Project on Cybercrime
www.coe.int/cybercrime

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

Version 12 March 2008

Discussion paper (draft)

National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices

Prepared by

Prof. Dr. Lorenzo Picotti
(Scientific Coordinator)
Professor of Criminal Law and
Criminal Information Law
University of Verona - Italy

Ivan Salvadori
University of Verona- Italy

This discussion paper has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:
Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France
Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Contents

1 Introduction

1.1 Purpose of the study

On 22 November 2001 the Convention on Cybercrime (CoC) - prepared by the Council of Europe with the participation of Canada, Japan, South Africa and the USA - was opened for signature in Budapest (Hungary). It entered into force in July 2004. By 1 March 2008, it had been ratified by 22 states and signed by another 21. In addition, Costa Rica and Mexico had been invited to accede.[1] Many others are reforming their legislation using the Convention as a guideline.

The CoC undoubtedly represents the most important international instrument in the fight against cybercrime.[2]

Cybercrime is a global offence and needs a global answer.[3] "Data heavens" in fact represent the greatest threat against security in the information society.[4] Attacks against critical infrastructure can be carried out from countries lacking cybercrime regulations, implying serious problems of jurisdiction.[5]

It is highly recommended that the majority of countries implement and accede to the CoC. It is therefore highly recommended that non-European countries are also encouraged to apply for accession to this Convention, in line with Article 37 of this treaty. The full implementation the CoC by a broad range of countries would permit effective harmonisation of computer crime and cybercrime legislation, of the investigative powers in the electronic environment and international co-operation.[6]

The Convention sets standards that can be adjusted to the specific needs of a given country. Thus, not all the countries have implemented the provisions of the CoC in the same way. This raises questions with regard to actual harmonisation of criminal law, but also of full compliance with the provisions of the Convention. Some of the national provisions - especially with regard to substantive criminal law – fulfil the requirements of the CoC, while some others have not yet met all the requirements.

The present study is meant as a resource for countries in the process of strengthening their national legislation against cybercrime in line with the CoC. It will also feed into the work of the Cybercrime Convention Committee (T-CY) of the Council of Europe.

It is a discussion paper prepared by independent researchers. The views expressed are thus not necessarily those of the Council of Europe.

---

1 See www.coe.int/cybercrime for a link to the Convention including the database on signatures and ratifications.

2 Miquelon M.F., 'The Convention on Cybercrime: an Harmonized Implementation of International Penal Law: What Prospects for', (23) 2005 J. Marshall J. Computer & Info. L., p. 329.; Gerke M., *The Convention on cybercrime*, MMR, 2004; Sarzana C., 'La Convenzione europea sulla cibercriminalità', in *Dir. pen. e proc.*, 2002, p. 509.; ID., *Informatica, Internet e diritto penale*, 2003, p. 403.

3 See Picotti L. (ed.), *Computer crimes and cyber crimes: global offences, global answers* (forthcoming); Guymon C.D., 'International legal mechanisms for combating transnational organized crime: the need for a multilateral convention', (18) 2000 *Berkeley J. Int'l L.*, p. 53.; Zakaras M., 'International computer crimes', *Revue internationale de droit penal*, 2001, p. 813.

4 Sieber U., *The International Handbook on Computer Crime*, 1986, Xiii; Sussman M.A., 'The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium', (9) *1999 Duke J. Comp. & Int'l. L.*, p. 453.

5 Brenner S.W., Koops B-J. (ed.), *Cybercrime and jurisdiction. A global survey*, 2006; Perisco B.A., 'Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure', (7) *1999 Com. Con.*, p. 153.

6 See Picotti L. (ed.), *Computer crimes and cyber crimes: global offences, global answers*. (forthcoming).

1.2 Methodology

The present study, ordered by the Council of Europe, consists of a comparative review of cybercrime legislations of 22 European and 9 non-European countries, based on legislative profiles and studies provided by the Council of Europe, including translations of laws attached to these documents.[7] Nevertheless, the present study should be able to raise issues and trigger further debates and reviews.

The aim of the study is firstly to analyse not only the substantive criminal law provisions, but also the procedural and international co-operation law provisions of these countries, pointing out their compatibility with the CoC. Secondly, it is to underline the differences in the ratification process, including some recommendations *de lege ferenda*, where necessary.

In order to simplify the analysis and the comparison of the various national legislations, each section is preceded by a short description of the dogmatic structure of the offences and procedural law provisions. Each description is concise, so as to ensure brevity, clarity, and usefulness for both state legislators and private users.

Each section is complemented by a practical table showing which European and non-European countries that already implemented the provisions of Cybercrime Convention.

With regard to the summarising table, more precise information is necessary. Sometimes the domestic law provisions seem to not be formally consistent with the CoC recommendations, but in some instances (in particular with regard to common law countries) case law and the interpretation of provisions by judges bring the law more in line with CoC than one would assume from the analysis on the legislation. For this reason the mentioned classification is mainly a recommendation for further analysis and seeks to give a picture of the current process of the implementation of the CoC at a domestic level.

A short analysis of each criminal offence provided by the CoC is included, concerning whether and how the computer and computer-related offences provided for by the Cybercrime Convention are covered, outlining the main differences between the countries and the objective (*actus reus*) and mental elements (*mens rea*) which are particularly problematic.

1.3 Countries covered

The study proposes an analysis of cybercrime provisions in the national legislations of 22 European countries and nine non-European countries against the provisions of the CoC. The European countries analysed are the following: Austria, Albania, Armenia, Bulgaria, Croatia, Czech Republic, Estonia, Latvia, Lithuania, France, Germany, Hungary, Italy, The Netherlands, Portugal, Romania, Serbia, Slovakia, "the former Yugoslav Republic of Macedonia", Turkey, Ukraine and United Kingdom. As for the nine non-European countries, the study considers current or draft legislation in Australia, Brazil, Egypt, India, Mexico, the Philippines, South Africa, Sri Lanka and the United States of America.

Three countries that have good practices to share have been looked at in more detail in this study, namely France, Germany and Romania. France and Romania have recently ratified the CoC,[8] while ratification by Germany is expected shortly.

The cybercrime legislation of France, Germany and Romania constitute good examples with regard to the most relevant issues related to the implementation of the CoC offences.

---

[7] Obviously, a full review of domestic legislation and its effectiveness would also require analyses of case law and help from local scholars and experts.

[8] France has ratified the CoC on 10.01.2006; Romania has ratified the CoC on 12.05.2004.

1.3.1 Summary description of cybercrime legislation in France

France signed the Convention on Cybercrime on 23 November 2001 and ratified it on 10 January 2006 with Law No. 297/2007 (5 March 2007).

Even before the ratification of the CoC it had already implemented some cybercrime offences. The first law (loi "Godfrain") concerning computer fraud (*fraude informatique*) was adopted in 1988.[9] The French Parliament has successively passed other important laws, in particular Law No. 1062/2002 "*pour la securité quotidienne*" and Law No. 204/2004 "*portant adaptation de la justice aux evolutions de la criminalité*".

Nowadays the majority of computer crime and cybercrime offences are within the Penal Code, chapter III concerning, "*atteintes aux système de traitment automatisé de données*". Nevertheless, even though France has ratified the CoC, its legislation does not expressly cover all the provisions provided for by the Cybercrime Convention. France does not have for example any specific provision regarding computer forgery and computer fraud. Nevertheless, these two offences seem to fall within the scope of the traditional provisions of forgery and fraud.

French cybercrime legislation is at the forefront of the fight against new cyber threats, criminalising illegal acts such as hacking (Article 321-1 CP), cracking (Article 323-1 CP) and the input of malicious codes causing a modification of data (Article 323-3 CP). The installation of illegal programs as spyware or key-logger can be punished by Article 225.15, paragraph 2, Criminal Code. Nevertheless any provision seems applicable to data theft. Identity theft could be covered partially by Article 434-23, Code penal (*usurpation d'identit*é).[10] With regard to these dangerous menaces, it is advisable that the legislator introduces specific provisions.

One of the most significant problems in France nowadays is represented by spam or unsolicited commercial e-mail.[11] In order to reduce the menace to the privacy and correct functioning of the computer systems and networks, the French legislator has approved the Law No. 575/2004 "*pour la confiance dans l'économie numérique"* (21 June 2004). Article 34 and 35 of Law No. 575/2004 punish with imprisonment up to two years or a fine the diffusion of unsolicited e-mails on the Internet. In order to facilitate the possibility to file a complaint against the spammer, the French law has simplified the procedure.

With regard to the criminal procedure law, French legislation does not expressly cover all the provisions provided for by the CoC. Nevertheless, it does not mean that French criminal procedure law is not consistent with the CoC, as it seems to be covered by general provisions of French criminal procedure law referring to the bilateral agreements or international conventions.

1.3.2 Summary description of cybercrime legislation in Germany

Germany has signed the Convention on Cybercrime on 23 November 2001 and is expected to ratify shortly. German law largely complies not only with the requirements of the CoC, but

---

[9] Law No. 88-19/1988. For a comment see Feral-Schuhl C., *Cyberdroit, Le droit a l'epreuve de l'Internet*, p. 596; Verbiest T., Wery E., *Le droit de l'Internet et de la societè de l'information*, p. 38.

[10] Article 434-23 Code Penal: "*Le fait de prendre nom d'un tiers, dans des circonstances qui ont determine ou auraient pur determiner contre celui-ci des poursuites pènales, est puni de cinq ans d'emprisonnement et de 75000 euros d'amende*". About identity theft see also Gercke M., *Internet-related identity theft* (a discussion paper), available on www.coe.int/cybercrime.

[11] For a definition of spam see CNIL: "*l'envoi massif et parfois rèpète de courier èlectronique non sollicitè. Le plus souvent à caractere commercial à des personnes avec lesquelles l'expèditeur n'a jamais eu de contact et don't il a captè l'adresse èlectronique dans les espaces public de l'Internet*".

also with the EU Framework Decision on attacks against information systems. With the recent Law, on 11 August 2007, the German legislator with Law No. 1786/2007 (*Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität in Kraft*) has in fact modified some cybercrime provisions (i.e. § 202a StGB; § 202b StGB: § 202c StGB) and introduced new provisions against cybercrime in the German Criminal Code (StGB).[12]

The majority of German cybercrime offences are consistent with the CoC. In particular, the provisions concerning illegal interception, data interference, computer fraud and copyright infringements fully comply with the requirements established by the CoC. A review could take into consideration only with regard to illegal access (Sec. 202(2)StGB) and misuse of devices (Sec. 202c StGB).

The German cybercrime legislation covers a lot of new menaces committed though information technologies. Phishing is covered by Sec. 202a, 202c and 269 StGB.[13] Spamming can be covered by Sec. 265a and 317 StGB.[14] Diffusion of malicious code is covered by Sec. 303a, 303b StGB and the installation of "*Trojanische Pferde*" (Trojan horse) by Sec. 202a StGB.[15]

Nevertheless, the German legislation does not seem to cover identity theft. Therefore it is advisable that the legislator introduces a specific provision.

With regard to the criminal procedure law, German legislation does not expressly cover all the provisions provided for by the CoC. Nonetheless, it does not mean that its criminal procedure law is not consistent with the CoC. In the majority of the cases where there is any specific provision, general provisions of criminal procedure law referring to the bilateral agreements or international conventions can be applied.

1.3.3 Summary description of cybercrime legislation in Romania

Romania signed the Convention on Cybercrime on 23 November 2001 and ratified it on 12 May 2004. Before ratification of the CoC, Romania implemented all the provisions of the CoC with Law No. 161/2003. Most of the European countries, such as Italy, Germany or Spain, have placed the computer related offences close to the traditional offences, taking their structure as a model for the new cybercrime provisions. In the absence of traditional offences where the new criminal phenomena connected to the new technologies can be included, Romania has created specific cybercrime offences without any relationship to the traditional provisions.[16] In the formulation of the criminal offences, the Romanian legislator has taken all the provisions of the CoC as model. As a result of this choice, Romania today has modern cybercrime legislation completely consistent with the provisions of the CoC. Its criminal legislation against cybercrime is undoubtedly a very useful model of good practice that can be taken into consideration by those countries that do not yet have specific provisions against cybercrime.

With regard to the criminal procedure law, Romanian legislation expressly covers almost all the provisions provided for by the CoC. An example of full alignment are the provisions concerning the "expedited preservation of stored computer data", "search and seizure of stored computer data", "real-time collection of data", or the provisions concerning mutual assistance that comply with the requirements of Articles 25-28 CoC.

---

[12] 'Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität' in *Kraft BGBl I*, p. 1786; for a comment see Ernst S., *Das neue Computerstrafrecht*, NJW, 2007, p. 2661.

[13] Ernst S., *Das neue Computerstrafrecht*, NJW, 2007, p. 2665. About phishing see also Knupfer, *Phishing for Money*, MMR, 2004, p. 641; Hilgendorf E., Frank T., Valerius B., *Computer-und Internetstrafrecht*, p. 205.

[14] Hilgendorf, etc., op cit., p. 199. FRANK T., Zur Strafrechtlichen Bewältigung des Spamming, 2004.

[15] Heinrich B., *Aktuelle Probleme des Internetstrafrechts*, op. cit.

[16] The choice of the legislator in the case of Cyprus is identical. See Cyprus Law No. 22(III)04.

2 Comparative analysis of the use of terms

> Article 1 CoC
> 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.

The first chapter of the Cybercrime Convention is devoted to the use of some relevant technical and legal terms. It defines four important and widely employed terms, namely *computer system*, *computer data*, *service provider* and *traffic data.*[17] They are frequently used in the description of cybercrime offences of all national legislations and some of them, in particular the concepts of *computer system* and *computer data* defined by the CoC, are similar to the definitions offered by Article 1 of the European Union Framework Decision on attacks against information systems.[18]

The Parties are not bound to adopt the same identical definitions of the CoC into their domestic laws.[19] They have the discretional power to decide the way to implement such concepts, but it must be consistent with the principles fixed by Article 1 CoC.

Not all the countries that have ratified the CoC have introduced these definitions.[20]

A definition of *computer system* has been introduced in the domestic law of the majority of the countries.[21] For a computer system to exist, the majority of the legislations analysed require that a device or a group of interconnected or related devices performs, pursuant to a program, automatic processing of data. In some states there is a dangerous lack of a general definition of computer.[22] This poses new difficulties in determining the types of computer

---

[17] For an explanation of these terms, see the Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. The definition of a computer system furnished by Article 1(a) EU Framework decision on Attacks against Information Systems is similar. See footnote No. 18. EU Framework Decision defines also other concepts, such as "legal person" and "without right".

[18] According to Article 1 EU Framework Decision on Attacks against Information Systems 'computer data' means "any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function"; 'information system' means "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance".

[19] Explanatory Report, 22.

[20] i.e. Albania, Armenia, Croatia, Estonia, France, "the former Yugoslav Republic of Macedonia", Hungary, Lithuania, Ukraine and Slovakia.

[21] Austria (Sec. 74, para 8 PC); Bulgaria (Article 93, items 21 PC), Cyprus (Article 2 Law. 22(III)04), The Netherlands (Article 80sexies CC), Portugal (Article 2 Law. No. 109/91). Romania (Article 35a) Law 161/2003), India (Sec. 2, subsection 1, l) ITA) or United States (Title 18, § 1030(e) US Code).

[22] i.e. Italy, France or Australia.

systems, computer and traffic data, as service providers to be included. For example, we can think of modern mobile phones which support Internet access or other optical, electrochemical, and high speed data processing devices.

A wide range of other terms are also employed in the CoC in the definitions of specific criminal acts, such as the term "child pornography" (Article 9, paragraph 2 CoC). Nevertheless, others are not defined anymore precisely in the CoC.[23] Very few countries define all the concepts provided for by Article 1 CoC.

A good model of full alignment with Article 1 CoC is represented by Article 2 of Cyprus Law No. 22 (III) 04[24], or Article 93, items 21,22,23 of the Bulgarian Penal Code and § 1(2) of the Bulgarian Penal Procedure Code.[25]

Completely consistent with Article 1 CoC is also Article 35 of Romanian Law No. 161/2003.[26] The Romanian provision goes beyond even Article 1 CoC, defining not only the concepts of "computer system", "computer data", "service provider" and "traffic data" as provided by Article 1 CoC, but also "computer program", "data of the users", "security measures", "pornographic materials with minors", and "without right".

---

[23] i.e. the concepts of "security measures", "without right", "without authorization", or "exceeds the authorization".

[24] Article 2 Cyprus Law No. 22(III)04: "for the purpose of this Law, the terms and phrases below have the following meaning:- "computer system" means any device or assembly of interconnected devices or that are in an operational relation, out of which they provide automatic data processing by means of a computer program. – "Computer data" means any representation of facts, information or concepts in a form that can be processed by a computer systems which includes any computer program that can cause a computer system to perform a function. - "Service provider" means – any public or private entity offering the users the possibility to communicate by means of a computer system, and – any other entity processing or storing computer data for the entity mentioned above or for the users of the services offered by these. – "Traffic data" means any computer data created by a computer systems and related to a communication achieved through computer systems, representing a part of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of service used for the communication".

[25] Article 93 of Bulgaria Criminal Code: "The words and expressions below have been used in this Code in the following context: 21. (New, SG 92/02) "Computer information system" is every individual device or a totality of interconnected or similar devices which, in fulfilment of a definite programme, provides, or one of the elements provides automatic data processing. 22. (New, SG 92/02) "Computer information data" is every presentation of facts, information or concepts in a form subject to automatic processing, including such a programme which is capable of doing so that a given computer system can fulfil a definite function. 23. (New, SG 92/02) "Provider of computer information services" is every corporate body or individual offering the possibility of communication through a computer system or which processes or stores computer data for this communication service or for its users. Bulgarian Penal Procedure Code Additional provisions: "§ 1. (2) For the purposes of this Code "data concerning traffic" shall mean all data related to a message going through a computer system which have been generated as an element of a communications chain indicating the origin, destination, route, hour, date, size and duration of the connection or of the main service".

[26] Article 35 Romanian Law No. 161/2003: " (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 at item 1 and for the users of the services offered by these; f) „traffic data" are any computer data related to a communication achieved through a computer system and its products, representing a part of the communication chain, indicating the communication 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 explicit behaviour or an adult person presented as a minor with an explicit sexual explicit behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual explicit 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 qualified 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".

Other countries define only the concept of data or traffic data.[27] For example, the German legislator with Sec. 202a (2) StGB only defines the concept of "data".[28] It is uncertain if it is a general definition because the provision affirms the definition operating for the meaning of Sec. 202a, subsection 1 StGB. The notion is more narrow than the definition of computer data furnished by Article 1b CoC, not including a program. A review of the current situation could be therefore advisable, introducing also the definition of "service providers" and "traffic data".

Countries that have introduced the definitions listed in the Convention on Cybercrime:[29]

European Countries (Full alignment)	Non-European countries (Full alignnment)
Austria (Sec. 74, para 1, 2 Criminal Code; Sec. 3 E-Commerce Act; Sec. 92, para 3 Telecommunication Act)	Egypt (Article 1 Draft Law)
Cyprus (Article 2 Law No. 22(III)04 (FC)	Sri Lanka (Article 38 Computer Crime Act No. 24/2007)
Bulgaria (Article 93, 21,22,23, Penal Code)	
Romania (Article 35 , para 1 No. 161/2003) (FC)	

By way of conclusion, it is advisable that the countries that do not yet have any provision defining these concepts in accordance with Article1 CoC, provide to cover this dangerous gap that represents a serious obstacle for the uniform interpretation and application of the common cybercrime offences at the international level.

Moreover, the CoC should define other technical concepts, firstly the problematic term of *security measures* in conformity with the fundamental criminal principle of legality. It is an indeterminate notion that creates a lot of problems, not only to the experts but also to the courts.[30] The problems that the Italian courts has found in defining the concept of "*misure di sicurezza*" ("security measures") of the Article 615ter Penal Code are paradigmatic in this sense.[31] Should they be effective, physical or logic? To guarantee that the technical definition of protection measures may be applied to the current and future technological developments would be important to use the same technological-neutral language of Article 1 CoC.

In addition, it is also necessary to clarify other important mental elements of the offences as: "unauthorised", "without right", "without permission", "unwarranted" and "intentionally". There is not a common agreement about the meaning of these expressions. Each Party can connect them with its domestic law.[32] Nevertheless, these terms can create some problems of due to their lack of homogeneity among the different national legal systems.[33]

---

27 The Czech Republic and Italy only define the term "traffic data" (Article 90 Czech Republic Electronic Communications Act; Article 4h) Italian D.lgs. 196/2003).

28 According to Sec. 202a (2) StGB data are only "which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner".

29 Legenda: D: difference in scope and content; FC: full covering; GP: general provisions; II: insufficient information; NC: not covered; NR: not relevant; U: unknown ; RN: Review necessary; C: Corresponding; PC: partially covered; CR: considering review; CRIM: a penal sanction is provided; ADM: an administrative sanction is provided.

30 Koops B-J., *Cybercrime Legislation in the Netherlands*, cit.

31 Sarzana C., 'Aperçu des stratégies normatives italiennes de droit matériel au sujet de la lutte à la cybercriminalité set des applications jurisprudentielles correspondantes'. Comparison avec les dispositions continues dans la Convention de Budapest, Octopus Interface Conference, Strasbourg 11-12 June 2007. With regard to the sentencing practice of Italian courts see Salvadorl I., "L'accesso abusivo ad un sistema informatico o telematico: una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica", in Picotti L. (ed.), 'Tutela penale della persona e nuove tecnologie', 2007, *Quaderni MIUR per la riforma del codice penale*, 2008, (forthcoming).

32 Explanatory Report, 38.

33 Picotti L., 'Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale', *Diritto dell'Internet*, 2005, p. 197.

3 Comparative review of the substantive law

3.1 Illegal access

> Article 2 CoC:
> 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 either by infringing security measures or 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.

Illegal access to a computer is a "basic offence" for the commission of other dangerous threats, such as illegal interception, fraud, forgery, and many other computer crimes and cyber crimes.[34] Hence, anticipating the criminalisation of the conduct of access is also justified.[35]

The provision protects the legal interest of integrity and security of computer systems.[36] The aim of the offence is not only to guarantee the owner a peaceful use of his/her information system, but also to guarantee that any access to the system is realised by an authorized subject.

The provision covers access to a computer system, computer network, or to a computer connected to another computer, such as a LAN, Intranet or wireless.[37] The objective element of the offence requires that the subject gain access to the *whole* or *any part* of a computer system. That permits to cover the frequent situation where the access may be authorised but not the access to specific files or programs. Nevertheless, the majority of the national legislation provides to the access to computer without distinguishing between the access to the *whole* or *any part* of a computer system.[38]

The conduct of access must be realised "without authorisation", which means that the conduct of access authorised by the owner of the system, or by another legitimate holder of it will not be punished. For the same reason, the conduct of access to a system that allows open and free access to the public will be not criminalised. In this case, access is legal.[39]

The *mens rea* requires that the system be accessed "intentionally", which means that the conducts caused by negligence are not punishable.[40]

As mentioned earlier in the study, any country defines the concept of "access", "without authorisation" and "security measures".[41] This poses severe problems in the practical application, especially with regard to the *locus commissi delicti* and *tempus commissi delicti*.

