). One caveat is provided: in no event may the range of offences be more narrow than the range of offences for which such measure is available in an equivalent domestic case. Indeed, because real time collection of traffic data is at times the only way of ascertaining the identity of the perpetrator of a crime, and because of the lesser intrusiveness of the measure, the use of the term "at least" in paragraph 2 is designed to encourage Parties to permit as broad assistance as possible, i.e., even in the absence of dual criminality.

34 Article 34 – Mutual assistance regarding the interception of content data

34.1 Text of the Convention

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.

Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Artigo 34º - Auxílio mútuo em matéria de intercepção de dados de conteúdo

As Partes concederão auxílio judiciário mútuo, na medida em que é permitido pelos tratados e pelas legislações aplicáveis no que diz respeito à recolha ou ao registo, em tempo real, de dados relativos ao conteúdo de comunicações específicas transmitidas por meio de um sistema informático.

34.2 Examples

ROMANIA, ART. 60 of Romania Law no 161/2003

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.

(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

34.3 Explanatory report

Mutual assistance regarding the interception of content data (Article 34)

297. Because of the high degree of intrusiveness of interception, the obligation to provide mutual assistance for interception of content data is restricted. The assistance is to be provided to the extent permitted by the Parties' applicable treaties and laws. As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, it was decided to defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist. In this regard, reference is made to the comments on Articles 14, 15 and 21 as well as to N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications.

35 Article 35 – 24/7 Network

35.1 Text of the Convention

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.

Artículo 35 – Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;
b. conservación de datos, de conformidad con los artículos 29 y 30; y
c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

Artigo 35º - Rede 24/7

1. Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:

   a) A prestação de aconselhamento técnico;

   b) A conservação de dados em conformidade com os artigos 29º e 30º; e

   c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.

2. a) O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida;

   b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.

3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.