Only some state legislators of the United States define the term "access".[42] The most

---

[34] Explanatory Report, 44; Sieber U., in Council of Europe, *Organised crime in Europe: the threat of cybercrime*, 2004, p. 87.

[35] Picotti L., *Reati informatici*, 20.

[36] Explanatory Report, 44. See also Gercke M., *The Convention on Cybercrime*, cit., p. 279.

[37] For a wide explanation of the specific problems connected with the access to a WI-FI, see Kern B.D., Whacking, Joyriding and War-Driving: Roaming Use of Wi-fi and The Law, (21) 2004 Santa Clara Computer & High Tech. L.J., p. 101.; SNOW N., Accessing The Internet Through The Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality, (84) 2006 Neb. L. Rev, p. 1226.

[38] The distinction between the access to the whole or any part of a system is typified by Article 323-1, paragraph 1, of French Criminal Code.

[39] Explanatory Report, 47.

[40] Explanatory Report, 39.

[41] Only Romania defines the concept of "security measures". According to Article 35h Romania Law No. 161/2003, they consist in "the use of certain procedures devices or specialized computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users".

[42] Ala. code § 13A-8-101 (11) (1994); Ark. code ann. § 5-41-102 (a) (1) (Michie 1997); Conn. Gen. Stat. § 53a-250 (1) (1994 & Supp. 1999); Del. Code Ann. Tit. 11, § 931 (1) (1995 & Supp. 1998); Iowa Code Ann. § 716A.1 (1) (1999); Kan. Stat. Ann. § 21-3755 (a) (1) (1995 & Supp. 1997); N.H. Rev. Stat. Ann. § 638:16 (I) (1996).

common definitions are three, namely: "to instruct, communicate with"; "store data in, retrieve data from"; "make use of any resources of a computer, computer system, or computer network".[43]

The CoC gives member parties the choice to criminalise mere hacking ("pure access to information system"). Alternatively, parties may attach any or all of the following three qualifying elements to this basic structure of the offence, with the aim of reducing the criminalisation of mere access:

Infringing security measures. This is, for example, the case of Austria ("specific safety precautions within the system"), Italy ("*misure di sicurezza*"), Germany ("access security mechanisms"), the Netherlands ("*einige beveiliging*"), Lithuania ("security measures"), Cyprus ("security measures") Estonia ("code, password or other protective measure") Hungary ("computer protection system") and Romania ("security measures").[44] Nevertheless, each of these countries, except for Romania, does not outline a definition of this concept.

Special intent to obtain computer data, other dishonest intent. This is for example the case of Portugal, Romania or Slovakia.[45]

Offence committed in relation to a computer system that is connected remotely to another computer system. Until presently no country has implemented it.[46]

Many national legislations contain provisions on *hacking* and *cracking* offences. Nevertheless the objective and subjective elements of the illegal access provision vary considerably. Italy, France and Belgium, in conformity with the Council of Europe Recommendation of the R (89) 9, do not criminalise, for example, just access to an information system, but also the unauthorised *permanence* in such system.[47]

A range of countries have followed a narrower approach requiring more additional qualified circumstances. Some countries go beyond the requirements of the Cybercrime Convention attaching different elements.[48] Armenia, for example, envisages a responsibility for illegal access when this negligently causes change, copying, obliteration, isolation of information, or spoilage of computer equipment, computer system or other significant damage.[49]

Some countries do not refer to the illegal access to the whole or any part of a computer but generically to the resources of a computer moving ahead the level of the criminalisation. Bulgaria, for example, punishes "access to the resources"; Armenia "the penetration into information stored in a computer system"; Croatia "access to computer data or programs", United Kingdom criminalises the "access to computer material".[50]

---

[43] For a wide explanation of the juridical experience of the USA about the offence of unauthorised access to a computer system, see Kerr O., 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statues', in (78) 2003 N. Y. Un. L. Rev., 1602 ss.

[44] Austria (Section 118a Penal Code); Italy (Article 615ter Penal Code); Cyprus (Article 4 Law no. 22(III)04); Estonia (Article 217 Penal Code); Romania (Article 42(3) Law No. 161/2003); Lithuania (Article 198-1 Criminal Code); The Netherlands (Article 138a Criminal Code) and Hungary (Article 300C(1) Criminal Code).

[45] Portugal (Article 7 Law No. 109/91); Romania (Article 42(2) No. 161/2003); Slovakia (Sec. 247(1) Criminal Code).

[46] For the opportunity of this objective element see, Morales Prats F., 'Los ilicitos en la red (II): pornografía infantil y ciberterrorismo', in Romeo Casabona C.M. (ed.), *El cibercrimen*, cit., p. 276.

[47] See Article 615ter Italian Criminal Code; Article 323-1 French Criminal Code; Article 550*bis* § 1 Belgium Criminal Code ("*celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient*"). For an explanation of Belgium illegal access provision see Meunier C., *La Loi du 28 novembre 2000 relative a la criminalité informatique ou le droit pénale et la procédure pénale à l'ère numérique*, in *Revue Droit Pénal Criminologie*, 2001, 630 ss.; Wery É., Verbiest T., *Le droit de l'Internet et de la société de l'Information*, Bruxelles, 2001, p. 24. Also Article 243, paragraph 1 Turkish Criminal Code No. 5237/2005 criminalises the unauthorised permanence in such systems.

[48] Armenia (Article 251 Criminal Code), Austria (Section 118a Penal Code).

[49] See Article 251 Armenian Criminal Code.

[50] See Bulgaria (Article 319a Criminal Code); Armenia (Article 251 Criminal Code); United Kingdom (Article 1b, paragraph 2 Computer Misuse Act), Croatia (Article 223(1) OG 105/04). For other similar examples see also the illegal access provision of Germany, Austria or Australia.

A model of full alignment with Article 2 CoC is represented by Article 42, paragraph 1,2,3 of the Romanian Law No. 161/2003.[51] Article 42, paragraph 1 Romanian Law No. 161/2003 criminalises, in accordance with Article 2 CoC, the "simple" hacking, namely the illegal access to a computer system. The act is punished with imprisonment from six months to three years.

Article 42, paragraph 2 Romanian Law No. 161/2003 provides for an aggravation circumstance for cracking, criminalising the illegal access committed with the intent of obtaining computer data. The punishment goes from six months to five years.

Article 42, paragraph 3, Law No. 161/2003 provides for a further aggravation circumstance (punishment from three to twelve years) for the illegal access committed by infringing the security measures.[52]

Article 2 CoC is completely covered also by Article 4 Cyprus law No. 22(III) 04 that criminalises (with imprisonment from five years or to 20,000 Cyprus Pounds) "any person who intentionally and without authority access a computer system by breaking the security measures".

Another example of full alignment with Article 2 CoC is represented by Article 323-1, paragraph 1, French Criminal Code that punishes the conduct of access to the whole or any part of a system that performs automatic processing of data ("*système de traitement automatisé de données*").[53] The provision requires that the subject acts in a fraudulent manner ("*frauduleusement*"). The access is fraudulent, for example, if the subject violates the security measures.[54] Article 323-1 Code Penal also criminalises the conduct of "remaining" ("*le fait de se maintenir*") in such a system.[55]

The mental element of Article 323-1 Code Penal does not provide the conduct can be committed "intentionally" and "without right".

This basic offence, provided for by Article 323-1 Code Penal, is punished with imprisonment of up to two years and a fine up to 30,000 euros. If the conduct of access determines the suppression or the modification of the computer data contained in the computer system or the alteration of its functioning, the offence is punished with the imprisonment up to three years and a fine of 45,000 euros.

Article 323-1 Code Penal does not demand the requirements of "infringing security measures" or gaining access "in relation to a computer system that is connected to another computer system". But in accordance with Article 2 CoC, the Parties are not bound to provide these requirements. Article 323-1 Code Penal therefore complies with the requirements established by Article 2 CoC.

The German legislation partially covers Article 2 CoC. Section 202a StGB places more emphasis on the criminal liability sanctioning not the access to the whole or any part of a

---

[51] Nevertheless it does not provide that the illegal access could be committed "to the whole or any part of a computer system", and concerning the mental elements that the act is committed "intentionally" and "without right".

[52] For the notion of security measure furnished by Article 35h) Romanian Law No. 161/2003 see above footnote 40.

[53] Article 323-1, para. 1 Code Penal: "*Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende".* For a comment see Feral-Schuhl C., *Cyberdroit, Le droit à l'épreuve de l'Internet*, 597.

[54] According to the Cour d'appel de Paris, 30 October 2002: "*Il ne peut être reproché à un internaute d'accéder aux données ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès*".

[55] See *Cour d'appel de Paris*, 5 April 1994, Dalloz, 1994, I.R. 130: "*la loi incrimine également de maintien irrégulier dans un système de la part de celui qui y serait entré par inadvertance, ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement* "; El Chaer N., *La criminalité informatique*, cit., 115 ss.

computer system, but only the (further) obtaining of the access to data.[56] Therefore Sec. 202a StGB seems to go beyond the requirements of the CoC.

Sec. 202a StGB focuses on the protection of the confidentiality of data. Not all the computer data are protected but only the data specially protected against unauthorised access. The offence is punished with imprisonment for not more than three years or a fine. Review of the current situation could be taken into consideration by the German legislator, criminalising the basic conduct of access to (a whole or a part of) an information system. It could be useful also to insert a detailed notion of security measures.

Countries that have introduced a provision corresponding to Article 2 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Lithuania (Article 198-1 CC)	Egypt (Article 33 Draft Law)
Hungary (Article 300C(1) CC)	USA (Title 18, Part I, Chapter 47, § 1030 of the US Code
Estonia (Article 217 CC)	Philippines (sec. 4.A.1 Draft Law)
The Netherlands (Article 138a CC)	India (Section 65 Ita)
Serbia (Article 302 CCRS)	
Slovakia (247 (1) Criminal Code Act No. 300/2005 Co)	
Cyprus (Article 4 Cyprus Law no. 22(III)04)	
Italy (Article 615ter c.p.)	
France (Article 323-1 Code Penal)	
Portugal (Article 7 L. No. 109/91)	
Romania (Article 42 No. 161/2003)	

The unauthorised access to a computer system (hacking or cracking) represents a "basic offence" for the commission of other more serious offences. For this reason, it needs to be criminalised by all the national legislation in the same way.[57]

The criminalisation of mere unauthorised access could constitute the first "basic offence". Parties could take into consideration the possibility to provide also for an aggravation of circumstances with regard to the acts of access committed which break security measures, or with the intent to obtain computer data, in accordance with Article 2, paragraph 2 and 3 CoC. A model of good practice is represented by Romanian law.

[56] Sec. 202a 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) Within the meaning of subsection (1), data shall be only those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner". For an explanation see Ernst S., Das neue Computerstrafrecht, cit., 2661.

[57] It would be advisable that the CoC specifies expressly the problematic concepts as mentioned above ("security measures, access, without authorisation") in order to guarantee the uniform application of this offence at the national level.

3.2 Illegal interception

> Article 3 CoC:
> 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.

The aim of the provision is to protect the confidentiality of computer data and systems.[58] Particularly, it warrants the correctness of the electronic data transfer process via computer systems, since the latter is less safe than the classic mail system.

The transfer process in cyberspace involves a wider range of providers. Therefore, it is easier for transferring data to be illegally intercepted.[59] The aim is to assure to the transmission of computer data the same criminal protection of the voice phone interception that in the majority of the national legislations are protected against the illegal tapping and recording acts.[60]

The provision of Article 3 CoC applies to "non-public transmissions" of data, as well as to "electromagnetic emissions". These objects must be interpreted in a wide sense, covering also the telephone, fax, e-mail or file transfer in order to ensure a more comprehensive scope.[61]

The term "non-public" refers to the nature of the transmission process that must be private, and not to the nature of the data transmitted. For some countries, the conduct of illegal interception refers not to *non-public transmissions* of computer data, but more generally to all kinds of communications. In particular a lot of countries use widely different expressions that are not consistent with the CoC provision. Bulgaria, for example uses the expression "message", instead of *transmissions* of computer data; Portugal refers generically to "all communication inside a computer system"; the USA refers to "wire, oral or electronic communications".[62]

As requested by Article 3 CoC, the interception must be committed *without right* and by *using technical means* in order to avoid over-criminalisation.[63] Nevertheless, not all the countries that have already ratified the Cybercrime Convention explicitly require that the illegal interception must be committed by using technical devices.[64] Other countries require expressly the use of technical devices.[65]

Few countries require that the offence be committed with *dishonest intent*, as provided in the Article 3, paragraph 2 CoC.[66] Moreover, none require that the offence must be committed in relation to a computer system that is connected to another computer system, as provided in the Article 3, paragraph 2 CoC.

The French legislator has partially covered Article 3 CoC with Article 226-15, paragraph 2

---

58 Explanatory Report, 51.
59 See Sieber U., in Council of Europe, *Organised crime in Europe*, cit.
60 Explanatory Report, 53.
61 Explanatory Report. No. 50.
62 Article 171(1), paragraph 3 Bulgarian Criminal Code; Article 8 Portugal Law No. 109/1991; title 18, Article I, chapter 119, § 2511 US Code).
63 Explanatory Report, 58.
64 I.e. Armenia (Article 254(1) Criminal Code), Croatia (Article 233(4) OG 105/04), Cyprus (Article 5, law No. 22(III)04), Estonia (Article 137 Penal Code) or Lithuania (Article 198 Penal Code).
65 I.e. Bulgaria (Article 171(3) Penal Code), Germany (Sec. 202b StGB), Portugal (Article 8, Law No. 109/91), Austria (Sec. 119a Penal Code), Slovakia (Article 247(2) Criminal Code); The Netherlands (Article 139c CC).
66 See for example Austria (Sec. 119a Criminal Code).

Code Penal.[67] It criminalises malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions.

A review of French provision should be taken into consideration with a focus on the following aspects: is the interception of non-public transmission of data covered? Is the interception of electromagnetic emissions of computer data covered?

As mentioned above, the interception of computer data should be punished only if committed by technical means, in order to avoid over-criminalisation. Article 226-15, paragraph 2, Code Penal goes beyond the provision of CoC, criminalising in addition the installation of devices to intercept communications.

An example of full alignment with Article 3 CoC is represented by Croatian, Cyprus, German and Romanian legislation.

Article 223, paragraph 4, Croatian OG 105/04 criminalises: "whoever intercepts or records the nonpublic transmission of electronic data to, within or from a computer system, not intended for his use, including the electromagnetic transmissions of data in the computer system, or whoever enables an unauthorized person to access these data shall". The perpetrator is punished by a fine or by imprisonment not exceeding three years.

Article 5, paragraph 1, Cyprus Law No. 22 (III) 04 criminalises "any person who intentionally and without authority intercept non-public transmissions of computer data to, from or within a computer data".

The German legislator has fully covered Article 3 CoC with Sec. 202b StGB ("Data Interception").[68] The German provision provides for: "whoever, without authorisation and through the use of technological means, obtains for himself or another party access to data not intended for him (section 202a subsection (2)) from non-public transmissions of data or from electromagnetic emissions of data processing equipment, shall be punished with imprisonment for no more than two years or a fine, provided that the offence is not subject to a more severe penalty under other provisions".

Article 43, paragraph 1,2, of Romanian Law No. 161/2003 also complies with the requirements established by Article 3 CoC. It provides for "the interception without right of non-public transmissions of computer data to, from or within a computer system [..] 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".

[67] Article 226-15, paragraph 2, Code Pénal: *"Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions".*

[68] For an explanation of the new Sec. 202b StGB see Ernst S., *Das neue Computerstrafrecht*, cit., p. 2664.

Countries that have introduced a provision corresponding to Article 3 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Austria (Article 119- 119a Austrian Criminal Code)	Sri Lanka (Article 8, Computer Crime Act, No. 24/2007)
Croatia (Article 223, para. 4, OG 105/04)	
Cyprus (Article 5 Cyprus Law No. 22(III)04	
Germany (section 202b)	
Italy (17il. 617quater, quinquies, sexies c.p.)	
Portugal (Article 8 Law No. 109/1991)	
Romania (Article 43 No. 161/2003)	
Slovakia (Article 247(2) Criminal Code Act No. 300/2005 Coll)	

To avoid an over-criminalisation, it is advisable that the countries criminalise only the interception of non-public transmission of computer data. For this reason, all these national legislations that refer generically to *communications* or other general concepts (correspondence, material, information, etc), without giving a precise definition of these terms must be criticised.

Not all the countries that have already ratified the CoC, have implemented the provision.[69] They should take into consideration the necessity to implement their domestic law in accordance with the CoC provision. A model of good practice is represented by German or Romanian criminal legislation.

3.3 Data interference

> Article 4 CoC:
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
> 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 4 CoC criminalises illegal data interference. The aim of the provision is to ensure that data and computer programs have the same protection given to corporeal objects. The protected legal interest is the integrity and correct functioning and use of technology products.[70]

The *actus reus* consists in causing a damage against computer data "without right". The provision punishes only the conducts that consist in *damaging, deleting, deteriorating, altering or suppressing* of computer data.

The term "alteration" must be interpreted as such a modification of computer data, including therefore also the input of malicious codes (for example, viruses, trojan horses, DDoS or malware programs) that cause a modification of data.[71]

In conformity with the principle of *extrema ratio,* the second part of the provision (Article 4, paragraph 2 CoC) enables Parties to criminalise only conducts causing *serious harm*. Each Party can therefore autonomously define the extent to which the provoked harm can be considered "serious", on the basis of its domestic law criteria. Some countries criminalise the data interference only in significant cases, requiring, in accordance with Article 4, paragraph

[69] Hungary, the Former Yugoslav Republic of Macedonia and Estonia.
[70] Explanatory Report, 60.
[71] Explanatory Report, 61.

2 CoC, that the conduct results in serious harm.[72]

As analysed above, the mental element (*mens rea*) requires that the subject carries out the conduct *intentionally* and *without right.*

In some country the provision is fully covered, except for the elements that might be committed *intentionally* and *without right.*[73] In addition, some countries criminalise not only the intentionality, but also the negligent computer data damage.[74]

Not all the national provisions cover all forms of data interference. The *actus reus* of Article 323-3 of French Penal Code is more restricted compared to Article 4 CoC.[75] It only covers the introduction, suppression or modification into an automated data processing system of the computer data committed with dishonest intent ("*fraudulent*").[76]

Some countries do not use the same words of the provision but only a generic expression: "interference in any way"[77], "obliteration"[78] or "unauthorized actions"[79]. For this reason it could be doubtful in some cases if these expressions may include all the acts of damaging, deletion, deterioration, alteration or suppression as provided by Article 4 CoC. It would be necessary therefore to analyse the sentencing practice of national courts.

Other countries do not criminalise interference to the computer data, but only to the "information".[80] In this case it would also be advisable to analyse the sentencing practice in order to understand if this different term (information, instead of computer data) determines a different scope of the provision.

A model of full implementation is represented by German, Romanian, Croatian and Cyprus legislation.

The German provision typified in Sec. 303a StGB ("Alteration of Data") provides for:

> (1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a subsection (2)) shall be punished with imprisonment for not more than two years or a fine. (2) An attempt shall be punishable. (3) Section 202c shall apply accordingly with respect to the preparation of a criminal offence under subsection (1).[81]

The provision does not expressly cover the conduct of damaging. Nevertheless, it could be covered partially by the conduct of "rendering unusuable". The offence is punished with imprisonment for not more than two years or a fine. Section 202b (2) StGB also criminalises the attempt.

---

[72] See for example Bulgaria (Article 319b Penal Code), Estonia (Article 206 Penal Code) or Lithuania (Article 197 Penal Code).

[73] Croatia (Article 223(3) OG 105/04); Slovakia (Article 247(1)b Criminal Code), Turkey (Article 244(2) Penal Code).

[74] i.e. Armenia (Article 253 Penal Code); The Netherlands (Article 350b CC).

[75] Article 323-3 Code Penal: "*Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende".*

[76] See for a comment Feral-Schuhl C., *Cyberdroit, Le droit a l'épreuve de l'Internet*, p. 598.

[77] Albania (Article 192/b Penal Code).

[78] Armenia (Article 253 Criminal Code).

[79] Ukraine (Article 362(1) Criminal Code).

[80] Sri Lanka (Article 5(a-c) Computer Crime Act), Ukraine (Article 362(1) Criminal Code), Slovakia (Article 247(1)b Criminal Code).

[81] For an explanation see Ernst S., *Das neue Computerstrafrecht*, cit., 2664; Trondle, Fischer (ed.), *Strafgesetzbuch und Nebengesetze*, p. 1966.

Article 44 Romanian Law No. 161/2003 provides for:

> 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".

The provision complies with the requirements established by Article 4 CoC, except the mental element that the act to be committed "intentionally" and the objective element that the act causes the "damaging" and the "suppression" of computer data. Unlike Article 4 CoC Article 44, paragraph 1, Law No. 161/2003 also criminalises the "restriction" of computer data.

Article 44, paragraphs 2 and 3, Romanian Law No. 161/2003 goes beyond criminalising with an aggravation of circumstances (imprisonment from 3 to 12 years), as well as the "unauthorised data transfer" from a computer system (Article 44, paragraph 2), and the unauthorised data transfer by means of a computer data storage medium (Article 44, paragraph 3).

Article 233, paragraph 3 of the Croatian OG 105/04 is also consistent with Article 4 CoC. It criminalises: "whoever damages, alters, deletes, destroys or in some other way renders unusable or inaccessible the electronic data or computer programs of another". The perpetrator is punished by a fine or by imprisonment not exceeding three years.

According to Article 6, Cyprus Law No. 22(III)04, data interference is committed by: "any person who intentionally and without authority destroys, deletes, alters, or suppress (hides) computer data". The perpetrator is punished with imprisonment of up to five years or with a fine up to 20,000 Cyprus pounds, or both.

Countries that have introduced a provision corresponding to Article 4 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Croatia (Article 233, para. 3, OG 105/04)	Sri Lanka (Article 5(a-c) Computer Crime Act)
Cyprus (Article 6 Law No.22(III)04) (FC)	Philippines (Sec. 4.B Draft Law)
Germany (Article 303a StGB)	
Italy (Article 420 c.p.; Article 635bis c.p.)	
Romania (Article 44 Law No. 161/2003) (FC)	
The Netherlands (Article 350a)	
Austria (Sec. 126 a CC)	
FyRoM (Article 251(1) CC)	
Slovakia (Sec. 247(1)b CC)	

Almost all the countries have a provision corresponding partially or fully with Article 4 CoC. The main difference is between the national offences concerning the description of the acts of interference.

The countries that do not already have the provision of Article 4 CoC implemented should take into consideration the necessity to modify their provisions in accordance with Article 4 CoC. They should take as a model the German, Romanian or Croatian provision.

To avoid an over-criminalisation, in conformity with the principle of legality, it would be better if they criminalise only the conducts that cause *serious harm*.

3.4 System interference

> Article 5 CoC
> 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.

The development of the Information Society depends on the correct functioning of computer systems and computer networks.[82] Therefore, it is crucial that the correct use and functioning of information systems must be guaranteed. There are a lot of conducts realised in the cyberspace that can cause serious threats to the correct availability of the systems and particularly of the critical infrastructure of society. For this reason, with the provision also known as *computer sabotage*, using the expression of the Recommendation (89) 9, the CoC aims to protect the legal interest of "operators and users of computer or telecommunications systems being able to have them functioning properly".[83]

The *actus reus* requires the "hinder" of *functioning* of a computer system. The term hindering means every conduct that interferes with the correct functioning and use of an information system. This event may be realised by *inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing* computer data. All these conducts require a computer data related interference. It is the case for example of the Denial of Service Attacks (DoS), the conduct of mail-bombing (spam or bulk-email), or the conducts of Net-strike.[84] Attacks such as the former can cause enormous financial losses.

Some countries do not typify the offence using these terms, but only indeterminate expressions as "interfere with the system"[85] or "render unusable".[86]

Article 323-2 French Penal Code criminalises, for example, the conduct of "interfering" ("*le fait d'entraver ou de fausser*") with the functioning of a computer system ("*système de traitement automatisé de données*"), without providing for it to be caused by the damaging, deleting, altering or suppression of computer data. The provisions could be broader than the Cybercrime Convention, covering all attempts to interfere, and not just the "serious hindering".

With respect to the principle of *extrema ratio*, the provision criminalises only serious hinders, but it does not define the concept of "serious". As a consequence, each Party is free to determine a minimum amount of damage to be caused which may be defined *serious.*[87] Depending of the level of the threshold of harm (partially, completely, temporally alteration of the functioning of the computer system) they could choose an administrative, civil or criminal sanction.[88]

The provision of the serious harm is appropriate because it avoids an over-criminalisation. In addition, the sending of an unsolicited e-mail (spam) could cause a nuisance to the recipient but does not create any damage for the computer.[89] This could be different in the case of bulk e-mail: the sending of a large quantity of unsolicited e-mails (bulk-email) could cause the interruption of the information system and therefore it should be punished.

---

82 Persico B.A., 'Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure', cit., p. 153; Hanseman R.G., *The Realities and Legalities of Information Warfare*, cit., p. 187.

83 Explanatory Report, 65.

84 Katyal K.N., Criminal Law in Cyberspace, in (4) 2001 U. of P. L. Rev., p. 1003; Gonzalez Rus J.J., *Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes*, in Romeo Casabona C.M. (ed.), *El cibercrimen*, cit, p. 241.

85 Portugal (Article 5,6 Law no. 109/91), Austria (Sec. 126b Criminal Code).

86 Croatia (Article 223(2) OG 105/04).

87 Explanatory Report, 67.

88 Explanatory Report, 69.

89 Explanatory report, 69. For a wide analysis of the legal problems concerning spam, see, in German, Frank T., *Zur Strafrechtlichen Bewältigung des Spamming*, 2004.

The mental element (*mens rea*) of Article 5 CoC requires the intentionality. It means that the perpetrator must have the intent to seriously hinder.

Only a few European countries have already fully implemented this provision. A model of good practice is represented by Cyprus and Romanian legislation.

Article 7 Cyprus Law No. 22(III)04 criminalises: "any person who intentionally and without authority causes serious hindering of the functioning of a computer system, by inputting, transmitting, destroying, deleting, altering, adding, or suppress computer".

Article 45 Romanian Law No. 161/2003 complies with the requirements established by Article 5 CoC. It provides for: "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".

Romanian law fully covers Article 5 CoC, except the mental element that the act be committed "intentionally", and the objective element that the serious hindering of the functioning of a computer system is committed also by "damaging" and "suppressing" computer data. The offence is punished with imprisonment from 3 to 15 years.

The German legislation is not completely consistent with Article 5 CoC – Section 303b StGB ("computer sabotage") criminalises:

> (1) Whoever seriously interferes with data processing which is of substantial significance to another party by 1. Committing an act under section 303a subsection (1); 2. Enters or transmits data (section 202a subsection (2)) with the intention of causing harm to another party or 3. Destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier.

According to Sec. 303b StGB, the serious interference must have a substantial significance to another party. The German provision does not specify that the serious hindering must concern the functioning of a system. This requirement permits the judge to take into consideration not only the objective element of the serious hindering, but also to evaluate if this act is of substantial significance to another party. This element could produce a restriction of the criminalisation. In a different way, Article 5 CoC requires that the serious damage must be necessarily related to a computer system.

The act of "computer sabotage", provided for by Sec. 303b StGB, is punished with imprisonment of up to three years or a fine. An aggravation of circumstances is provided if the conduct causes significant interference to the business or enterprise of another person or to a public authority. In these cases the penalty consists of imprisonment of no more than five years or a fine.

Countries that have introduced a provision corresponding to Article 5 CoC:

European countries (full alignment)
Cyprus (Article 7 Law No. 22(III)04) (FC)
Romania (Article 45 Law No. 161/2003) (FC)
Slovakia (Article 247(1)d Criminal Code Act No. 300/2005)
Austria (Sec. 126b CC)
France (Article 323-1 Criminal Code)

By way of conclusion, it is advisable that the CoC should also criminalise the new cyber threats such as Net-strike, or mail-bombing, that do not necessarily cause in each case a damage in the form of a serious hindering, but only a menace for the functioning of the

system as the (partially or fully) *obstacle* or *interruption* of the functioning of the system.[90]

A lot of countries do not criminalise the serious hindering of the functioning of the computer system. It is advisable that they introduce in their provisions this requirement, taking the German or Romanian legislation as a model.

3.5 Misuse of devices

> Article 6 CoC
> 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 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 authorized testing or protection of a computer system.
> 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.

The aim of the offence is to criminalise the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing some different offences against the legal interests of confidentiality, integrity and availability of computer systems or data.[91]

For the commission of many cybercrimes, the criminals need some "hacker tools" or other specific tools (malware or sniffing programs, trojan horses, spamware, etc.). For this reason there is a big offer in the cyber market for "hacker kits". The aim of this offence is to reduce the offer of these programs and devices, already criminalising the *possession* and the *distribution* of them.

Paragraph 1(a) of Article 6 CoC criminalises different acts: the *production, sale, procurement for use, import*, *distribution* or otherwise *making available* of a device, including a computer program. The provision requires that the device is designed exclusively or specifically or adapted primarily for committing one of the offences under Articles 2-5 CoC. The aim is to exclude the criminal relevance of the dual use devices that could also be used for a legal purpose: for example, all the devices designed to test the level of security of a computer system (port scan program) or designed to control the reliability of the information technologies products by the industries.[92]

Paragraph 2 of Article 6 CoC criminalises the same acts (*production, sale, procurement for use, import, distribution or making available*) that concern *computer password*, *access code* or *similar data*. Each country can determine the number of items in the presence of which

[90] A model of provision could be represented by Article 4 EU Framework Decision on attacks against information systems.
[91] Explanatory Report, 71.
[92] Explanatory Report, 77.

the acts are criminalised. Only the USA provides a minimum number of devises for the criminalisation.[93]

The aim of the second paragraph is to avoid in particular the unauthorised access to information systems. In both the cases the CoC requires a specific mental element: the criminal must use these data with the intent to commit one of the offences established in Articles 2-5 CoC. In addition, many national provisions do not require moreover, contrary to the Article 6 CoC, that the offender has to act with the intent to commit a computer crime.[94]

A lot of national provisions do not cover all illegal acts (i.e. *production, sale, procurement for use, import, distribution or otherwise making available*) regarding the devices, and prefer to use different concepts.[95] The *actus reus* of Article 323-1 of French Code Penal is more limited than Article 6 CoC, not covering *production, sale, procurement for use, and distribution* of such items.

Not all the countries provide the criminalisation for all the tools (i.e. *computer password, access code or similar data*).[96] The majority criminalise only the sale or production of computer programs, but do not mention the possession of password, or access devices.

Article 6 CoC is partially covered by Sec. 202c StGB ("Preparation of Data Espionage or Data Interference).[97] The conducts criminalised by Sec. 202c StGB and Article 6 CoC are the same. Both of them criminalise the creation, procurement, sale, dissemination or making available passwords, security codes or computer programs. The material object of the offence is different.

According to Article 6 CoC, passwords, access codes or other similar data (computer programs, etc.) must enable the whole or any part of a computer crime. The aim of Sec 202c StGB seems more narrow: it criminalises only the conducts having as object devices that only permit the "access to data". According to Article 6 CoC, passwords, access codes, computer programs, must be designed or adapted primarily for the purpose of committing one of the offences provided by Articles 2-5 CoC.

The criminal aim of Sec. 202c StGB is more limited. It criminalises only the conducts that have as object passwords or other security codes that enable "access to data". For this reason Sec. 202c StGB does not criminalise the possession, sale, making available of devices adapted to commit a data interference or system interference.

A model of full alignment is represented by Romanian, Austrian, and Croatian criminal legislation.

Article 46, paragraph 1,2, Romanian Law No. 161/2003 provides for:

> It is a criminal offence and shall be punished with imprisonment from 1 to 6 years. a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45; b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42–45.

---

93 USA (Title 18, Article 1, Chapter 47 § 1030 (6) US Code).

94 See for example Albania (Article 286/a Penal Code); Armenia (Article 255, 256 Penal Code), Croatia (Article 223 (6-7) OG 105/04), Italy (Article 615quinquies Penal Code).

95 See i.e. Albania (Article 286/a Penal Code), France (Article 323-3-1 Penal Code), Slovakia (Article 247(2)b Penal Code) or Lithuania (Article 198-2 Penal Code).

96 Armenia (Article 255, 256 Penal Code).

97 For a first comment of the new provision see Ernst S., *Das neue Computerstrafrecht*, cit., p. 2662.

Paragraph 2 provides that "the same penalty shall sanction the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45".

Sec. 126c of Austrian Penal Code provides for:

> (1) whoever produces, introduces, distributes, sells or otherwise makes accessible 1. A computer program or a comparable equipment which has been obviously created or adapted due to its particular nature to commit an unlawful access to a computer system (sect. 118°), an infringement of the secrecy of telecommunications (sect. 119), an unlawful interception of data (sect. 119°), a damaging of data (sect. 126°) or an interference with the functioning of a computer system (sect. 126b), or 2. A computer pass word, an access code or comparable data rendering possible the access to a computer system or a part of it, with the intent that they will be used for the commitment of any criminal offence mentioned in para.1, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines. (2) A person shall not be punished under para. 1 who prevents voluntarily that the computer program mentioned in para. 1 or the comparable equipment or the pass word, the access code or the comparable data will not be used in a way mentioned in sections 118°, 119, 119°, 126° or 126b. If there is no danger of such a use or if it has been removed without an activity of the offender, he shall not be punished in case he, unaware of that fact, makes voluntarily and seriously an effort to remove it.

Article 223, paragraph 6 and 7 Croatian OG 105/04 is compliant with the requirements of Article 6 CoC. The Croatian provision criminalises:

> (6) Whoever, without authorization, produces, procures, sells, possesses or makes available to another person special devices, equipment, computer programs and electronic data created or adapted for the perpetration of the criminal offense referred to in paragraphs 1, 2, 3 and 4 of this Article. (7) Special devices, equipment, computer programs or electronic data created, used or adapted for the perpetration of criminal offenses and used for the perpetration of the criminal offense referred to in paragraphs 1, 2, 3 and 4 of this Article shall be forfeited.

Countries that have introduced a provision corresponding to Article 6 CoC:

European countries (full alignment)
Austria (Section 126c Austrian Penal Code)
Italy (Article 615quater e quinquies c.p.)
Republic of Croatia (Article 223, para. 6-7 OG 105/04)
Romania (Article 46 Law No. 161/2003)

By way of conclusion, it is advisable that all the countries provide that devices must be primarily designed or adapted to commit the computer crimes provided for by the Convention in Articles 2-5 CoC (illegal access, data interception, data interference and system interference). That will avoid a dangerous over criminalisation.

It would be opportune to also provide that the offenders act with the intent to commit these offences. The states could use as a model the provision of Austrian or Romanian Criminal Code.

3.6 Computer-related forgery

> Article7 CoC:
> 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.

The offence protects the legal interests of the security and reliability of electronic data that have relevance for legal and economic relations.[98] The aim of the provision is to ensure that electronic documents have the same protection provided for tangible documents.

The basic offence of Article 7, paragraph 2, CoC criminalises unauthorised abuse of computer data, in order to give a different evidentiary value during the legal transactions. The *actus reus* consists in *inputting, altering* (i.e. modification, variation, partial changes)*, deleting* (i.e. removal of data from a data medium) or *suppressing* (holding back of computer data, concealment of data). The common element of all acts is the effect to falsify a genuine document through the illegal input of correct or incorrect data.

The concept of *computer data* must be interpreted in a wide sense, covering both public and private documents that have legal effects.[99]

The illegal act must be committed *intentionally* and *without right*. In accordance with Article 7, paragraph 2, CoC, the Parties may require a further specific mental element as *an intent to defraud*, or *similar dishonest intent*. The aim is to avoid an over-criminalisation requiring a stronger mental element that is evidently in contrast with the legal interest protected by the provision as mentioned above.

The concept of computer forgery varies frequently in the national legislations. Specifically, two different concepts of computer forgery may be outlined. The first one is based on the authenticity of the author of the document, while the second one is based on the truthfulness of the content of the document. However, the common basic element must be concerned with the alteration of the authenticity and veracity of the contents of the data.

Some countries do not expressly cover or have not yet adequately implemented Article 7 CoC.[100] Nevertheless, the majority of cases of computer-related forgery can fall within the scope of the traditional provision.[101]

Most of the national legislations do not cover all the acts concerning computer data provided by Article 7 CoC.[102] Some countries criminalise not only the modification or alteration of data but also of programs. This distinction does not seem to be necessary because programs are part of the wider concept of data, in accordance with Article 1 CoC.

Very few countries criminalise the act committed with a specific illegal intent.[103]

The German Criminal Code partially covers Article 7 CoC. Sec. 269 StGB ("Falsification of Legally Relevant Data"), criminalising the store or the modification of legally relevant data

---

98 Explanatory Report, 81.
99 Explanatory Report, 83.
100 Albania, Armenia or Slovakia.
101 See for example France or the Netherlands (Article 255 Dutch Criminal Code). For a comment see Koops B-J., 'Cybercrime Legislation in the Netherlands', in Reich P.C., *Cybercrime and Security*, vol. 2005/4.
102 Albania (Article 252 Penal Code), Armenia (Article 252 Criminal Code), Estonia (Article 344 Penal Code), Ukraine (Article 200 Penal Code), Turkey (Article 244, paragraph 2 Penal Code), Bulgaria (Article 319b,c Penal Code), Serbia.
103 i.e. Cyprus (Article 9 Law No. 22(III) 04), Portugal (Article 4 Law no. 109/91) or Austria (Sec. 225a Penal Code).

for the purposes of deception in legal relations resulting in a counterfeit or falsified document.[104]

The *actus reus* results more limited than Article 7 CoC. The provision criminalises only the storing or the modification of computer data, but not the input, alteration, deletion or suppression of computer data. The offence is punished with imprisonment for not more than five years or a fine.

A review could be taken into consideration in order to also expressly cover the *alteration, suppression and input* of computer data.

A model of full alignment is represented by Article 48 of Romanian Law No. 161/2003. It criminalises: "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". The offence is punished with imprisonment from two to seven years.

The Romanian provision complies with the requirements established by Article 7 CoC, except the mental element that the act to be committed "intentionally" and the objective element that the conduct could consist also in the "suppression" of computer data. Moreover Article 48 Romanian Law does not specify, in accordance with Article 7 CoC, that the "falsification" of computer data must be punished "regardless whether or not the data is directly readable and intelligible". This lack however seems to be not in contrast with the *ratio* of Article 7 CoC.

Another example of full alignment with Article 7 CoC is represented by Article 223a of Croatian OG 105/04, that criminalises: "(1) Whoever, without authorization, develops, installs, alters, deletes or makes unusable computer data or programs that are of significance for legal relations in order for them to be used as authentic, or whoever uses such data or programs". The illegal conduct is punished by a fine of by imprisonment not exceeding three years.

In the Austrian Penal Code, Section 225a is also completely consistent with Article 7 CoC. It criminalises: "a person who produces false data by input, alteration, erasure or suppression of data or falsifies authentic data with the intent for using them legally as evidence of a right, legal relationship or fact is to be sentenced to imprisonment up to one year".

"The former Yugoslav Republic of Macedonia" Criminal Code also contains a provision completely aligned with Article 7 CoC. Article 379-a FYRoM Criminal Code criminalises whoever without authorisation "(1) will produce, input, change, delete or make useless, with an intention to use them as real, computer data or programs which are determined or suitable to serve as evidence of facts with a value for the legal relations or one that will use such data or programs as real". The basic offence is punished with a fine or imprisonment up to three years.

Article 379a, paragraph 2 provides for an aggravation circumstance "if the crime stipulated in paragraph (1) is performed on computer data or programs that are used in the activities of the state authorities, public institutions, enterprises or other legal entities or individuals that perform activities of public interest or in the legal traffic with foreign countries or if significant damage is caused by their use". In this case the stipulator shall be sentenced to

[104] Sec. 269 StGB: "(1) Whoever, for purposes of deception in legal relations, stores or modifies legally relevant data in such a way that a counterfeit or falsified document would exist upon its retrieval, or uses data stored or modified in such a manner, shall be punished with imprisonment for not more than five years or a fine. (2) An attempt shall be punishable. (3) Section 267 subsections (3) and (4), shall apply accordingly". For a comment of Sec. 269 StBG see Hilgendorf E., Frank T., Valerius B., *Computer-und Internetstrafrecht*, cit. p. 53; Trondle, Fischer (ed.), *Strafgesetzbuch und Nebengesetze*, cit. p. 1856

imprisonment of one to five years.

Countries that have introduced a provision corresponding to Article 7 CoC:

European countries (full alignment)
Austria (Section 225a Penal Code)
Croatia (Article 223 A OG 105/04)*
Cuprys (Article 9 Law No. 22(III)04)
FYRoM (Article 379-a Penal Code)
Portugal (Article 4 Law No. 109/91)
Romania (Article 48 Law No. 161/2003)
Slovakia (Section 247d Criminal Code Act)

Until some years ago, a large part of the documents had a tangible nature. The development of the new technologies not only in the public but also in the private sector has determined an exponential increase of electronic documents. The majority of the national legislations recognises them as having the same legal relevance of the traditional documents.

In order to guarantee the correct and safe unrolling of the economic, social and public relationships, it is advisable that the countries that until today do not have a specific provision against computer forgery, introduce an offence consistent with Article 7 CoC.

An appropriate model of implementation could be represented by the Croatian, Romanian or Austrian legislation, as seen above.

3.7 Computer-related fraud

> Article 8 CoC:
> 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.

The quick development and diffusion of new technologies has increased the possibilities to commit economic crimes, such as fraud, credit card and banking fraud, and other related crimes committed frequently through techniques of "social enginnering" (*phishing, vishing, smishing, pharming*, etc.).[105] In accordance with recent statistics nowadays, electronic fraud is one of the most frequent crimes in cyberspace.[106]

In order to fight against these economic crimes, Article 8 CoC provides for a specific criminal offence against *computer-related fraud*. The offence protects firstly the legal interest of the property, but beyond the property the aim of the offence is to guarantee the correct and faithful activation and execution of the programmed procedures.[107]

The aim is to criminalise any unauthorised manipulation committed during data processing with the specific intent to cause an illegal transfer of property (i.e. electronic funds, deposit money, e-gold, etc).[108] Fraudulent manipulation of computer data is criminalised only if it

[105] Katyal K.N., *Criminal law in cyberspace*, in (4) 2001 Pennsylvania U. L. Rev.; Davis E.S., *A world wide problem on the world wide web: international responses to transnational identity theft via the internet*, 12 (2003) Wash. U. J.L. & Pol'y 201; Popp A., *"Phishing", "Pharming" und das Strafrecht*, MMR, No. 2, 2006, p. 84; Gonzales Rus J.J., *Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes*, in Romeo Casabona C.M. (ed.), *El cibercrimen,* cit. p. 241.
[106] See CSI/FBI, Computer Crime and Security Survey, 2006, available on www.GoCSI.com.
[107] Picotti L., *Sistematica dei reati informatici*, p. 55.
[108] Explanatory report, No. 86.

causes a direct economic or possessory loss of another person's property. The concept of "loss of property" has a wide scope and includes each loss of money with tangible or intangible economic value.[109]

The *actus reus* consists in any *inputting, altering, deleting, suppressing* of computer data that causes a loss of property. In order to cover all the relevant undue manipulations of computer data, Article 8, letter b CoC, also criminalises the general act consisting in any *interference with the functioning of a computer system*.

The mental element requires not only the *intentionality*, but also a specific fraudulent or other dishonest intent to gain economic profit for oneself or for another person. The aim is to avoid an over-criminalisation of the conducts that cause a loss to a person with a benefit for another, but that are not realised with a dishonest and fraudulent intent.[110]

Not all the countries that have already ratified the CoC have covered or adequately implemented Article 8 CoC.[111] The main differences between the national provisions regarding the offence of computer fraud and the Article 8 CoC model concern the formulation of the objective and mental elements.

With regard to the *actus reus*, not all the countries that have introduced an offence about computer-related fraud criminalise all forms of manipulations committed in the course of data processing.[112]

A lot of national legislations do not require specific mental elements, but only the intentionality.[113] In addition, some legislations do not require that the fraudulent acts must be committed "without right".[114]

Nowadays the French Criminal Code does not provide for a specific provision against computer-related fraud. With Law No. 88-19/1988 (known as "loi Godfrain"), the French legislator introduced a specific provision against computer fraud into the Criminal Code, criminalising "*la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui*". Nevertheless, in 1992 the legislator decided to eliminate this specific provision, considering that the computer fraud could be punished with the traditional fraud provision.[115]

Nowadays computer-related fraud falls in part within the scope of the traditional provision on fraud ("*escroquerie*"), Article 441-1 Code Penal, consisting in: "*toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplir par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques*".

It is advisable that the French legislator implement the criminal legislation introducing a specific provision about computer related fraud consistent with Article 8 CoC.

A model of full alignment with Article 8 CoC is represented by Sec. 263a German Criminal Code.[116] According to Sec. 263a StBG, computer fraud is committed by:

---

[109] Explanatory Report, 88.
[110] Explanatory report, 90.
[111] Albania (Article 191a Criminal Code), Armenia (Article 252 Criminal Code), Bulgaria (Article 212a Criminal Code), Croatia (Article 24a OG 105/04), Estonia (Article 213 Criminal Code), Hungary (Article 300/c, 300/e Criminal Code), Lithuania (Article 192 Criminal Code), "the former Yugoslav Republic of Macedonia", Ukraine.
[112] See for example Croatia (Article 244a OG 105/04); Armenia (Article 252 Criminal Code).
[113] Estonia (Article 213 Penal Code). Italy (Article 640ter Criminal Code).
[114] Croatia (Article 224a OG 105/04).
[115] For a comment see Verbiest T., Wery E., *Le droit de l'Internet et de la société de l'information*, p. 43.
[116] For a comment see Hilgendorf E., Frank T., Vvalerius B., *Computer-und Internetstrafrecht*, cit., p. 39; Fischer (ed.), *Strafgesetzbuch und Nebengesetze*, p. 1717.

> (1) whoever, with the intent of obtaining an unlawful material benefit for himself or a third person, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the order of events.

The offence is punished with imprisonment for not more than five years or a fine.

Sec. 263a (3) StGB provides for a lower penalty (imprisonment for not more than three years or a fine) if the perpetrator "prepares a criminal offence under subsection (1) by manufacturing computer programs, the purpose of which is to commit such an act, or for himself or another, obtains offers for sale, holds, or gives to another".

According to Sec. 263a StGB, the act of the unlawful influence is wide and it may be committed through the incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the order of events. Also any input, alteration, deletion or suppression of computer data that cause a loss of property to another person could be criminalised. Sec. 263a StGB does not provide for these illegal acts. Nevertheless, German legislation has used a wide expression ("other unauthorised influence on the order of events") that could include also these acts.

Sec. 263a StGB goes beyond the provision of Article 8 CoC, criminalising in addition those acts of preparation of computer fraud consisting in manufacturing computer programs, the purpose of which is to commit such an act, obtains, offers for sale, holds, or gives to another.

The provision against computer fraud contained in the Austrian Criminal Code is very similar. Sec. 148a Austrian Criminal Code criminalises:

> A person who, with the intent to enrich himself or a third person unlawfully, causes economic damage to another's property by influencing the result of automation-aided data processing through arrangement of the program, input, alteration or erasure of data (sect. 126a para. 2) or through other interference with the course of data processing.

The offence is punished with the imprisonment up to six months or to pay a fine up to 360 day-fines.

Sec. 184a, paragraph 2, provides for a aggravation circumstance if the person commits this offence professionally or causes damage exceeding 2,000 euros. In this case the offence is punished with imprisonment up to three years.

Article 49 of Romanian Law No. 161/2003 is also completely consistent with Article 8 CoC. It criminalises: "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". The offence is punished with imprisonment from 3 to 12 years.

Another model of full alignment is represented by Article 10 Cyprus Law 22(III) 04. According to Article 10, computer fraud is committed by:

> Any person who intentionally and without authority and with intent to defraud causes 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 the intent of procuring without right an economic benefit for oneself or for another person.

The perpetrator is liable to five years imprisonment or to a 20,000 Cyprus Pounds fine, or both.

Countries that have introduced a provision corresponding to Article 8 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Austria (Section 148a Penal Code)	Philippines (Article 4.B.3 Draft Law)
Cyprus (Article 10 Law No. 22(III)04)	
Germany (Section 263a)	
Italy (Article 640ter c.p.)	
Portugal (Article 221 Penal Code)	
Romania (Article 49 Law No. 161/2003)	

A lot of cybercrime offences are committed with the dishonest intent to gain an economic benefit. Today computer fraud represents one of the most frequent and dangerous offences in cyberspace. Nowadays more and more people shop on the Internet using a credit card, or deposit or transfer money using a home-banking system. It is not so difficult for the cyber criminals to obtain these personal data (credit card and bank account number, etc.) and use them to gain illegal economic benefits. The computer fraud, as with the other cybercrime offences, assumes a transnational character in the cyberspace, because the criminals may easily actuate from a country and interfere online with the functioning of a computer system that is situated in another country.

By way of conclusion, it is advisable that the Parties implement their domestic law in accordance with the provision of Article 8 CoC, introducing a common offence about computer fraud.

They could take the German or Romanian provision into consideration as model of legislation, as seen above.

3.8 Offences related to child pornography

> Article 9 CoC:
> 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.
>
> 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.
> 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.

The new technologies, and in particular the ever-increasing use of the Internet, have allowed Internet users to easily and quickly share every kind of file. Nowadays it is very easy to share not only music, movies and information, but also materials with pornographic or illegal character. In particular there are a lot of forums, chat-rooms or web communities where it is very easy to share pictures, images or materials concerning children engaged in sexually

conducts in real time. The increase in this business is due to the ease with which material can be exchanged at low cost from all over the world, and with the probability to avoid the control of the police.

In order to protect children from exploitation and to combat the traffic of children and pornography committed by means of a computer system, the Cybercrime Convention has introduced a specific criminal offence in the Article 9 CoC.[117] This choice is advisable and in compliance with the international trend that seeks to ban child pornography.[118]

Article 9 CoC defines "child pornography" as material in which a minor is represented engaged in sexually explicit conduct or a person appearing to be a minor engaged in sexually explicit conduct (virtual pornography), or realistic images representing a minor engaged in sexually explicit conduct.

For the provision "minor" is a person under 18 years old, as defined by Article 1 UN Convention on the Rights of the Child. Nevertheless, the definition varies from country to country. For this reason, paragraph 3, Article 9 CoC of the provision gives to the Parties the possibility to require a lower age-limit, although it must be not less than 16 years old.

Not all the countries that have already ratified the CoC have covered or adequately implemented Article 9 CoC.[119] Some legislations do not define the terms "child pornography" and "minor".[120] Other countries define a minor as a person under 16 years old or younger.[121]

The provision criminalises a wide list of acts: *production, offering, making available, distribution, transmitting, procuring, possessing* child pornography.[122] All the acts must be committed through a *computer system*, but few national legislations require expressly that the offence be committed through it.[123]

A model of full implementation of Article 9 CoC is represented by Article 51, paragraph 1 of Romanian Law No. 161/2003. The Romanian offence criminalises:

> 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.

The perpetrator is punished with imprisonment from 3 to 12 years and denial of certain rights.

Romanian legislator has adopted a wide approach, criminalising all the conducts provided for by Article 9 CoC. For the purpose of Article 51, the term "child pornography" is defined, in accordance with the criteria established by Article 9, paragraph 2 CoC, by Article 35i) Law No. 161/2003, regarding "pornographic materials with minors".

The German legislation partially covers Article 9 CoC. Section 184b StGB ("Dissemination, Purchase and Possession of Pornographic Writings involving Children") criminalises a wide

---

117 Explanatory Report, 91.

118 See for example Optional Protocol to the UN Convention on the rights of the child and other European Commission initiative (i.e. Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography).

119 Albania (Article 117 Criminal Code), Armenia (Article 263 Criminal Code), Bulgaria (Article 159(3)(4) Criminal Code), Croatia (Article 179a OG 105/04); Estonia (Article 309 Criminal Code), Ukraine (Article 301 Criminal Code).

120 Albania (Article 117 Criminal Code), Armenia (Article 263 Penal Code), Cyprus (Article 11 Law No. 22(III04 defines only "child pornography"), Croatia (Article 197 a OG 105/04), France (Article 227(23-24) Code Penal), Lithuania (Article 162, 309 Criminal Code), Slovakia (Sec. 368-370 Criminal Code Act), Turkey (Article 226(4) Criminal Code).

121 Germany (Sec. 184b StGB), Portugal (Article 172 Criminal Code), Serbia (Article 185 Penal Code), Estonia (Articles 177, 178 Criminal Code).

122 Explanatory Report, 93.

123 Cyprus (Article 12(1) Law No. 22(III)04), Italy (Article 600ter Criminal Code), Romania (Article 51(1) Law 161/2003), France (Article 227-23 Code Penal).

range of acts consistent with Article 9 CoC.[124] The offence punishes in particular:

> (1) whoever disseminates pornographic writings (section 11 subsection (3)) that have as their object the sexual abuse of children, publicly displays, posts, presents or otherwise makes them accessible; or produces, obtains, supplies, stocks, offers, announces, commends or undertakes to import or export them, in order to use them or copies made from them within the meaning of numbers 1 or 2 or makes such use possible by another; (2) Whoever undertakes to obtain possession for another of pornographic writings involving children that reproduce an actual or true to life event.

The offence is punished with imprisonment for three years to five years. If the perpetrator acts on a commercial basis or as a member of a gang that has combined for the continued commission of such acts, an imprisonment for 6 months to 10 years shall be imposed. If the perpetrator undertakes to obtain possession of pornographic writings involving children that reproduce an actual or true to life event, this shall be punished with imprisonment for up two years or a fine.

All these acts regard "pornographic writings" that have as object the sexual abuse of children. In accordance with Sec. 11, subsection 3, the writings are "audio and visual recording media, data storage media, illustrations and other images".

According to Article 9, paragraph 3 CoC the term "minor" includes all persons under 18 years of age or at least not less than 16 years old. Therefore an amendment of the offence should be necessary with respect to the age of the person involved (currently a person under the age of 14).

A model of good practice is represented by Article 227-23 of French Criminal Penal Code, that complies with the requirements established by Article 9 CoC, except the definitions of terms "child pornography" and "minor".[125] Article 227-23 Code Penal covers various acts of production, distributing, diffuse, offering and possession of a material (image or representation) of a minor having a pornographic character. The offence does not expressly define the concept of "pornographic character" ("*caractère pornographique*"). According to Article 227-23, paragraph 4 Code Penal the images of a person appearing to be a minor also have a pornography character.

Article 227-23, paragraph 3 Code Penal goes beyond the aim of Article 9 CoC, sanctioning in addition the habitual consultation of a web page or any resource publicly accessible – for example on the Internet - ("*service de communication*") that makes available such material. The conduct is punished with imprisonment of up to 10 years and a fine of up to 30,000 euros.

The basic offence is punished with imprisonment of up to five years and a fine of up to 75,000 euros. The penalty is increased (imprisonment up to seven years and fine up to 100,000 euros) by Article 227-23, paragraph 2, Code Penal if the perpetrator uses a communication network ("*réseau de communications éléctroniques*"). According to Article 227-23, paragraph 3 Code Penal, the attempt is punished with the same sanction.

Countries that have introduced a provision corresponding to Article 9 CoC:

---

[124] For a comment see Hilgendorf E., Frank T., Valerius B., *Computer-und Internetstrafrecht*, cit. p. 100; Hornle, *Pornographische Schriften im Internet; die Verbotsnormen im deutschen Strafrecht und ihre Reichweite*, NJW, 2002, p. 1008.

[125] Article 227-23 French Criminal Code provides for: *(1)* "*Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende. (2) Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines. Les peines sont portées à sept ans d'emprisonnement et à 100 000 Euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques*".

European countries (full alignment)	Non-European countries (full alignment)
Austria (Section 207a Criminal Code)(II)	Australia (Section 474.19; 474.20; 474.21)
Cyprus (Article 12 (1) Law No. 22(III)04)	
France (Article 227-23/24 Code Penal)	
Italy (Article 600*ter*, *quarter* Code Penal)	
Romania (Article51(1) Law No. 161/2003)	

In conclusion, it is advisable that all the countries provide a common definition of the terms "minor" and "child pornography".

It should be taken into consideration moreover the opportunity to also criminalise the conducts of possession, offering, making available, distributing, transmitting or procuring pornographic material that depicts "a person appearing to be a minor engaged in sexually activities" or "realistic images representing a minor engaged in sexually activities". That could permit a reduction in the market and the requests of pornographic material concerning "children" on the Internet that could be used to encourage or seduce minors into taking part in sexual conducts and hence form part of a subculture favouring child abuse.[126]

3.9 Offences related to infringement of copyright and related rights

> Article10 CoC:
> 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.

The development of new technologies has increased the possibilities for Internet users to duplicate and copy each kind of file concerning movies, music, videos, games, computer programs and other literature and artistic works at a low cost, even before they are performed or before the première. It is extremely frequent to find a lot of copies of protected works on the Internet without the consent of the copyrights holders. Their quality is frequently very good and thanks to their quick reproduction through free computer programs and devices it is not so difficult to find on the Internet. In particular, there are a lot of tools that enable the users to copy DVD's and CD's, even if they are protected by Digital Rights Management (DRM) systems.

The ever-increasing use of the file-sharing systems (i.e. P2P) has caused huge economic damage to the companies that have the copyright, and other related rights to these protected works. In order to defend their copyright they try to implement a new technical mechanism (DRM) every day, with the scope to prevent the copy and illegal diffusion of their

126 Explanatory Report, 103.

reproduction. But this strength appears not enough to protect the infringements of intellectual property rights.

With the aim to protect these copyrights, the CoC has included a specific criminal provision in Article 10 CoC covering the offences against the copyright and other rights. Nevertheless, in order to avoid an over-criminalisation, the provision has introduced some important requisites. The most important is the necessity that the illegal conduct is committed "on a commercial scale" and "by means of a computer system". That is consistent with Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which requires the infringement of copyright to be criminalised only in the case of "piracy on a commercial scale".[127]

According to Article 10, paragraph 3 CoC, Parties can provide other effective remedies (as civil and/or administrative measures) instead of criminal liability with regard to limited circumstances (e.g. parallel imports, rental rights).[128]

Unlike all other criminal provisions of the Cybercrime Convention, Article 10 CoC does not require for the criminal liability that the perpetrator must act "intentionally". Article 10 CoC requires instead that copyrights and neighbouring rights offences must be committed "wilfully", in line with the term employed by Article 61 of the TRIPS Agreement.[129]

Very few national legislations require that the infringement of copyright must be committed through a computer system.[130] General provisions for protecting copyrights and related rights do not address computer system as a means to commit the offences. Sometimes they use general expression as "in any manner" or "in any other way" that could extend the application of the provisions and cover Article 10 CoC.[131]

No country seems to require that the conduct must be committed on a commercial scale. Germany provides for an aggravation circumstance in the case where the acts are realised on a commercial basis.[132] Other countries use a different expression, requiring that the offences against the copyright and other rights are committed "for commercial purposes".[133] Some countries criminalise the infringement of copyright only where such actions caused a significant pecuniary loss.[134] This choice could be advisable in order to avoid an over-criminalisation, but the countries could take into consideration the opportunity to define the concept of significant loss.

A model of full implementation of Article 10 CoC is represented by Sections 106 ff. of the German Copyright Act (*Urheberrechtsgesetz*, UrhG), even if the German legislator does not expressly require that the infringement must be committed by means of a computer system.[135]

Sec. 106 ff UrhG (regarding the *unauthorized exploitation of copyrighted works*) criminalises the reproduction, distribution, or publicly communication of a work or an adaptation or transformation of it without the right of the holders. The offence is punished with

---

127 Explanatory Report, 114.
128 Explanatory Report, 116.
129 Explanatory Report, 113.
130 Armenia (Article 158 Criminal Code), Cyprus (Article 12 Law No. 22(III)04), Romania (Article 139(8),(9), 143 Law No. 8/1996).
131 Croatia (Article 230 OG 105/04), Bulgaria (Article 172a Criminal Code), Turkey (Article 71,72 Law No. 5846/1951); Albania (Article 50 Law on copyright); Hungary (Article 329a, 329c Law No. 4/1978).
132 Germany (Sec. 108b UrhG).
133 Cyprus (Article 12 Law No. 22(III)04); Estonia (Article 223,225 Criminal Code); Romania (Article 139, para 8, 139, para. 9, 143 Law No. 8/1996); Lithuania (Article 192 Criminal Code).
134 Armenia (Article 158 Criminal Code); Ukraine (Article 176 Criminal Code).
135 For a comment see Hilgendorf E., Frank T., Valerius B., *Computer-und Internetstrafrecht*, 2005, p. 162. About German copyright offences see more generally Czychowski, *Das Gesetz zur Regelung des Urheberrecht*, GRUR, 2001, p. 1106; Abdallah, Gercke, Reinert, *Die Reform des Urheberrechts. Hat der Gesetzgeber das Strafrecht übersehen?*, ZUM, 2004, p. 31.

imprisonment for up to three years or a fine. Sec. 106, paragraph 2 UrhG also criminalises the attempt.[136]

The same sanctions are provided for by Sec. 107 UrhG with regard to *the unlawful affixing of designation of author* committed without the author's consent.[137] Section 108 UrhG, concerning *infringement of neighbouring rights*, criminalises the reproduction, distribution or public communication committed other than in a manner allowed by law and without the right holder's consent of a scientific edition, a photograph, an audio, broadcast, video or a database.

All these conducts are punished with imprisonment for up three years or a fine.[138] Sec. 108a UrhG provides for a heavier sanction (imprisonment up to five years or a fine) if the unlawful exploitations mentioned above are committed on a commercial basis.

In order to anticipate the protection of copyright and related rights, the German legislator also criminalises with Sec. 108b UrhG the unauthorised interference with technical protection measures and information necessary for rights management. In particular, Sec. 108b, subsection 1, UrhG punishes the circumvention of an effective technical measure without the consent of the right holder. The offence is punished only if the perpetrator does not act for an exclusive private use. In this case the offence is punished with imprisonment for no more than one year or a fine. The offence provides for an aggravation circumstance if the conduct is committed on a commercial basis. In this case the penalty shall be punished with imprisonment of no more than three years or a fine.

Completely consistent with the requirements established by Article 10 CoC is Article 12, paragraph 1, Cyprus Law No. 22(III) 04. According to Article 12, paragraph 1, an illegal infringement of copyright is committed by "any person who intentionally does for commercial reasons any act through a computer system which according to the Intellectual property and related rights law of 1976 violates Intellectual property right or relative right".

French copyright provisions are not consistent with Article 10 CoC.

Article L111-1 refers only to general principles of copyright. Article R111-1 concerns the nature of the copyright; Article L112-1, L112-2 determines the protected works: books, conferences, brochures, etc. Any provision of the *Code de la Proprieté Intellectuelle* provides for a criminal offence for the infringement of copyright as required by Article 10 CoC. For this reason it could be advisable that the French legislator introduces a specific provision about the infringement of copyright, criminalising such acts committed wilfully on a commercial scale and by means of a computer system as required by Article 10 CoC.

Romanian copyright legislation is not completely consistent with Article 10 CoC. Articles

[136] Sec. 106 UrhG: "1) Whoever reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, other than in a manner allowed by law and without the right holder's consent, shall be punished with imprisonment for up to three years or a fine.(2) An attempt shall be punishable".

[137] Sec. 107 UrhG: "(1) Whoever 1. without the author's consent, affixes a designation of author (section 10 subsection (1)) to the original of a work of fine art or distributes an original bearing such designation, 2. affixes a designation of author (section 10 subsection (1)) on a copy, adaptation or transformation of a work of fine art in such manner as to give to the copy, adaptation or transformation the appearance of an original or distributes a copy, adaptation or transformation bearing such designation, shall be punished with imprisonment for up to three years or a fine provided the offence is not subject to a more severe penalty under other provisions. (2) An attempt shall be punishable".

[138] Sec. 108 UrhG: "1) Whoever, other than in a manner allowed by law and without the right holder's consent: 1. reproduces, distributes or publicly communicates a scientific edition (section 70) or an adaptation or transformation of such edition; 2. exploits a posthumous work or an adaptation or transformation of such work contrary to section 71; 3. reproduces, distributes or publicly communicates a photograph (section 72) or an adaptation or transformation of a photograph; 4. exploits a performance contrary to section 77 subsection (1) or (2) or section 78 subsection (1); 5. exploits an audio recording contrary to section 85; 6. exploits a broadcast contrary to section 87; 7. exploits a video or video and audio recording contrary to section 94 or section 95 in conjunction with section 94; 8. uses a database contrary to section 87b (1), shall be punished with imprisonment for up to three years or a fine. (2) An attempt shall be punishable".

139.8, 139.9, 143 of the Romanian Copyright Law No. 8/1996 cover Article 10 CoC, except in the part which the provision requires that the acts consisting in an infringement of copyright or related rights be committed "on a commercial scale". That could determine an over-criminalisation, sanctioning not only the conducts that cause a significant economic damage to the copyright and related rights holders, but also to the private conducts that do not have relevant economic consequents. In these lighter cases, the possibilities to sanction the conducts with an administrative or civil sanction should be taken into consideration.

Article 139.8. Law No. 8/1996 criminalises the infringement of copyrights or related rights, consisting in making available protected work to the public through Internet or other networks, without the consent of the owners of them, and permitting access to these work to the public.[139] The offence is punished with imprisonment from one to four years and a fine.

Article 139.9 Law No. 8/1996 criminalises the unauthorised *reproduction* in through a computer system of computer software.[140] The notion of reproduction must be interpreted as *installing*, *running* or *executing* or *displaying* the software. The offence is punished with imprisonment from one to four years or a fine.

Article 143, paragraph 1, Law No. 8/1996 criminalises the act of manufacturing, importing, distributing or rental, offering without right and in view of sale, rental or possess for sale, devices or components that permit the neutralisation of technical measures of protection.[141] The same punishment is provided for the performing services that lead to the neutralising of technical measures of protection. Both the offences are punished with imprisonment from three months to three years.

Article 143, paragraph 2, Law No. 8/1996[142] criminalises the act which, without the consent of copyright holders, causes or conceals a violation of their copyrights in two manners:

> Removing or modifying any electronic information concerning the applicable regulations on copyrights or connected rights, of the protected works for commercial purposes.
>
> Distributing, importing in view to distribute, broadcast or publicly communicate or make available to the public, or allow access from anyplace and to any time, without right works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights.

The conducts provided by Article 143, paragraph 2 a), b), are punished with imprisonment from three months to three years.

Countries that have introduced a provision corresponding to Article 10 CoC:

---

[139] Article 139.8 Law No. 8/1996: "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".

[140] Article 139.9 Law No. 8/1996: "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".

[141] Article 143, para 1, Law No. 8/1996: "(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 neutralization of technical measures of protection or that perform services that lead to neutralization of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment".

[142] Article 143, para 2, Law No. 8/1996: "(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 authorization".

European countries (full alignment)	Non-European countries (full alignment)
Armenia (Article 158 Criminal Code)	Brazil (Law No. 9609/98; Law No. 9610/98; Law No. 10695/2003)
Croatia (Articles 230-231 Penal code) (II)	
Cyprus (Article 12, Law No. 22(III)04)	
Germany (URHG)	
Italy (Article 171*bis* ss. L. 633/1941)	
Albania (Article 50 Law on Copyright)	
Austria (Sec. 91 Federal Law on Copyright) (II)	
Bulgaria (Article 172a Penal Code)	
Ukraine (Articles 176, 216 Criminal Code;	

In conclusion, it is advisable that all the countries implement Article 10 CoC, introducing a criminal offence in order to criminalise the infringement of copyrights committed by means of a computer system.

In order to avoid an over-criminalisation, they should criminalise only the acts committed on a commercial scale. That could avoid the criminalisation of the conducts of reproduction of files committed by private Internet users. In these cases, the legislators could apply other lighter sanctions, such as civil or administrative sanctions, or implement effective remedies such as new technical mechanism (DRM), with the aim to prevent the copy and illegal diffusion of their reproduction.

3.10 Attempt and aiding or abetting

> Article 11 CoC
>
> 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.

The aim of this provision is to establish additional offences with regard to attempt and aiding or abetting the commission of the cybercrime offences, defined under Articles 2-10 CoC.[143] The Parties are not bound to criminalise the attempt to commit each offence established in the Cybercrime Convention. It is only required, by Article 11, paragraph 2, CoC, that the attempt be criminalised with regard to the offences provided for by Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c) CoC. The Parties are only bound to establish as a criminal offence the aiding or abetting of the commission of any of the offences provided for by Articles 2-10 CoC.[144] Not only should the perpetrator of the offence be sanctioned, but also the person who has aided him with the intent that the crime be committed.

With regard to cyber threats, the criminalisation of the aiding and abetting is very important because in a lot of cases the perpetrator needs the assistance and the help of third parties (service provider, system operators, insiders, etc.).

[143] Explanatory Report, 118.
[144] Explanatory Report, 118.

The majority of the countries analysed provide for the criminal liability for attempt, aiding or abetting a crime in their criminal code. However, the additional offences related to attempt and aiding or abetting the commission of criminal offences should be established in connection with the offences defined in the Cybercrime Convention. Nevertheless, this solution is not necessary for the correct implementation of the CoC. In a lot of countries these offences are regulated by the general provisions of the criminal code.

The implementation into domestic law of the Parties of Article 11 CoC does not create particular problems. Aiding, abetting and aiding are already criminalised in most of national systems.

The French criminal legislation complies with the requirements established by Article 11 CoC. Article 11, paragraph 1, CoC is covered by the general provisions concerning the attempt contained in French Criminal Code. Article 11, paragraph 2, CoC is fully covered by Article Articles 323-7 Code Penal.

The German criminal legislation is also completely consistent with Article 11 CoC. Article 11 CoC is fully covered by the general provisions of the German Criminal Code (StGB). In particular, attempt is covered by sections 22-24 StGB. Aiding and abetting are covered by sections 26 and 27 StGB.[145]

The country profile for Romania does not identify any specific offence related to aiding or abetting as provision corresponding with Article 11, paragraph 1 CoC, Nevertheless, it does not mean that the Romanian legislation is not consistent with Article 11, paragraph 1 CoC. There is no reason to believe that the general provisions of the Romanian criminal code can be extended to the cybercrime offences.

The country profile identifies Articles 47, 50, 51, paragraph 2 Law No. 161/2003 as provision corresponding with Article 11, paragraph 1 CoC., regarding "attempt". The Romanian legislator reserves, in accordance with Article 11, paragraph 3, CoC, the right to apply only in part paragraph 2 of Article 11 CoC, criminalising the attempt only with regard to *computer forgery* (Article 47 Romanian Law No. 161/2003), *computer fraud* (Article 50 Law No. 161/2003) and offences related to *child pornography thorough computer system* (Article 51, paragraph 3 Law No. 161/2003).

[145] Sec. 22 StGB (Definition of Terms): "Whoever, in accordance with his understanding of the act, takes an immediate step towards the realisation of the elements of the offence, attempts to commit a crime". Sec. 23 StGB (Punishability for an attempt): "(1) An attempt to commit a serious criminal offence is always punishable, while an attempt to commit a less serious criminal offence is only punishable if expressly provided by law. (2) An attempt may be punished more leniently than the completed act (section 49a subsection (1)). (3) If the perpetrator, due to a gross lack of understanding, fails to recognise that the attempt could not possibly lead to completion due to the nature of the object on which or the means with which it was to be committed, the court may withhold punishment or in its own discretion mitigate the punishment (section 49 subsection(2)"). Sec. 24 StGB (Abandonment): "(1) Whoever voluntarily renounces further execution of the act or prevents its completion shall not be punished for an attempt. If the act is not completed due in no part to the contribution of the abandoning party, he shall not be punished if he makes voluntary and earnest efforts to prevent its completion. (2) If more than one person participate in the act, whoever voluntarily prevents its completion will not be punished for an attempt. However his voluntary and earnest efforts to prevent the completion of the act shall suffice for exemption from punishment if the act is not completed due in no part to his contribution or is committed independently of his earlier contribution to the act".

Countries that have introduced a provision corresponding to Article 11 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Albania (Articles 23,27 Criminal Code - General provision)	Egypt (Article 38 Draft law)
Armenia (39rt. 33.3, 33.2, 39 Penal Code)	Mexico (General Rules of the Code)
Austria (Section12 and 15 Penal Code)	Philippines (Sec. 8 Draft Law)
Bulgaria (Articles 18, 20-22 PC)	Sri Lanka (Articles 11,12 Computer Crime Act, No. 24/2007)
Cyprus (Article 13 Law No. 22(III)04)	
FYRoM (Articles 24(1), 19, 251(7) Criminal Code)	
Germany (sections 22-24 StGB; 26 and 27 StGB)	
Italy (39rt. 56 c.p.; 110 c.p.)	
Portugal (Articles 22, 23, 27 Penal code)	
Slovakia (SEC. 14 (1), 20, 21(1)d of the Criminal Code Act no 300/2005 Coll)	
Turkey (Articles 35, 37-40 Penal Code)	
France (GP Criminal Code)	
Estonia (Articles 20, 21, 22, 25, 26 Criminal Code)	
Ukraine (Articles 13(2), 15, 26-27, 29 Criminal Code)	
Serbia (Article 35 Criminal Code)	

By way of conclusion, it is advisable that all the countries provide to criminalise the attempt, abetting and aiding, in accordance with the prescription of the CoC. They have two possibilities: the first one consists in the insertion of common provisions regarding attempt, aiding operating for all the offences into the Penal Code; the second one is to introduce specific offences with regard to the provisions provided the CoC. Both are fully consistent with the CoC.

3.11 Corporate liability

> Article 12 CoC:
> 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.
>
> 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.
> 2. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
>
> 3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 12 CoC is in line with the international legal trend to recognise corporate liability.[146]

[146] Explanatory Report, 123. With regard to the liability of legal persons, see also Article 8 EU Framework Decision on

The aim of the provision is to impose liability on corporations, associations and similar legal persons (Internet Service Providers, business, etc.) for the criminal actions undertaken by a natural person in a leading position within such legal person, and for the benefit of that one.[147] The term "person who has a leading position" refers to a person who has a high position in the management of a legal person (e.g. director, chairman of the executive committee, responsible person of the organisation, etc.).

At the same time, Article 12 CoC provides for a liability where a criminal action was committed by an employee or an agent of the legal person, without power of representation, and was able to do so because a leading person failed to supervise or control him.[148] After all, according to the requirements of the Article 12 CoC, a legal person can be held liable if four conditions are met:

1. One of the computer and cybercrime offences provided for by Articles 2-10 CoC must have been committed;
2. The offence must have been committed for the benefit of the legal person;
3. A person who has a leading position must have committed the offence (including aiding and abetting);
4. The person who has a leading position must have acted on the basis of one of these powers (power of representation, authority to take decision, power of direction or organisation, etc.).

The Convention leaves the contracting Parties free to decide the type of liability (criminal, civil or administrative). Parties can choose one or all of these types of liability, in accordance with their legal principles. Nevertheless, they should respect the criteria established by Article 13 CoC, providing for effective, proportionate and dissuasive sanctions and also including monetary sanctions. In order to evaluate if the domestic law of the Parties complies with the requirements of Article 13 CoC, it could be necessary to also evaluate the civil or administrative law provisions, but it is not possible in this study to make this further analysis.

Not all the countries analysed in this study have already implemented Article 12 CoC.[149] Article 12 CoC is partially covered by Articles 19 and 53 of the Romanian Criminal Code, amended by Law No. 278/2006. According to Article 19 Romanian Criminal Code[150], concerning the conditions for the criminal liability of the legal persons, they shall be criminally liable for criminal offences committed by a natural person only in three cases: (1) in order to activate in their activity field; (2) in the interest of them; (3) on behalf of them. Article 19 Romanian Criminal Code does not establish any criteria in order to determine the natural person that has actuated for the benefit or behalf of the legal person.

Attacks against Information Systems: "Each Member State shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: (a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person. 2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority. 3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of the offences referred to in Articles 2, 3, 4 and 5".

147 Explanatory Report, 123.

148 Explanatory Report, 123.

149 See i.e. Albania, Armenia, The Czech Republic, Serbia, Ukraine or "the former Yugoslav Republic of Macedonia".

150 Article 19 of the Romanian Criminal Code (amended by Law No. 278/2006): "Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence".

On the contrary, Article 12 CoC specifies seasonably that the natural person, that actuates either individually or as a member of an organ inside the legal person, must have a specific leading. Moreover, it does not provide a "passive" hypothesis of corporate liability for the legal persons if the commission of the offence realised by the natural person that has a leading position inside the legal person was responsible for the lack of supervision or control by the legal person.

Article 53 of the Romanian Criminal Code provides for the types of penalties applicable to legal persons. They are divided into main and complementary. The main penalty consists in a fine from RON 2,500 to RON 2,000,000. There are five complementary penalties: a) dissolution of the legal person; (b) suspension of the activity of the legal person for a period from 3 months to one year or suspension of that of the activities of the legal person which served in the perpetration of the offence, for a period from 3 months to 3 years; (c) closing of working locations belonging to the legal person, for a period from 3 months to 3 years; (d) prohibition to participate in public procurement for a period from one to 3 years; (e) display or broadcasting of the sentencing judgment.

Article 12 CoC is fully covered by Sections 30 and 130 of the German Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OwiG), except for the case where the natural person acts individually, as provided for by Article 12, paragraph 1 CoC. Sec. 30 OWIG ensures that legal persons are liable for a criminal offence or regulatory offence committed by a natural person having a leading position. The legal person shall be liable and punished with a regulatory fine if the natural person has committed a criminal offence or a regulatory offence, as a result of which duties incumbent on the legal person have been violated, or where the legal person has been enriched or was intended to be enriched.[151] According to Sec. 30 OWIG, the amount of regulatory fine is different depending on: (1) the criminal offence is committed with intent (fine to not more than 1 million Euros); (2) the criminal offence is committed with negligence (fine to not more than 500,000 Euros).

Sec. 130 OWIG criminalises the owner of an operation or undertaking if he has intentionally or negligently omitted to take the supervisory measures required to prevent contravention, and this lack of supervision or control would have prevented or made much more difficult the commission of the contraventions. The required supervisory measures also comprise appointment, careful selection and surveillance of supervisory personnel.[152]

---

[151] Section 30 OWIG: "(1) Where a person acting: 1. as an entity authorised to represent a legal person or as a member of such an entity, 2. as chairman of the executive committee of an association without legal capacity or as a member of such committee, 3. as a partner authorised to represent a partnership with legal capacity, or 4. as the authorised representative with full power of attorney or in a managerial position as procura holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3, 5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position, has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association. (2)The regulatory fine shall amount: 1. in the case of a criminal offence committed with intent, to not more than one million Euros,; 2. in the case of a criminal offence committed negligently, to not more than five hundred thousand Euros. Where a regulatory offence has been committed, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence at issue. The second sentence shall also apply where an act simultaneously constituting a criminal offence and a regulatory offence has been committed, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the maximum pursuant to the first sentence. (3) Section 17 subsection 4 and section 18 shall apply mutatis mutandis. (4) If criminal proceedings or proceedings to impose a regulatory fine are not instituted in respect of the criminal offence or the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. However, independent assessment of a regulatory fine against the legal person or association of persons shall be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1, second sentence, shall remain unaffected. (5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a forfeiture order, pursuant to sections 73 or 73a of the Criminal Code or pursuant to section 29a, against such person or association of persons".

[152] Section 130 OWIG: (1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties

Another model of full implementation of Article 12 CoC is represented by French criminal legislation, Articles 323-6 Code Penal.[153] The criminal corporate liability for the legal persons is based on the conditions provided by Article 121.2 Code Penal. The liability of the legal persons has a criminal nature and is punished with a fine in accordance with the criteria provided for by Article 131-38 ("*amende*"), Article 131-139, and Article 131-139, paragraph 2 Code Penal ("*interdiction*").

Section 3 of the Austrian Federal Statute on Responsibility of Entities for Criminal Offences (VbVG)[154] is also completely consistent with the requirements of Article 12 CoC.

Countries that have introduced a provision corresponding to Article 12 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Austria (Section 3 of the Federal Statute on Responsibility of Entities for Criminal Offences (*Verbandsverantwortlichkeitsgesetz – VbVG*))	Sri Lanka (For Article 12(1) see Articles 30(a-b), for Article 12(2) see Article 30© Computer Crime Act No. 24/2007)
Cyprus (Article 14 Law No. 22(III)04) (II)	
France (Article 323-6 Code Pénal)	
Germany (sections 30 and 130 of the German Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OwiG)).	
Lithuania (Article 22 Penal Code)	
Portugal (Law No. 109/91 (17 August) – Article 10(5))	
Romania (Article 19 of Criminal Code)	
Croatia (Law on liability of legal entities OG 151/03)(II)	
Italy (Article 24bis D.lgs. No. 231/2008)	

By way of conclusion, it is advisable that all the countries recognise corporate liability for the criminal actions undertaken for the benefit of the legal person and committed by a natural person acting under its authority. The corporate liability should not however exclude

incumbent on the owner as such and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel. (2) An operation or undertaking within the meaning of subsection 1 shall include a public enterprise. (3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum regulatory fine imposable for the breach of duty. The second sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine imposable for the breach of duty exceeds the maximum pursuant to the first sentence.

[153] Article 323-6 French Criminal Code : "*Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre. Les peines encourues par les personnes morales sont : 1º L'amende, suivant les modalités prévues par l'article 131-38 ; 2º Les peines mentionnées à l'article 131-39. L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise*".

[154] Sec. 3 VbVG: "(1) Subject to the additional conditions defined in paragraphs 2 or 3 an entity shall be responsible for a criminal offence if 1. the offence was committed for the benefit of the entity or 2. duties of the entity have been neglected by such offence. (2) The entity shall be responsible for offences committed by a decision maker if the decision maker acted illegally and culpably. (3) The entity shall be responsible for criminal offences of staff if 1. the facts and circumstances which correspond to the statutory definition of an offence have been realised in an illegal manner; the entity shall be responsible for an offence that requires willful action only if a staff has acted with willful intent, and for a criminal offence that requires negligent action only if a staff has failed to apply the due care required in the respective circumstances; and 2. commission of the offence was made possible or considerably easier due to the fact that decision makers failed to apply the due and reasonable care required in the respective circumstances, in particular by omitting to take material technical, organizational or staff related measures to prevent such offences. (4) Responsibility of an entity for an offence and criminal liability of decision makers or staff on grounds of the same offence shall not exclude each other".

individual liability.

3.12 Sentences and measures

> Article 13 CoC
> 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.

This provision obliges the Parties to provide for criminal sanctions to ensure that computer crimes established by Articles 2-11 CoC be punished with effective, proportionate and dissuasive sanctions.

The Convention leaves the contracting Parties free to decide the type and the level of the sanctions.[155] They can have criminal, administrative or civil nature, including the possibility to provide for monetary sanctions on legal persons.[156] This discretionary power must respect however the principles of criminal policy. The criminal sanctions must be "effective, proportionate and dissuasive" as provided for by Article 13 CoC. It is not easy to define whether the national provisions concerning sanctions are "effective, proportionate and dissuasive". For this reason it would be necessary to analyse the sentencing practice of national courts, but in this study it is not possible.

In a lot of countries most of the offences provided in Articles 2-11 CoC are not adequately covered by criminal sanctions as well as criminal liability for legal persons. Not all the countries have criminalised the offences with criminal sanctions. It is for example the case of India, which has provided for administrative sanctions in the majority of the cases.[157]

The majority of the countries provide for criminal or administrative sanctions for the legal persons, in accordance with Article 12 CoC. On the contrary, other countries do not yet provide liability for legal persons.[158]

Austria provided for that the offender is prosecuted only with the consent of the offended party with regard to some computer offences. That could limit the prosecution of computer crimes. But it is a choice of criminal policy. Italy also limits the criminalisation of some offences (i.e. illegal access or computer related fraud) in the presence of the consent of the offended party.

Article 13 CoC is covered by general provisions of theFrench Criminal Code. In order to evaluate the agreement of the French sentences with Article 13 CoC, it would be necessary to take into consideration the sentencing practice of French courts, but there is not any element to affirm that the French legislation does not meet the requirements of Article 13 CoC.

Article 13 CoC is fully covered also by the general provisions of German Criminal Code, and with regard to the corporate liability, by the provisions of German Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OWiG). In particular, Article 13 (1) CoC is covered by Sections 202a, 202b, 202c, 263a, 269, 303a, 303a StGB and section 106 UrhG. Article 13 (2) CoC is covered by section 30 OWiG.

---

155 Explanatory Report, 131.
156 Explanatory Report, 129.
157 See Kaspersen H.W.K., *Comparative Analysis of the Criminal Law of India in view of its compatibility with the requirements of the Convention of Cybercrime of the Council of Europe* (a discussion paper), in Council of Europe, The Project on Cybercrime.
158 See for example Armenia, "the former Yugoslav Republic of Macedonia", Ukraine, Albania, Serbia or India.

Romanian legislation is also completely consistent with Article 13 CoC. With regard to the criminal sanctions, it must be underlined that each offence has its specific punishment. All computer and computer-related offences provided for by Article 42-51 Romanian Law No. 161/2003 are punished with the deprivation of liberty. As mentioned, above it would be necessary to take into consideration the sentencing practice of the Romanian courts in order to value if the offences are punishable with effective, proportionate and dissuasive sanctions. Concerning the sanction for the legal person, see the consideration mentioned above sub paragraph 1.12.

Countries that have introduced a provision corresponding to Article 13 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Austria (Section 118a, 119, 119a, 126, 126b, 126c, 148a, 225a. 207a of Penal Code and Section 91 of the Federal Law on Copyright in Work of Literature and Art and on Related Rights; Section 4 of the Federal Statute on Responsibility of Entities for Criminal Offences)	India
Bulgaria (Articles 171(1)-(3), 172a, 159,212a, 216(3), 319a, 319e Penal Cod; Article 83a Law on Administrative Offences and Sanctions)	Mexico (Articles 211 bis 1 to 211 Bis 7 Penal Code)
Croatia (44rt. 197. Articles, 223, 223. A, 224. A, 230, 231 and Article 174. Paragraph 4. – Protocol (OG 105/04.)	Sri Lanka
Cyprus (Articles 4-7, 9-12 Law No. 22(III)04)	Brazil
France (Article 323-6 Code Penal;GP)	USA
Germany (sections 202a, 202b, 202c, 263a, 269, 303a, 303a StGB and section 106 UrhG; section 30 OWiG)	
Hungary (Articles 204, 300(C, 300/E, 329/A-329/C Law No. 19/1998 Criminal Code)	
Italy (GP)	
Lithuania (GP)	
Portugal (GP)	
Romania (Articles 42-46, 48-49 and 51 of Romania Law No. 161/2003; Article 53 of Criminal Code)	
Serbia (General provisions on Penal Code)	
Slovakia (Sections 196,247,369, 283 Criminal Code Act No. 300/2005)	
Turkey (GP)	
Estonia (GP)	

By way of conclusion, it is advisable that each country provides for criminal sanctions that are effective, proportionate and dissuasive. A useful criteria in order to determine the nature of the sanction for each computer offence is represented by the fundamental principles of criminal policy (legality, *extrema ratio,* etc.). The national legislator would chose the sanction moving from the seriousness of the offences and the significance of legal interest (e.g. information security, confidentiality, integrity, availability of computer data and systems, etc.) offended by each offence.

4 Comparative review of the criminal procedure law

4.1 Introduction

One of the most important challenges in the fight against computer crime and cybercrime is the difficulty for the police, judicial, administrative and other law enforcement authorities, not only in identifying the "cyber criminals", but also in determining the *locus commissi delicti* and *tempus commissi delicti*.[159] It is also very difficult to determine the extent and impact of the criminal acts committed through the new technologies[160]. The principal reason is represented by the great possibility for the offenders to be almost completely anonymous in the cyberspace. Secondly it depends on the characteristic volatility of electronic data and evidence which can be altered, deleted or erased.

In order to warrant the success of the investigations, it is extremely important to therefore assure the speed and secrecy of the investigative techniques and the international co-operation between the national competent authorities.[161]

The Council of Europe Convention on Cybercrime has individuated and described some procedural measures to be taken at a national level for the purpose of improving the criminal investigations, and has fixed some general provisions in order to implement the international co-operation. First, the Convention has adapted the traditional procedural measures (i.e. search, seizure, interception) to the new technological environment.[162] Nevertheless, the technological revolution facilitates the possibilities to share data, information and communication through the electronic highways, giving more opportunities to the offenders to commit illegal acts in the cyberspace. The development of the network of communications has opened new doors for the cyber criminals, changing not only the traditional commission of the crimes but also some substantial aspects of the criminal law and criminal procedure.[163] That has led the Council of Europe to introduce some new procedural measures. In particular, the CoC contains specific provisions concerning the *collection of evidence in electronic form*, the *expedited preservation of computer and traffic data* (Article 16 CoC), *real-time collection of traffic data* (Article 20 CoC) and *interception of content data* (Article 21 CoC).

In accordance with Article 14 CoC, each Party shall adopt in its domestic law each measure, in order to apply the powers and procedures established with Section 2 CoC concerning procedural law with regard to: offences provided for by Articles 2-11 CoC, other offences committed through a computer system and to the collection of evidence in electronic form a criminal offence.[164] Article 14, paragraph 3, CoC provides for two exceptions to the aim of the provision. The first exception establishes that each Party may limit the power to intercept content data (Article 21 CoC) of specific computer communications or telecommunications with regard to a limited range of serious offences that are determined by domestic law.[165] The second exception gives to the Party the right to limit the application of Article 20 CoC concerning the real-time collection of traffic data only to those serious offences specified in the reservation. The range of this category of offences cannot be more restricted than the range of offences regarding the interception measure as established by Article 21 CoC.

---

[159] About these problems see, for example, Zoller M.A., *Verdachtlose Recherchen und Ermittlungen im Internet*, GA, 2000; Sieber U., *The International Emergence of Criminal Information Law*, 1992, p. 41.

[160] Yang D.W., Hoffstadt B.M., Essay, "Countering the Cyber-Crime Threat", in (43) 2006 *Am. Crim. L. Rev.*, 203. With regard to the economic impact of cybercrime see Katyal K.N., *Digital Architecture as Crime Control*, in (112) 2003 Yale L. J., 2261.

[161] Explanatory Report, 133.

[162] Explanatory Report, 134.

[163] Explanatory Report, 132.

[164] Explanatory Report, 141.

[165] Explanatory Report, 142.

The Parties have the discretional power to determine the modalities of establishing and implementing the power and procedure measures provided for by the CoC into its domestic law. Nevertheless, according to Article 15 CoC, they should include some conditions or safeguards into their domestic law, in order to balance the requirements of law enforcement provided for by the CoC and the protection of human rights and liberties.[166] The Cybercrime Convention does not specify in detail these conditions and safeguards but provides for including some general criteria referring back to obligations that each Party has undertaken under international human rights instruments.

4.2 Summary description of the procedural measures

The first two procedural measures provided for by the CoC are the *expedited preservation of stored computer data* (Article 16 CoC) and the *expedited preservation and partial disclosure of traffic data* (Article 17 CoC).

Data preservation power is a new investigative legal tool in most of the domestic laws. The aim of the provision is to guarantee the integrity of all these data that are easy to modify, destroy, alter or delete. Preserving and protecting the integrity of these data is very important for the success of a lot of investigations with regard to crimes committed in cyberspace. Most of the communications through the information systems may contain illegal content or evidence of criminal activities very important in identifying the perpetrators of the offence. The aim of the data preservation order is to avoid the risk of losing the critical evidence contained in these communications.

Both of the measures can only be applied to computer data that have already been collected and retained by data-holders (service providers, business, etc.). For this reason, data preservation must be distinguished by data retention. The aim of preservation is to secure and make safe data which already exist and are stored.

The concept of data must be interpreted in a wide manner, including all these data particularly subject to loss, delete or modification (for example, business, health, personal, sensitive, or other records data).[167]

Some European legal sources (Directive 95/46/EC, Directive 02/58/EC) provide for the prohibition for the holders to retain some types of data (personal data, traffic data, etc.). But these legal sources do not prevent member states from implementing the data preservation power into their domestic law, in order to preserve and secure specific data for specific and problematic investigations.

Neither of the articles specify how the data must be preserved. The provision gives to each Party the right to determine in their domestic law the specific manner of preservation. That means that in some cases the Parties could provide that the data could be "frozen" or could be rendered inaccessible.

In accordance with Article 16 CoC, in order to preserve "specified stored computer data", it must be directed to the person that has the possession or the control of data. The person who receives this order must be guaranteed for a period of time as long as necessary. But it can be not longer than 90 days, even if each Party may provide for subsequent renewal of it.

The preservation order is an important preliminary investigation measure. In order to guarantee the success of the investigation, each Party should adopt every measure capable of obliging the data-holders or the custodian to keep the undertaking of data preservation order confidential, so that the suspect of the investigation does not know that the law

[166] Explanatory Report, 145.
[167] Explanatory report, 161.

enforcement authority is investigating.

Only some states provide expressly for the power to order the data preservation in their domestic procedural law, as required by Article 16 CoC.[168] Some countries do not have specific provisions directly prescribed the expedited preservation and partial disclosure of computer and traffic data as provided for by Article 16 CoC.[169] In these cases computer data and traffic data could be preserved and obtained only through the traditional procedural measures such as search and seizure or production order. But the challenge of the fight against cybercrime requires that all the states implement these provisions, introducing the data preservation order into their domestic law.

A model of full alignment is represented by Sec. 90 Code of Criminal Procedure of the Slovak Republic.[170]

Article 54, Romanian Law No. 161/2003 is also completely consistent with Article 16 CoC. According to Article 54 Law No. 161/2003:

> 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.

Article 17 CoC (*expedited preservation and partial disclosure of traffic data*) provides for some obligations to preserve traffic data and to expeditious disclosure of some data in order to permit the identification of other service providers involved in the transmission of the communication.

Obtaining stored traffic data concerning communications is very important for the competent authority in order to discover the perpetrators of the cybercrime offences (i.e. distributed child pornography, illegal contents, computer viruses, malware programs, etc.). In most cases, one ISP does not posses enough traffic data to determine the source or destination of the communications. The aim of Article 17 CoC is to allow that the expeditious preservation of traffic data can be realised with regard to all the chain of ISPs that are involved in the transmission of the communications.

Each Party is free to determine how to achieve the preservation order. The best practice is to give the competent authorities the possibility to obtain a single preservation order operating for all the service providers involved. Another efficient solution could be to order to the

---

[168] Romania (Article 54 Law No. 161/2003), Sri Lanka (Article 19(1), (2), 24 (1,4) Computer Crime Act), and Slovakia (Sec. 90 Procedural Criminal Code).

[169] See i.e. Albania (Article 299, para. 1 Criminal Procedure Code), Armenia, Portugal (Article 6 Law No. 69/98); Estonia (Article 215 Criminal Procedure Code); Bulgaria (Article 159 Penal Procedure Code); Serbia (Article 85, para 1, 146, para. 1,7, Article 155 255, para 2) or France (Article 56, paragraph 7 Code de Procedure Penale). Germany has only a specific provision regarding the collection of traffic data (Sec 100g StPO), Portugal limits the preservation of traffic data to billing purposes (Article 6 Law No. 69/98 (26 October 1998)).

[170] Sec. 90 Criminal Procedure Code: (1) "If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a) storing and keeping completeness of such data; b) enabling production and keeping/possession of copies of such data; c) making access to such data impossible; d) removing from computer system such data; e) handing over such data for the purposes of criminal proceedings". (2) The order issued pursuant to the par. 1 must state a period of time during which data storage shall be carried out, maximum period is 90 days, and if repeated storage is necessary, new order shall be issued. (3) If storage is no longer necessary of computer data including traffic data for the purposes of criminal proceedings, presiding judge or prosecutor in the stage before the commencement of criminal prosecution or within pre-trial proceedings shall issue the order to cancel data storage without delay. (4) An order issued pursuant to the par. 1 to 3 shall be served on a person in whose possession or control the data are or to a service provider of such services; both of them may be imposed the obligation of keeping in secret the measures contained in the order".

service provider to notify the following service provider involved in the transmission chain.[171]

In order to determine if a ISP possesses all the crucial traffic data necessary for the success of the investigation, Article 17 CoC gives the competent authority the possibility to require the partial disclosure of the data from the ISPs. That allows the identification of any other service provider involved in the chain.

Some states do not have specific legislation in force consistent with Article 17 CoC.[172] Other countries do not have a specific provision.[173]

The country profile for France identifies Article 60-2, paragraph 2, Code de Procedure Penale as provision corresponding with Article 17 CoC. Nevertheless, Article 60-2, paragraph 2 seems to only partially cover Article 17 CoC. The provision does not refer expressly to traffic data but only to "content data" ("*contenu des informations consultées*"). Moreover, it does not ensure in fact 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 ISP's involved, as required by Article 17 CoC.[174]

Section 90 Slovak Criminal Procedure Code of Republic of Slovak and Article 54 Romanian Law No. 161/2003 are completely consistent with Article 17 CoC and could be taken as model of good practice.[175]

Another important procedural measure is the "production order", provided for by Article 18 CoC. The aim of the provision is to give to the competent authority the power to compel a person in its territory to provide specific stored computer data (Article 18, para. 1a) CoC), or to compel a ISP to furnish the subscriber information necessary for the criminal investigation that are in those persons' possession or control (Article 18, para. 1b CoC).[176] The concept of "subscriber information" is defined in Article 18, paragraph 3 CoC.

The production order is a flexible measure, less intrusive and onerous in comparison to other measures such as search and seizure of data. It could be applied only with regard to those persons that are custodians of data. The data must be already existent and not data that refer to future communication.

The implementation is extremely important not only for the law enforcement authorities, but also for the custodians of data (for example ISPs), who are often used to collaborating with the authorities by providing data and subscriber information under their control, but who prefer a legal basis for such assistance in order to avoid any contractual or non-contractual liability.[177]

Not all the countries analysed have already implemented this provision.[178] Some states have only general provisions that, although do not refer to the power of ordering the production of specified computer data, can be extended in their application covering fully or partially

---

171 Explanatory report, 168.

172 i.e. Albania, Armenia, Portugal and Mexico.

173 il.e. Albania, Armenia, Bulgaria (Article 159 Criminal Procedure Code); Estonia (Article 215 Criminal Procedure Code) or France (Article 60, paragraph 2, Code de Procedure Penal).

174 According to Article 60-2, para 2 Code de Procedure Penale: "L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs. Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais".

175 The text of Sec. 90 Slovak Criminal Procedure Code and Article 54 Romanian Law No. 161/203 can be read above.

176 Explanatory report, 170.

177 Explanatory report, 171.

178 See for example, Portugal, Ukraine, Cyprus or Mexico.

Article 18 CoC.[179] Only a few countries define the concept of "subscriber information".[180]

The country profile for France identifies Articles 60-1 and 99-3 Code de Procedure Penale as provisions corresponding with Article 18 CoC. They seem to cover Article 18 CoC, although they do not expressly refer to the power of ordering the production of specified computer data, using a different expression ("*document intéressant l'enquete*").[181]

Article 19 CoC provides for *search and seizure of stored computer data*. The aim of the provision is to extend the traditional investigative powers of search and seizure concerning tangible objects to computer systems and stored computer data as well, in order to allow evidence to be obtained, with respect to specific cyber criminal investigations.[182] In a lot of countries stored computer data are not considered tangible objects, with the consequence that the law enforcement can not work in a parallel manner in the new technological environment.

In order to facilitate the search and seizure of protected computer data, Article 19, paragraph 4, CoC has introduced a coercive measure giving the competent authorities the power to order any person who has particular knowledge about the functioning of the information system (i.e. system administrator) to give the necessary information to enable the undertaking of the measures referred to in paragraphs 1 and 2 Article 19 CoC.

The power to order the co-operation of knowledgeable persons could be a very important benefit for the investigating authorities, making searches and seizure more effective, speed and cost efficient.[183] It is advisable that all the countries implement this provision. Some countries have only general provisions concerning traditional search and seizure measures that could be insufficient in order to ensure that its authorities have the powers provided by Article 19 CoC.[184] For this reason it would be necessary to analyse the sentencing practice of national courts, but in this study it is not possible.

A model of full alignment with Article 19 CoC is represented by 56 Romanian Law No. 161/2003. It provides for:

> (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 Article 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

[179] Armenia (Article 225,239 Criminal Procedure Code); Albania (Article 191, 211 Criminal Procedure Code); France (Article 56, 97 Code de Procedure Penal); Germany (Sec. 95 StPO); Romania (Article 16 Law No. 508/2004) or Serbia (Article 82, 85 Criminal Procedure Code).

[180] See for example Italy (Article 4f), g), h), D.lgs. 196/2003); Romania (Article 35f) Law No. 161/2003); Bulgaria (Sec. 1(2) Penal Procedure Code); Cyprus (Article 2 Law No. 22(III)04).

[181] According to Article 60-1, paragraph 1 Code de Procedure Penale: "*Le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-3, la remise des documents ne peut intervenir qu'avec leur accord*".

[182] Explanatory report, 184.

[183] Explanatory report. 201.

[184] See for example Albania (Article 202, 203, 209 Criminal Procedure Code), Armenia (Article 226 Criminal Procedure Code), Croatia (Article 211B (2), 215 OG 58/02), Lithuania (Article 139, 141 Criminal Procedure Code); Estonia (Article 91, 126 Criminal Procedure Code); The Netherlands (Article 96b, 96c, 97, 110 Dutch CCP); Portugal (Article 176, 177, 178 Penal Procedure Code), United Kingdom (Article 10,14 CMA 1990; Article 16-19 ICA 2003).

or computer data storage medium searched for.

In the French Criminal Procedure Code, Articles 56 and 97, paragraph 3-4, are also consistent with Article 19 CoC, although the provisions empower the authority to search and seize different objects ("*papiers, documents, donnes informatiques ou autres objets*") compared with Article 19 CoC.[185]

Articles 20 and 21 CoC provide respectively for "real-time collection of traffic data" and "real-time interception of content data". According to both the provisions, the data must be associated with specified communications transmitted by a computer system. There are two types of data that can be collected: traffic data and content data.

The notion of "traffic data" is defined in Article 1 CoC. The term "content data" is not expressly defined but it can be interpreted as the content of communications.[186]

It is evident that the private interests associated to content data are greater than traffic data due to the nature of the communication content or message. For this reason Parties provide generally for more limitations regarding the real-time collection of content data.

Until presently, only a few countries expressly provide a measure consistent with Article 20 CoC in their domestic law.[187]

In some national legislation Article 20 CoC is not yet implemented or it is not completely covered.[188] Some countries have only general provisions concerning traditional collection of data that could be insufficient in order to ensure that its authorities have the powers provided by Article 20 CoC.[189] For this reason it would be necessary to analyse the sentencing practice of national courts, but in this study it is not possible.

A lot of states have already introduced a specific provision for the interception o**f** content data.[190] On the contrary, some countries empower their competent authorities to intercept only a restricted range of communications (i.e. telephone conversation).[191]

An example of full implementation of Article 21 CoC is represented by Section 90 of Criminal Procedure Code of Slovakia or Article 57 Romanian Law No. 161/2003.

Paragraph 1, Article 57 Romanian Law provides for: "the access to a computer system, as

---

185 According to Article 56, para. 1, Code de Procedure Penale: "*Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal*". According to Article 97 Code de Procedure Penale: "*Lorsqu'il y a lieu, en cours d'information, de rechercher des documents ou des données informatiques et sous réserve des nécessités de l'information et du respect, le cas échéant, de l'obligation stipulée par l'alinéa 3 de l'article précédent, le juge d'instruction ou l'officier de police judiciaire par lui commis a seul le droit d'en prendre connaissance avant de procéder à la saisie. (2) Tous les objets, documents ou données informatiques placés sous main de justice sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, l'officier de police judiciaire procède comme il est dit au quatrième alinéa de l'article 56. (3) Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition. (4) Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur ordre du juge d'instruction, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens*".

186 Explanatory report, 209.

187 Romania (Article 54 Law No. 161/2003), Slovakia (Sec. 90(1)a,b,e Criminal Procedure Act) and Germany (Sec. 100g StPO).

188 Serbia; Armenia; Albania, The Czech Republic (Sec. 88 Criminal Procedure Code), Sri Lanka or Mexico.

189 France (Article 60, para 2 Code de Procedure Penal).

190 See i.e. Albania (Article 221, 22 Criminal Procedure Code); Bulgaria (Article 172 Criminal Procedure Code), France (Article 100, 100-3. 100-6, 706-95 Code de Procedure Penal), Slovakia (Sec. 90 Criminal Code Act), or Germany (Sec. 100a, 100b StPO).

191 Armenia (Article 241 Criminal Procedure Code).

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".

Article 14, paragraph 3 CoC, provides that a Party may reserve the right to apply the provisions of Articles 20 and 21 CoC only to offences specified in the reservation. But the range of offences may not further restrict the range of offences to which it applies the measure of interception of content data.[192] Nevertheless, by just giving the power to apply these provisions to the competent authority, the success of such investigative operations concerning specific cyber crimes (hacking, cracking, distribution of malwares, etc.) could be guaranteed.

In order to permit an effective means for the investigation concerning the offences provided by the CoC, it would be advisable that all Parties apply these two important measures.

4.3 Jurisdiction over cybercrime offences

One of the biggest problems connected with cybercrime is jurisdiction.[193] For this reason, the CoC has established with Article 22 CoC some criteria in order to establish jurisdiction for the criminal offences enumerated from Article 2 to Article 11 CoC.

The first criteria provided by Article 22, paragraph 1 *a*) CoC, is based upon the traditional principle of territoriality. Each Party can punish the commission of the cybercrime offences that are committed in its territory. This criteria is already implemented in the procedural law of many states.[194] In order to determine the territorial jurisdiction, a Party could take into consideration the location of the person attacking a computer system, or the location of the victim.[195]

Paragraph 1, *b)* and *c)* Article 22 CoC provides for a variant of the general principle of territoriality, establishing criminal jurisdiction over cybercrimes committed on board ships flying the flag or aircraft registered under its laws.[196]

Paragraph 1, *d*) Article 22 CoC is based upon the principle of nationality. For this reason if a national commits a cybercrime abroad, the Party is obliged to prosecute him if his conduct also constitutes an offence in the country where he has committed the crime. That is the criteria most frequently applied by the Parties belonging to civil law tradition.

Parties could enter a reservation to the jurisdiction criteria provided for by paragraph 1 *b*), *c*) and *d*) Article 22 CoC. Nevertheless, no reservation is permitted with respect to paragraph a) Article 22 CoC or with respect to the obligation to determine jurisdiction with regard to those cases falling under the principle of "extradite or prosecute" (*aut dedere aut judicare*).[197]

The aim of Article 22, paragraph 3 CoC is to establish jurisdiction over the offences referred to in Article 24, paragraph 1 CoC, in those cases where Parties have refused to extradite an offender present in their territory, they have the legal ability to carry out investigations and proceedings domestically.

These criteria are not bonding for the Parties. In conformity with their domestic laws, they could apply other criteria.

---

[192] Explanatory report, 213.
[193] See Brenner S.W., Koops B-J. (ed.),*Cybercrime and jurisdiction*, cit.; Sieber U., *The International Handbook on Computer Crime,* cit., p. 110.
[194] See i.e. Armenia (Article 14 Criminal Code); Italy (Article 6 c.p.); Bulgaria (Articles 3, 6 Criminal Code); Germany (Sec. 3 StGB); Lithuania (Article 4 Criminal Procedure Code); Romania (Article 3 Criminal Code).
[195] Explanatory report, 233.
[196] Armenia (Article 14 Criminal Code); Germany (Sec. 4 StGB).
[197] Explanatory Report, 237.

In order to avoid useless duplication of efforts or competition among national law enforcement, it will be better if the Parties, in accordance with Article 22, paragraph 5 CoC, consult themselves in order to determine the proper venue for prosecution. In some cases the states could come to an agreement on a single venue for prosecution; in other cases, it could be better if one state prosecutes some participants while another state prosecutes others.[198]

4.4 Summarising tables of procedural law provisions

4.4.1 Expedited preservation of stored computer data

> Article 16 CoC
> 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.

Countries that have introduced a provision corresponding to Article 16 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Romania (Article 54 Law No. 161/2003)	Sri Lanka (Article 19(1), (2), Article 24(1,4) Computer Crime Act No. 24/2007)
Slovakia (Section 90(1) Code of Criminal Procedure Act)	
Austria ((Sec. 109, 134, para. 2, subpara 2 Criminal Procedure Code) (II)	
Bulgaria (Articles 125, 159, 162, 163 Criminal Procedure Code; Articles 55, 56, 148 Ministry of Interior Act)	

4.4.2 Expedited preservation and partial disclosure

> Article 17 CoC
> 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.

[198] Explanatory Report, 239.

Countries that have introduced a provision corresponding to Article 17 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Romania (Article 54 Law No. 161/2003)	USA (Title 18, Part I, Chapter 121, § 2702 US Code)
Slovakia (Section 90 (1)a,b,e Code of Criminal Procedure Act No. 301/2005)	
Germany (Section 100g Draft Law)	
Austria ((Sec. 109, 134, para 2, subpara 2 Criminal Procedure Code) (II)	

4.4.3 Production order

> Article 18 CoC
> 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.
> 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.

Countries that have introduced a provision corresponding to Article 18 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Germany (for Article 18(1) lit. a CoC see Section 95 stop; for Article 18(1) lit. b see Section 112, 113 TKG)	USA (Article 18 1(b), 2,3, Title 18, Part I, Chapter 211, § 2703 US Code)
Romania (Article 16 Law No. 508/2004)	
Slovakia (Section 90(1)a,b,e Code of Criminal Procedure Act n. 301/2005)	
The Netherlands (Article 125i Criminal Procedure Code)	
Estonia (Articles 112, 113 Electronic Communication Act)	
Austria (Sec. 111, para 2, 134, para 2, subpara 2, 138 Criminal Procedure Code)	
The Czech Republic (Sec. 47 Police Act No. 283/1991)(II)	
Turkey (Article 6 para. 1 subpar (b), Code number 5651/2007) (II)	

4.4.4 Search and seizure of stored computer data

Article 19 CoC
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.
The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Countries that have introduced a provision corresponding to Article 19 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Austria (Sections 109 seq; 119-122 Code of Criminal Procedure) (II)	Sri Lanka
Bulgaria (Articles 159, 160(1), 165(5) PPC)	
Germany (for Article 19(1) CoC see Sections 94,95,102, 103, 105, 161 163 stop; for Article 19(2) see Section 110(3))	
Romania (for Article 19 (1-2) CoC see Article 56(1)(3) Law n. 161/2003; for Article 19(3) see Articles 96, 99 Criminal Procedure Code)	
France	
Slovakia	
Turkey	

4.4.5 Real-time collection of data

Article 20 CoC
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:
stop 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.

Countries that have introduced a provision corresponding to Article 20 CoC:

European countries (full alignment)
Austria (Section 134, 137 Code of Criminal Procedure) (II)
Germany (Section 100g stop Draft law)
Romania (Article 54 Law No. 161/2003)
Slovakia (Section 90(1)a,b,e Code of Criminal Procedure Act No. 301/2005)
France

4.4.6 Interception of content data

Article 21 CoC
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:
stop 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.

Countries that have introduced a provision corresponding to Article 21 CoC:

European countries (full alignment)
Albania (Articles 221, 222, 223 Criminal Procedure Code)
Austria (Section 134, 137 Code of Criminal Procedure) (II)
Bulgaria (Article 172 PPC)
France (Article 706-95, para. 1; Article 100-100-3, Article 100-6 Code de Procedure Penale)
Germany (Sections 100a, 100b stop)
Portugal (Article 190 Penal Procedural Code)
Romania (Article 57 Law No. 161/2003)
Slovakia (Section 90 Code of Criminal Procedure Act No. 301/2005)
Turkey (Article 135 Criminal Procedure Code n. 5271/2005)
Estonia (Article 118 Criminal Procedure Code, Article 113 Electronic Act)
Italy
Estonia

4.4.7 Jurisdiction

Article 22 CoC
Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
a in its territory; or
b on board a ship flying the flag of that Party; or
c on board an aircraft registered under the laws of that Party; or
d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Countries that have introduced a provision corresponding to Article 22 CoC:

European countries	Non-European countries
Armenia (Article 14 Criminal Code)	Sri Lanka
Bulgaria (Articles 3-6 Criminal Code)	
Croatia (Articles 13,14,15 ,16 OG 105/04) (II)	
Germany (Section 3-9 StGB)	
Italy (general provisions from Penal Code)	
Lithuania (Articles 4, 5 Criminal Code)	
Portugal (Articles 5,6 Penal Code)(GP)	
Romania (Articles 3-4, Articles 142-143 Criminal Code)	
Slovakia (Section 3 Criminal Code Act No. 300/2005)	
Turkey (Article 8-13 Penal Code No. 5237/2005)	
United Kingdom (Articles 4-5, 7, 9, 13, 16 CMA 1990)	
Cyprus (Article 16 Law No. 22(III)04)	
Austria	
France (GP)	
Estonia	
Hungary (Article 3-5 Law No. 100/2003)(II)	
United Kingdom (GP)	

5 Comparative review of international co-operation provisions

5.1 Summary description of the provisions concerning international co-operation

Cybercrime has always had a transnational character.[199] For it to be fought, it is very important to secure the widest international co-operation among the national competent authorities. The aim of Article 23 CoC is to move the Parties to provide for the largest extension of co-operation to each other, eliminating all the impediments for the rapid flow of information and evidence.[200] Moreover, the aim of Article 23 CoC is to extend the co-operation to all cybercrime offences provided for by the CoC, implementing investigative and proceeding activities, collection of evidence in electronic form.

One example of co-operation among Parties is represented by extradition. Article 24 CoC contains principles that regulate extradition. Paragraph 1 Article 24 CoC establishes that the obligation to extradite can be applied only to those offences provided for by Articles 2-11 CoC that are punishable under the laws of both Parties, concerned by deprivation of liberty for a maximum period of at least one year or by a more severe penalty. Paragraph 1 *b)* Article 24 CoC provides that where a treaty on extradition or an arrangement on the basis of uniform or reciprocal legislation is in force between two or more Parties and it provides for a different threshold for extradition, this threshold shall apply.

In order to guarantee a great extension of the power for extradition, paragraph 2 CoC provides that the cybercrime offences established in accordance with Articles 2-11 CoC are to be considered extraditable offences in any extradition treaty between or among the Parties and are to be included in future treaties concluded between or among them.

Paragraph 6 Article 24 CoC refers to the principle "*aut dedere aut judicare*". If a Party has refused the request of extradition with regard to a national offender it must, upon the request of the requesting Party, submit the case to its authorities in order to value the possibility to prosecute him.

Some countries only cover general aspects of extradition without providing for the obligation to extradite for one of the offences established by Article 2 to Article 11 CoC, or the principle "*aut dedere aut judicare*".[201]

Other countries have only general provisions concerning extradition that could be insufficient in order to ensure that its authorities have the powers provided by Article 19 CoC.[202] For this reason it would be necessary to analyse the sentencing practice of national courts.

5.2 Summary description of the provisions concerning mutual assistance

Articles 25-28 CoC provide for general principles regulating the obligation to provide mutual assistance. Mutual assistance must be carried out in conformity with the applicable mutual legal assistance treaties, laws and arrangements.

In order to facilitate acceleration of the process to obtain a mutual legal assistance concerning, for example, the collection of evidence in electronic form of a criminal offence, a Party can make a request for co-operation using expedited means (communications, e-mail,

[199] Podgor E.S., *Cybercrime: national, transnational, or international?*, (50) 2004, Wayne L. Rev. 97.
[200] Explanatory report, 242.
[201] Albania (Article 11 Criminal Code); Turkey (Article 18 Turkish Penal Code).
[202] See for example Portugal.

fax, etc). The requested Party could answer through the same communications. Nevertheless, these communications should warrant appropriate levels of security and authentication. Until presently few countries have implemented this provision.[203]

Other countries have only general provisions concerning mutual assistance that is executed referring to the bilateral agreements or international conventions.[204]

An example of good practice is represented by Article 61 Romanian Law No. 161/2003.[205]

In order to secure and facilitate the co-operation among countries it is advisable that all the Parties implement Article 25 CoC.

In order to secure the effective co-operation among Parties, Article 26 CoC (*spontaneous information*) empowers the states that have valuable information that they believe may be useful for the investigation of another state to forward it to the other state, even if there is not a prior request. The aim of this provision is to facilitate the mutual assistance among those states that do not provide assistance in the absence of a prior request.

Until presently, few countries have implemented this provision generally through ratification of the relevant international instruments.[206]

Consistent with Article 26 CoC is Sec. 61a, 83j German Act on International Legal Assistance in Criminal Matters (IRG) or Article 66 Romanian Law No. 161/2003. It provides for that:

> The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.

If there are no mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, they must apply certain specific mutual assistance procedures in conformity with Article 27 CoC (*procedures pertaining to mutual assistance requests in the absence of applicable international agreements*). Paragraphs 2-10 Article 27 CoC provide for a number of rules for providing mutual assistance in the absence of a MLAT or specific arrangement.[207]

According to Article 28 CoC (*confidentiality and limitation on use*), the requested Party, in cases in which such information or material is sensitive, can satisfy the supply of information only if the use of information is limited to that for which assistance is granted or it is not disseminated beyond law enforcement officials of the requesting Party.

The aim of this provision is to provide specific safeguards for data protection.[208] Article 28 CoC could be applied only in the absence of specific LMTs between the requesting and requested Parties.

Articles 29, 30, 31, 32 CoC provide for specific mechanisms in order to guarantee effective and concerted international action with regard to cases involving cybercrime offences and

---

[203] See for example Bulgaria (Articles 471-477 Criminal Procedure Code).
[204] See i.e. Portugal; "the former Yugoslav Republic of Macedonia".
[205] Article 61 Romanian Law No. 161/2003: "(1) At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cybercrime. (2) The common investigations referred to at paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities. (3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation".
[206] See i.e. Germany (Sec. 61a, 83j IRG) or Romania (Article 66 Law No. 161/2003; Article 166 Law No. 302/2004).
[207] Explanatory report, 274.
[208] Explanatory report, 275.

evidence in electronic form.[209]

Article 29 CoC (*expedited preservation of stored computer data*) provides for a mechanism at the international level that authorises the requesting Party to make a request in order to obtain the expeditious preservation of data stored in the territory of the requested party by means of a computer system. It is the international equivalent of the practice established for domestic use in Article 16 CoC (see comment above).

The aim of this mechanism is to ensure that the data is not altered, removed or deleted during the time necessary to prepare a legal request of LMA for search, access, seizure or similar securing or disclosure of computer data.[210] The request for expeditious preservation of stored data must respect the contents established by paragraph 2.

The usefulness of this legal mechanism is due to its greater rapidity than ordinary mutual assistance instruments. At the same time, it is less intrusive because the requested Party must not obtain the possession of computer data but it must only ensure the preservation of the data during the pending process to ask for mutual legal assistance. The advantage of this mechanism is that it is rapid and more respectful of the privacy of the person whom the data concerns. Until presently, only a few Parties have implemented this practice. Some countries apply the international agreements.[211]

It is advisable that all of the Parties introduce this mechanism in order to guarantee that during the process of requesting, the data is not altered, removed, etc., with negative consequences for the success of the investigations.

A model of full alignment is represented by Article 63 Romanian Law No. 161/2003. It provides for that:

> (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 Article 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.

Article 30 CoC (*expedited disclosure of preserved traffic data*) is the international equivalent established for domestic use in Article 17 CoC (see comment above). A requested Party preserving traffic data regarding a transmission realised through a computer systems in order to identify the perpetrator of the offence or locate critical offence, can discover that the traffic data reveals that the transmission has been routed from an ISP in a third state or from an ISP in the requesting state itself. In these cases, the requested Parties must expeditiously provide to the requesting Party a sufficient amount of the traffic data in order to ensure the identification of the ISP.

In accordance with paragraph 2, the requested Party can refuse to disclose the traffic data only in two cases: the disclosure could prejudice its sovereignty, security, pubic order or other essential interest; when it considers the offence has a political nature or it is connected

[209] Explanatory report, 281.
[210] Explanatory report, 282.
[211] See i.e. Estonia; Portugal, Italy.

with a political offence.

Only Romania provides for a expedited disclosure of preserved traffic data measure completely consistent with Article 30 CoC. According to Article 64 Romanian Law No. 161/2003:

> If, in executing the request formulated according to Article 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.

Article 31 CoC (*mutual assistance regarding accessing of stored computer data*) authorises a Party to request another Party to search, similarly access, seize or similarly secure, and disclosure computer data stored located within its territory. The majority of the countries do not have specific provisions in force concerning LMA and apply, where existent, international agreements.[212] The question is to determine if the general rules are fully compliant with the specific requirements of the CoC. For this reason it would be better to encourage the full implementation of Article 31 CoC.

Article 32 CoC (*transborder access to stored computer data with consent or where publicly available*) allows computer data stored in another Party to be unilaterally accessed without the prior mutual assistance request, only if the data are publicly available or if the Party has accessed or received data located outside of its territory through a computer system in its territory. In this last case, the Party should have the lawful and voluntary consent of the person that has the authority to disclose the data to the party.[213] The majority of the countries do not have a specific provision in force and apply, where existent, international agreements.[214]

Completely consistent with Article 32 CoC is Article 65 Romanian Law No. 161/2003. The Romanian provision provides for that:

> (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.

Article 33 CoC (*mutual assistance regarding the real-time collection of traffic data*) requires the mutual co-operation between Parties in order to collect traffic data in real time for another Party. The real-time collection of traffic data is often the sole instrument that may allow the real identity of the perpetrator of a crime to be discovered. It is less intrusive compared to other practices (interception of content data). The majority of the countries do not have a specific provision in force and apply, where existent, international agreements.[215] It is advisable that all the countries take into consideration the opportunity to implement this provision.

Article 34 CoC (*mutual assistance regarding the interception of content data*) regulates the mutual assistance regarding the interception of content data. The obligation to provide mutual assistance with regard to interception of content data is restricted, due to the high level of intrusiveness of interception.[216] The majority of the countries do not have a specific

[212] See Estonia; Bulgaria (Article 172, 471(2)); Germany (Sec. 66 IRG); France (Article 695-10 Code de Procedure Penale); Slovakia (Article 537 Criminal Procedure Act).
[213] Explanatory Report, 294.
[214] See i.e. Estonia; France; Germany; Portugal; Slovakia; Italy.
[215] See i.e. Estonia; France; Germany; Romania; Portugal; Italy; Slovakia.
[216] Explanatory Report, 297.

provision in force and apply, where existent, international agreements.[217] An effort should be made in order to implement into domestic law this provision.

The scope of Article 35 CoC (*24/7 Network*) is to create a permanently contact point in each country, available 24 hours a day, 7 days a week, in order to guarantee immediate assistance in investigations and proceedings.[218] Each Party's point of contact must facilitate the providing of technical advice, the preservation of data, the collection of evidence, providing legal information and locating the suspects. For this reason, each Party must provide to its point of contact proper equipment (computer and analytical equipment, fax, etc.).[219] The CoC leaves the countries free to decide in which manner to actuate this provision and to decide where to locate the point of contact.[220]

Until presently, very few countries are listed in the 24/7 contact point list. That constitutes a limitation in order to ensure effective, immediate and permanent international co-operation in the fight against cybercrime within the other national and international organism and authorities. It would be advisable that all countries make an effort to implement this provision in order to permit effective fighting against computer crime and cybercrime.

5.3 Summarising tables

5.3.1 Extradition

Article 24 CoC
1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.
5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
b. The Secretary General of the Council of Europe shall set up and keep updated a

[217] See for example Croatia; Estonia; France; Germany and Slovakia.
[218] Explanatory Report, 298.
[219] Explanatory Report, 302.
[220] Explanatory Report, 300.

register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Countries that have introduced a provision corresponding to Article 24 CoC:

European countries (full alignment)	Non-European countries (full alignment)
Slovakia (Section 498-514 Criminal Procedural Act No. 301/2005) (II)	USA (Title 18, part II, Chapter 209 § 3181, 3184, 3188, 3192, 3193, 3195, 3196 US Code)
Croatia (Articles 32-61 OG 178/04) (II)	Sri Lanka (Articles 33, 34, 36 Computer Crime Act n. 24/2007)
France (Articles 696-1, 696-7 Code de Procedure Penal) (GP)	
"The former Yugoslav Republic of Macedonia" (Article 510, 510(5-7), 511, 521, 523-524 Macedonian Criminal Code)	
Germany (Section 2,3, Act on International Legal Assistance in Criminal Matters) (GP)	
Portugal (GP)	
Romania (Article 60 Law No. 161/2003; Title II Law No. 302/2004 amended by Law No. 224/2006)	
Cyprus	
Italy	
France (Articles 696-1; 696-7)	
Estonia	
Cyprus	

5.3.2 General principles relating to mutual assistance

Article 25 CoC
The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Countries that have introduced a provision corresponding to Article 25 CoC:

European countries (full alignment)
Bulgaria (Articles 471, 477 Section III Mutual Legal Assistance) (II)
France (Article 695-10 Code de Procedure Penal)
Germany (Sections 2 ff, 59 ff IRG)
Portugal (GP)
Romania (Article 61 Law No. 16172003)
Slovakia (Section 531-537 Code of Criminal Procedure Act No. 301/2005) (II)
Austria
Italy (GP)
Turkey (GP)
Estonia

5.3.3 Spontaneous information

Article 26 CoC
1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Countries that have already introduced a provision corresponding to Article 26 CoC:

European countries (full alignment)
Bulgaria (Articles 57(2), 55 (6)Article 471 (1), (4) PPC, Chapter 7 Law on Protection of the Classified Information)
Germany (Sections 61a, 83j IRG)
Romania (Article 66 Law No. 161/2003; Article 166 Law n. 302/2004)
Slovakia (Section 484 Code of Criminal Procedure act No. 301/2005)
France
Austria
Estonia

5.3.4 Procedures pertaining to mutual assistance request in the absence of applicable international agreements

Article 27 CoC

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
b. The central authorities shall communicate directly with each other;
c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Countries that have introduced a provision corresponding to Article 27 CoC:

European countries (full alignment)
Austria (Section 3 ARGH) (II)
Romania (Article 2(2)b Law No. 64/2004)

5.3.5 Confidentiality and limitation on use

Article 28 CoC
1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
b not used for investigations or proceedings other than those stated in the request.
3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information

should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Countries that have already introduced a provision corresponding to Article 28 CoC:

European countries (full alignment)	Non- European countries (full alignment)
Germany	Philippines (Article 17 Draft Law)
Romania (Article 12 Law No. 302/2004) (II)	
Slovakia	

5.3.6 Expedited preservation of stored computer data

Article 29 CoC
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.

Countries that have already introduced a provision corresponding to Article 29 CoC:

European countries (full alignment)
Austria (Section 58 ARHG, Section 143 seq, Section 115 revised Code of Criminal Procedure) (II)
Romania (Article 63 Law No. 161/2003)
Slovakia (section 551 Code of Criminal Procedure Act No. 301/2005) (II)
Germany

.

5.3.7 Expedited disclosure of preserved traffic data

Article 30 CoC
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.
The scope of the provision is to provide the effectiivty of the Article 29 and in particular with the request to preserve traffic data concerning specific communication.

Countries that have already introduced a provision corresponding to Article 30 CoC:

European countries (full alignment)
Austria (section 58 ARHG, Section 149a seq Code of Criminal Procedure) (II)
Romania (Article 63 Law No. 161/2003)
Slovakia (Section 551 Code of Criminal Procedure Act No. 301/2005) (II)
Germany

5.3.8 Mutual assistance regarding accessing of stored computer data

Article 31 CoC
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.

Countries that have introduced a provision corresponding to Article 31 CoC:

European countries (full alignment)
Austria (Section 58 ARHG, Section 149a seq Code of Criminal Procedure)
Romania (Article 60 Law No. 161/2003)

5.3.9 Transborder access to stored computer data with consent or where publicly available

Article 32 CoC
A Party may, without the authorization 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.

Countries that have already introduced a provision corresponding to Article 32 CoC:

European countries (full alignment)
Austria (II)
Romania (Article 65 Law No. 161/2003)

5.3.10 Mutual assistance in the collection of real-time traffic data

Article 33 CoC
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.

Countries that have already introduced a provision corresponding to Article 33 CoC:

European countries (full alignment)
Romania (Article 60 Law No. 161/2003)
Slovakia (Article 537 Criminal procedure Act No. 301/2005)
Austria (Section 58 ARHG; Section 149a seq Criminal Procedural Code)

5.3.11 Mutual assistance regarding the interception of content data

Article 34 CoC
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.

Countries that have already introduced a provision corresponding to Article 34 CoC:

European countries (full alignment)
Austria (Section 58 ARHG; Section 149a seq. Criminal Procedure Code) (II)
Romania (Article 60 Law n. 161/2003)

5.3.12 Network of 24/7 contact points

Article 35 CoC
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.

Countries that have already introduced a provision corresponding to Article 35 CoC:

European countries (full alignment)
Austria (AC)
Bulgaria (AC)
Germany (AC)
Italy
Lithuania
Romania (Article 62 Law No. 161/2003) (FC)

6 Conclusion

Nowadays the Cybercrime Convention represents undoubtedly the most important international treaty in the fight against cybercrime. At the time of writing, it has been ratified by a significant number of countries. The increasing number of countries that are moving towards accession demonstrates how the Cybercrime Convention is a fundamental guideline for the legislative harmonisation of national substantial criminal law and procedural criminal law against computer crime and cybercrime. Nevertheless, in order to effectively fight this transnational phenomenon further efforts must be made to encourage as many countries as possible to apply for accession and to prevent "computer crime havens".

The provisions provided for by the Cybercrime Convention are not always directly applicable into domestic law and require a specific adaptation by each Party, in conformity with the national criminal law system.[221] Nevertheless, in the process of implementation, each country has to respect the aim of each provision.

The majority of the countries that have ratified the Cybercrime Convention have implemented their substantial criminal law in compliance with the requirements of the CoC. Nevertheless, in some domestic laws dangerous gaps still exist.

With regard to the implementation of the substantial criminal law provisions, the problems concern in particular Articles 4 (data interference) and 5 (system interference), 6 (misuse of devices), 7 (computer-related forgery) and 8 (computer-related fraud) CoC.

Not all the countries analysed distinguish correctly between data interference and system interference. In the majority of the cases they criminalise both data and system interference with the same sanction, without taking into consideration the different impact of the illegal acts. It would be advisable therefore to provide for a separate criminalisation of the illegal acts concerning data and information systems. A model of good practice is represented by Cyprus or Romanian Law.

Article 6 CoC is a "*delicte obstacle*" (or basic offence) for the commission of more dangerous crimes to be prevented. At this point, very few countries have implemented this provision in

[221] About the contradiction between cybercrime and national criminal law systems see Sieber U., in Council of Europe, *The threat of cybercrime*, cit., p. 215.

compliance with the CoC requirements. The states that have not already implemented the provision could take as model of good practice Austrian, Croatian, Romanian or Sri Lankan law, requiring a more general penalisation of misuse of devices, in conformity with Article 6 CoC.

In order to also cover illegal acts committed through social engineering techniques, the opportunity to criminalise also the possession, sale, use and distribution of identity information obtained illegally could be taken into consideration, in order to adequately fight identity theft, which represents a basic offence for the commission of other dangerous crimes. To this end an example of good practice could be represented by US Code 18 § 1028 (a)7 that criminalises "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity".[222]

In a lot of countries (i.e. Albania, Bulgaria, France, The Netherlands or Slovakia) no specific provision exists with regard to cyber-forgery and cyber-fraud. The wide structure of the traditional penalisations of forgery and fraud allow the major part of the new illegal acts committed though the information technologies to be covered. Nevertheless, it would be advisable, for an effective harmonisation of the cybercrime legislation, that the countries make a further effort in order to align their law with the requirements established by the Cybercrime Convention. They could take Austrian or Romanian legislation as model of full implementation of substantial criminal law.

The biggest problems in the process of implementation concern the procedural law provisions. Only a full alignment with the Convention of Cybercrime could give law enforcement and investigation authorities the power to investigate, and prosecute computer-related crime more effectively. The majority of the countries, in particular non-European countries, have only general provisions that are not always able to guarantee the circulation of evidence and data in real time.

For this reason it would be advisable for each country to implement specific provisions, such as search and seizure of stored computer data, preservation of data and electronic evidence. Very often there are bureaucratic and political obstacles between the countries that obstruct the activities of law enforcement and investigative authorities. In this sense examples of good practices are the Slovakian and Romanian criminal procedure laws.

In addition, the global nature of computer crime and cybercrime requires that an effort is made in order to go beyond the traditional provisions regarding the territorial application of national procedural laws. One of the most important characteristics of cyberspace is the absence of borders and temporal and spatial limits. It makes the commission of cybercrimes easier and faster, as well as from a big distance from the place where the information system is violated. That determines an evident separation not only between the action and the outcome, but also between the perpetrators and victims of the crime, with great difficulties in order to determine the competence and the jurisdiction and rules for legal co-operation. For this reason, a wide ratification of the Cybercrime Convention would represent a fundamental step in order to solve these problems.

Nevertheless, much work remains to be done in order to guarantee the effectiveness of cybercrime legislation. In almost all the countries, the aversion of the victims to report cybercrime is still a challenge. Very often the victims do not know that there are legal remedies. Business and banks do not file complaints because they are afraid of the reputational damage and the loss of market capitalisation or consumer confidence.[223] For this

[222] See Seger A., *Identity theft and the Convention on Cybercrime*, UN ISPAC Conference on the Evolving Challenge of identity-related crime (Courmayer, Italy, 30/11-02/12- 2007).

[223] Yang D.W., Hoffstadt B.M., Essay, "Countering the Cyber-Crime Threat", in (43) 2006 *Am. Crim. L. Rev.*, p. 202; Kalinich K.P., McGrath K., "Identifying the Business Impact of Network Risks and Liabilities", in *ABA Brief*, Winter

reason they do not report incidents but prefer to solve them themselves.[224]

In order to reduce the "grey figure" that limits the effectiveness of cybercrime provisions, it would be advisable to introduce legal mechanisms that facilitate the possibility to file a complaint against cybercriminals.

Another problem concerns the weak deterrence value of the criminal sanctions, which emerges from the criminological studies. In order to guarantee information security and a peaceful development of the social, economic and juridical relationship in the information society, criminal intervention is not enough. For this reason is would be advisable that countries implement specific and extra-criminal measures in order to prevent the commission of computer crimes and cyber crimes.

By way of conclusion, it would be advisable to adopt comprehensive strategies that go beyond the use of criminal measures but introduce soft law measures, such as a common regulation of the public access to the web (Internet point, cyber café, libraries, universities, etc.), the adoption of the ethical codes for Internet users and specific measures to educate them to use new technologies in a responsible manner. It would also be very important to introduce new "positions of responsibility" for ISPs, system operators, bloggers, persons responsible for the automatic processing of personal data, etc., in view of a constructive development of social, economic and legal relations in cyberspace. The adoption of such "comprehensive strategies" would help avoid over-criminalisation and a dangerous competition between cyberthreats and the law.

2004, 21.

[224] See i.e. Mitchell S.D., Banker E.A., "Private Intrusion Response", (11) 1998 Harv. J. L. & Tech., p. 699.

7 Appendix

7.1 Cybercrime legislation in France, Germany and Romania – comparative tables

7.1.1 Convention on cybercrime – correponding provisions in national legislation

Article CoC	DESCRIPTION	Article FRANCE LAW	STATUS-COMMENT	Article GERMANY LAW	STATUS	Article ROMANIA LAW N. 161/2003	STATUS - COMMENT
1	*Definitions*	- **-**	NC	Sec. 202a(2)StGB	PC	Article 35	**FC**
2	*Illegal Access*	Article 323-1 Code Penal	C	Sec. 202(2)StGB	PC	Article 42	**FC**
3	*Illegal Interception*	Article 226-15, para. 2, Code Penal	PC	Sec.202b StGB	FC	Article 43	**FC**
4	*Data interference*	Article 323-1 Code Penal	RN	Sec.303a StGB	C	Article 44	**FC**
5	*System interference*	Article 323-1 code Penal	C	Sec.303b StGB	C	Article 45	**FC**
6	*Misuse of Devices*	Article 323-3-1 Code Penal	RN	Sec.202cStGB	PC-CR	Article 46	**FC**
7	*Computer-related Forgery*	Article 323-4 Code Penal	RN	Sec.263a StGB	PC	Article 48	**FC**
8	*Computer-related Fraud*	Article 323-3-1 Code Penal	RN	Sec.263a StGB	FC	Article 49	**FC**
9	*Child Pornography*	Article 227-23; Article 227-24 Code Penal	C	Sec.184b StGB	CR	Article 51(1)	**FC**
10	*Copyright Infringements*	Article L 112-1; Article 112-2; Article L. 111-1; Article R 111-1 Code de la Proprietè Intellectuelle	RN	Sec. 176,177,178 URHG	C	Articles 139 – 139 and Article 143 of Law on copyright No. 8/1996	**C**
11	*Attempt; aiding or Abetting*	Article 11 (2)-Article 323-7 Code Penal	C	Sec.22-27StGB	C	Articles 50 and 51(2)	**C**
12	*Corporate liability*	Article 323-6 Code Penal	**FC**	Sec.30,130 OWIG	FC	Article 19 of Criminal Code (amended by Law No. 278/2006)	**C**
13	*Sanctions and Measures*	Article 323-6 Code Penal	**C**	Sec. 202a, 202b, 202c,	C	Articles 42-46, Articles 48-49 and	**C**

				263a, 269, 303a StGB, Sec. 106 URGH, Sec.30,130 OWIG		Article 51 Article 53 of Criminal Code (amended by Law No. 278/2006)	
14	*Scope of Procedural Prov.*	*Article 56,57, 94, 97 Code de Procedure Penale*	**C**		C	Article 58	**C**
15	*Conditions and Safeguards*	*Article 57 du Code de Procédure Pénale et Article 96, paragraphe 3du Code de Procédure Pénale. Article 97, paragraphe 1, alinéa 2 du Code de Procédure Pénale.*	**C**		C	Articles 26 (1), 27 (3), 28 of Romania Constitution , Article 91 Criminal procedure Code, Article 57 (1), (2) of Romania Law No. 161/2003, Article 3 (3), (5) of Romania Law No. 365/2002 on electronic commerce (amended by Law No. 121/2006)	**C**
16	*Expedited Preservation*	*Article 56, paragraphe 7 du Code de Procédure Pénale*	**C**	Sec. 94, 95, 98 StPO Sec. 100g, 100h StPO	C	Article 54	**C**
17	*Partial Disclosure*	*Article 60-2 du Code de Procédure Pénale,*	**C**	Sec. 100g, 100h StPO	C	Article 54	**C**
18	*Production Order*	*Article 56 paragraphe 11 du Code de Procédure Pénale et Article 60-1/60-2 du Code de Procédure Pénale. Article 99-3 du Code de Procédure Pénale*	**C**	Sec. 95 StPO. Sec. 112, 113 TKG.	C	Article 16 of Law No. 508/2004 on establishing , organising and operating of the Directorate for	**C**

						Investigation of the Organised Crime and Terrorism Offences	
19	*Search and Seizure*	*Article 56 du Code de Procédure Pénale et Article 97, paragraphs 3-4.*	**C**	Sec. 94, 95, 102, 103, 105, 119(3) 161, 163 StPO.	C	Articles 96 and 99 of Criminal procedure Code. For Article 19 (1-2) of Convention on Cybercrime - Article56 (1) (3) of Romania Law No. 161/2003.	**C**
20	*Collection Traffic Data*	*Article 60-2 du Code de Procédure Pénale*	**C**	Sec. 100g StPO	C	Article 54	**C**
21	*Interception Content Data*	*Article 706-95, paragraphe 1 du Code de Procédure Pénale. Egalement Article 100- 100-3 et Article 100-6 du Code de Procédure Pénale.*	**C**	Sec. 100a, 100b StPO.	C	Article 57	**C**
22	*Jurisdiction*		**C**	Sec. 3-9 StGB	C	Articles 3-4 and Articles 142-143 Criminal Code	**C**
23	*General Principle*	- -		- -		- -	
24	*Extradition*	*Article 696-1- 696-7 du Code de Procédure Pénale.*	**C**	Sec. 2, 3 IRG	C	Article 60 of Romania Law No. 161/2003 and Title II of Law No. 302/2004 on international judicial co-operation in criminal matters as amended and	**C**

						supplemented by Law No. 224/2006	
25	*Mutual Assistance*	*Article 695-10 du Code de Procédure Pénale*	**C**	Sec. 2 ff., 59 ff. IRG	C	Article 61	**C**
26	*Spontaneus Information*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 61a, 83j IRG	C	Article 66 Article 166 of Law No. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006	**C**
27	*Absence Int. Agreements*	*Article 694- 694-4 du Code de Procédure Pénale. Egalement Article 694-9 du Code de Procédure Pénale*	C	Sec. 59 ff. IRG	C		**C**
28	*Confidentiality*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 59 ff. IRG	C	Article 12 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006	**C**
29	*Exp. Preservation*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 66 ff. IRG	C	Article63	**C**
30	*Partial Disclosure*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 59 ff. IRG	C	Article64	**C**
31	*Accessing Store Data*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 66 IRG	C	Article 60	**C**
32	*Trans-border Access*	*Article 695-10 du Code de*	C	Sec. 94 StPO	C	Article65	**C**

		Procédure Pénale					
33	*Collection Traffic Data*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 59 ff. IRG	C	Article 60	**C**
34	*Interception Content Data*	*Article 695-10 du Code de Procédure Pénale*	C	Sec. 59 ff. IRG	C	Article 60	**C**
35	*24/7 Network*		C	Member of the 24/7 Network of the "G8 High-Tech Crime Subgroup" and of the ICPO Interpol	C	Article 62	**C**

7.1.2 France – criminal provisions concerning new cyber threats

Relevant incidents	Applicable provision	Status-comment	Sanction
Malicious code	Article 323-3 Code Penale	C	CRIM
Denial of service	Article 323-2, 323-3 Code Penale	CR	CRIM
Spam	Article 34, 35 della l. n. 575/2004 « *pour la confiance dans l'économie numérique* »	C	CRIM
Phishing	Article 226-18 Code Penale	PC	
Identity theft	Article 434-23 Code Penale	CP-CR	
Hacking	Article 323-1 Code Penale	C	CRIM
Cracking	Article 323-1 Code Penale	CR	CRIM
Data theft		NC	

7.1.3 Romania – criminal provisions concerning new cyber threats

Relevant incidents	Applicable provision	Status-comment	Sanction
Malicious code	Article 44 L. 161/2003	C	CRIM
Denial of service	Article 44, para. 1 L. 161/2003	C	CRIM
Spam (e-bombing)	Article 45 l. 161/2003	PC	CRIM
Phishing	Article 49 L. 161/2003	C	CRIM
Identity theft	- -	NC	
Hacking	Article 42 L. 161/2003	C	CRIM
Cracking	Article 42 L. 161/2003	C	CRIM
Data theft	Article 44, para. 2,3 L. 161/2003	PC	CRIM

7.1.4 Germany – criminal provisions concerning new cyber threats

RELEVANTS INCIDENTS	APPLICABLE PROVISION	STATUS-COMMENT	SANCTION
Malicious code	Sec. 303a; 303b StGB;	C	CRIM
Denial of service	Sec. 303a, 303b StGB	C	CRIM
Spam (E-bombing)	Sec. 265a, 303b, 317 StGB	PC- CR	CRIM
Phishing	Sec. 202a, 269 StGB	C	CRIM
Identity theft	- -	NC	
Hacking	Sec. 202a StGB	PC- CR	CRIM
Cracking	Sec. 202a StGB	C-CR	CRIM
Data theft	- **-**	NC	

7.2 Country profile on cybercrime legislation – France

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Project on Cybercrime
www.coe.int/cybercrime

Revised draft (26 Feb 2008)

Cybercrime legislation – country profile

France

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

Comments may be sent to:

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

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

Country:	**FRANCE**
Signature of Convention:	Yes: 23.11.2001
Ratification/accession: ***Provisions of the Convention***	Yes: 10.01.2006 ***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	ART. 323-1 du Code Pénal
Article 3 – Illegal interception	ART. 226-15, paragraphe 2 du Code Pénal
Article 4 – Data interference	ART. 323-1 du Code Pénal
Article 5 – System interference	ART. 323-1 du Code Pénal
Article 6 – Misuse of devices	ART. 323-3-1 du Code Pénal
Article 7 – Computer-related forgery	ART. 323-4 du Code Pénal
Article 8 – Computer-	ART. 323-3-1 du Code Pénal

related fraud	
Article 9 – Offences related to child pornography	ART. 227-23 et ART. 227-24 du Code Pénal Il est à noter que les articles 706-81- 706-87 du Code de Procédure Pénale, de même que la loi n°2007-297 du 5 mars 2007 peuvent être consultés à titre informatif. Ces dispositifs législatifs sont largement utilisés lors de l'investigation des crimes commis sous l'Art. 227-23 et l'Art. 227-24 du Code Pénal français.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	ART. L112-1, ART. L 112-2 du Code de la Propriété Intellectuelle
Article 11 – Attempt and aiding or abetting	ART. 11 (2)- Art. 323-7 du Code Pénal
Article 12 – Corporate liability	ART. 323-6 du Code Pénal
Article 13 – Sanctions and measures	ART. 323-6 du Code Pénal
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	Pour ART. 14 (1-2)- ART. 56 du Code de Procédure Pénale et ART. 57-1 du Code de Procédure Pénale et ART. 94 du Code de Procédure Pénale. Pour ART. 14 (1-2)- ART. 97 du Code de Procédure Pénale.
Article 15 – Conditions and safeguards	ART. 57 du Code de Procédure Pénale et ART. 96, paragraphe 3du Code de Procédure Pénale. ART. 97, paragraphe 1, alinéa 2 du Code de Procédure Pénale.
Article 16 – Expedited preservation of stored computer data	Pour ART. 16 (1)- ART. 56, paragraphe 7 du Code de Procédure Pénale
Article 17 – Expedited preservation and partial disclosure of traffic data	ART. 60-2 du Code de Procédure Pénale, voir paragraphe 2.
Article 18 – Production order	Pour ART. 18 -1 (a)- ART. 56 paragraphe 11 du Code de Procédure Pénale et ART. 60-1/60-2 du Code de Procédure Pénale. Egalement pour ART. 18-1- ART. 99-3 du Code de Procédure Pénale.
Article 19 – Search and seizure of stored computer data	ART. 56 du Code de Procédure Pénale et ART. 97, paragraphes 3-4.
Article 20 – Real-time collection of traffic data	Pour ART. 20-1 – ART. 60-2 du Code de Procédure Pénale
Article 21 – Interception of content data	ART. 706-95, paragraphe 1 du Code de Procédure Pénale. Egalement ART. 100- 100-3 et ART. 100-6 du Code de Procédure Pénale.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	

Chapter III – International co-operation	
Article 24 – Extradition	ART. 696-1- 696-7 du Code de Procédure Pénale.
Article 25 – General principles relating to mutual assistance	ART. 695-10 du Code de Procédure Pénale
Article 26 – Spontaneous information	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	ART. 694- 694-4 du Code de Procédure Pénale. Egalement ART. 694-9 du Code de Procédure Pénale.
Article 28 – Confidentiality and limitation on use	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 29 – Expedited preservation of stored computer data	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 30 – Expedited disclosure of preserved traffic data	ART. 695-10 du Code de Procédure Pénale (voir annexe 2, surtout paragraphe 1er)
Article 31 – Mutual assistance regarding accessing of stored computer data	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 32 – Trans-border access to stored computer data with consent or where publicly available	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 33 – Mutual assistance in the real-time collection of traffic data	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 34 – Mutual assistance regarding the interception of content data	ART. 695-10 du Code de Procédure Pénale (voir annexe 2)
Article 35 – 24/7 Network	
Article 42 – Reservations	**Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 21 of the Convention, France shall apply the provisions contained in Article 21 only if the prosecuted offence is punished with a deprivation of liberty superior or equal to two years of custody. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 21 **Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 27 of the Convention, France declares that, even in cases of urgency :

	- requests for mutual assistance from the French judiciary authorities and directed to foreign judiciary authorities are transmitted through the Ministry of Justice (*Ministère de la Justice, 13, Place Vendôme, 75042 Paris Cedex 01*); - requests for mutual assistance from foreign judiciary authorities and directed to the French judiciary authorities are transmitted through diplomatic channel (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*). **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 27 **Reservation contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 9, paragraph 2.b, of the Convention, France shall apply Article 9, paragraph 1, to any pornographic material that visually depicts a person appearing to be a minor engaged in sexually explicit conduct, in so far as it is not proved that the said person was 18 years old on the day of the fixing or the registering of his or her image. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 9 **Reservation contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 22 of the Convention, France reserves itself the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State. France declares also that, whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the public prosecutor and must be preceded by a complaint from the victim or his/her beneficiaries or by an official complaint from the authorities of the State where the act was committed (Article 22, paragraph1.d). **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 22 **Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 24 of the Convention, France declares that : - the Ministry for Foreign Affairs is the authority responsible for making or receiving requests for extradition in the absence of a treaty (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*); - the territorially competent State Prosecutor shall be the authority responsible for making or receiving requests for provisional arrest in the absence of a treaty. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 24 **Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 35 of the Convention, France designates as point of contact the "*Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication" (11, Rue des Saussaies, 75800 Paris)*. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 35

Annexe 1. **Solutions porposées dans la législation nationale.**

Code Pénal.

CODE PENAL
(Partie Législative)

Paragraphe 2 : De l'atteinte au secret des correspondances

Article 226-15

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

CODE PENAL
(Partie Législative)

Section 5 : De la mise en péril des mineurs

Article 227-23

(Loi nº 98-468 du 17 juin 1998 art. 17 Journal Officiel du 18 juin 1998)

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2002-305 du 4 mars 2002 art. 14 Journal Officiel du 5 mars 2002)

(Loi nº 2004-204 du 9 mars 2004 art. 6 VIII Journal Officiel du 10 mars 2004)

(Loi nº 2004-575 du 21 juin 2004 art. 44 Journal Officiel du 22 juin 2004)

(Loi nº 2006-399 du 4 avril 2006 art. 16 IV Journal Officiel du 5 avril 2006)

(Loi nº 2007-293 du 5 mars 2007 art. 29 Journal Officiel du 6 mars 2007)

(Loi nº 2007-297 du 5 mars 2007 art. 35 V 2º Journal Officiel du 7 mars 2007)

Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.

Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à 100 000 Euros d'amende

lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.

La tentative des délits prévus aux alinéas précédents est punie des mêmes peines.
Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 Euros d'amende lorsqu'elles sont commises en bande organisée.

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image.

Article 227-24

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2007-297 du 5 mars 2007 art. 35 V 3º Journal Officiel du 7 mars 2007)

Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

CODE PENAL
(Partie Législative)

CHAPITRE III : Des atteintes aux systèmes de traitement automatisé de données

Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-3

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 III Journal Officiel du 22 juin 2004)

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1

(inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004)

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

(Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-6

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :
1º L'amende, suivant les modalités prévues par l'article 131-38 ;
2º Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

(Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Code de la Propriété Intellectuelle.

CODE DE LA PROPRIETE INTELLECTUELLE
(Partie Législative)

Chapitre Ier : Nature du droit d'auteur

Article L111-1

(Loi nº 2006-961 du 1 août 2006 art. 31 Journal Officiel du 3 août 2006)

L'auteur d'une oeuvre de l'esprit jouit sur cette oeuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous.

Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial, qui sont déterminés par les livres Ier et III du présent code.

L'existence ou la conclusion d'un contrat de louage d'ouvrage ou de service par l'auteur d'une oeuvre de l'esprit n'emporte pas dérogation à la jouissance du droit reconnu par le premier alinéa, sous réserve des exceptions prévues par le présent code. Sous les mêmes réserves, il n'est pas non plus dérogé à la jouissance de ce même droit lorsque l'auteur de l'oeuvre de l'esprit est un agent de l'Etat, d'une collectivité territoriale, d'un établissement public à caractère administratif, d'une autorité administrative indépendante dotée de la personnalité morale ou de la Banque de France.

Les dispositions des articles L. 121-7-1 et L. 131-3-1 à L. 131-3-3 ne s'appliquent pas aux agents auteurs d'oeuvres dont la divulgation n'est soumise, en vertu de leur statut ou des règles qui régissent leurs fonctions, à aucun contrôle préalable de l'autorité hiérarchique.

CODE DE LA PROPRIETE INTELLECTUELLE
(Partie Législative)

Chapitre II : Oeuvres protégées

Article L112-1

Les dispositions du présent code protègent les droits des auteurs sur toutes les oeuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination.

Article L112-2

(Loi nº 94-361 du 10 mai 1994 art. 1 Journal Officiel du 11 mai 1994)

Sont considérés notamment comme oeuvres de l'esprit au sens du présent code :

1º Les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;

2º Les conférences, allocutions, sermons, plaidoiries et autres oeuvres de même nature ;

3º Les oeuvres dramatiques ou dramatico-musicales ;

4º Les oeuvres chorégraphiques, les numéros et tours de cirque, les pantomimes, dont la mise en oeuvre est fixée par écrit ou autrement ;

5º Les compositions musicales avec ou sans paroles ;

6º Les oeuvres cinématographiques et autres oeuvres consistant dans des séquences animées d'images, sonorisées ou non, dénommées ensemble oeuvres audiovisuelles ;

7º Les oeuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;

8º Les oeuvres graphiques et typographiques ;

9º Les oeuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;

10º Les oeuvres des arts appliqués ;

11º Les illustrations, les cartes géographiques ;

12º Les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;

13º Les logiciels, y compris le matériel de conception préparatoire ;

14º Les créations des industries saisonnières de l'habillement et de la parure. Sont réputées industries saisonnières de l'habillement et de la parure les industries qui, en raison des exigences de la mode, renouvellent fréquemment la forme de leurs produits, et notamment la couture, la fourrure, la lingerie, la broderie, la mode, la chaussure, la ganterie, la maroquinerie, la fabrique de tissus de haute nouveauté ou spéciaux à la haute couture, les

productions des paruriers et des bottiers et les fabriques de tissus d'ameublement.

CODE DE LA PROPRIETE INTELLECTUELLE
(Partie Réglementaire)

Chapitre Ier : Nature du droit d'auteur

Article R111-1

(inséré par Décret nº 95-385 du 10 avril 1995 annexe Journal Officiel du 13 avril 1995)

Les redevances visées à l'article L. 111-4 (alinéa 3) du code de la propriété intellectuelle sont versées à celui des organismes suivants qui est compétent à raison de sa vocation statutaire, de la nature de l'oeuvre et du mode d'exploitation envisagé :
Centre national des lettres ;
Société des gens de lettres ;
Société des auteurs et compositeurs dramatiques ;
Société des auteurs, compositeurs et éditeurs de musique ;
Société pour l'administration du droit de reproduction mécanique des auteurs, compositeurs et éditeurs ;
Société des auteurs des arts visuels.
Au cas où l'organisme compétent n'accepte pas de recueillir lesdites redevances ou à défaut d'organisme compétent, ces redevances seront versées à la Caisse des dépôts et consignations.

Code de Procédure Pénale.

CODE DE PROCEDURE PENALE
(Partie Législative)

Chapitre Ier : Des crimes et des délits flagrants

Article 56

(Ordonnance nº 60-529 du 4 juin 1960 art. 2 Journal Officiel du 8 juin 1960)

(Loi nº 99-515 du 23 juin 1999 art. 22 Journal Officiel du 24 juin 1999)

(Loi nº 2001-1168 du 11 décembre 2001 art. 18 Journal Officiel du 12 décembre 2001)

(Loi nº 2004-204 du 9 mars 2004 art. 79 I Journal Officiel du 10 mars 2004)

(Loi nº 2004-575 du 21 juin 2004 art. 41 Journal Officiel du 22 juin 2004)

Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal.

Il a seul, avec les personnes désignées à l'article 57 et celles auxquelles il a éventuellement recours en application de l'article 60, le droit de prendre connaissance des papiers, documents ou données informatiques avant de procéder à leur saisie.

Toutefois, il a l'obligation de provoquer préalablement toutes mesures utiles pour que soit

assuré le respect du secret professionnel et des droits de la défense.

Tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues à l'article 57.

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

Si une copie est réalisée, il peut être procédé, sur instruction du procureur de la République, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Avec l'accord du procureur de la République, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité.

Le procureur de la République peut également, lorsque la saisie porte sur des espèces, lingots, effets ou valeurs dont la conservation en nature n'est pas nécessaire à la manifestation de la vérité ou à la sauvegarde des droits des personnes intéressées, autoriser leur dépôt à la Caisse des dépôts et consignations ou à la Banque de France.

Lorsque la saisie porte sur des billets de banque ou pièces de monnaie libellés en euros contrefaits, l'officier de police judiciaire doit transmettre, pour analyse et identification, au moins un exemplaire de chaque type de billets ou pièces suspectés faux au centre d'analyse national habilité à cette fin. Le centre d'analyse national peut procéder à l'ouverture des scellés. Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés entre les mains du greffier de la juridiction compétente. Ce dépôt est constaté par procès-verbal.

Les dispositions du précédent alinéa ne sont pas applicables lorsqu'il n'existe qu'un seul exemplaire d'un type de billets ou de pièces suspectés faux, tant que celui-ci est nécessaire à la manifestation de la vérité.

Si elles sont susceptibles de fournir des renseignements sur les objets, documents et données informatiques saisis, les personnes présentes lors de la perquisition peuvent être retenues sur place par l'officier de police judiciaire le temps strictement nécessaire à l'accomplissement de ces opérations.

Article 57

(Ordonnance nº 58-1296 du 23 décembre 1958 art. 1 Journal Officiel du 24 décembre 1958 en vigueur le 2 mars 1959)

(Ordonnance nº 60-529 du 4 juin 1960 art. 1 Journal Officiel du 8 juin 1960)

Sous réserve de ce qui est dit à l'article précédent concernant le respect du secret professionnel et des droits de la défense, les opérations prescrites par ledit article sont faites en présence de la personne au domicile de laquelle la perquisition a lieu.

En cas d'impossibilité, l'officier de police judiciaire aura l'obligation de l'inviter à désigner un représentant de son choix ; à défaut, l'officier de police judiciaire choisira deux témoins requis à cet effet par lui, en dehors des personnes relevant de son autorité administrative.

Le procès-verbal de ces opérations, dressé ainsi qu'il est dit à l'article 66, est signé par les personnes visées au présent article ; au cas de refus, il en est fait mention au procès-verbal.

Article 60

(Loi nº 72-1226 du 29 décembre 1972 art. 9 Journal Officiel du 30 décembre 1972)

(Loi nº 85-1407 du 30 décembre 1985 art. 11 et 94 Journal Officiel du 31 décembre 1985 en vigueur le 1er février 1986)

(Loi nº 99-515 du 23 juin 1999 art. 12 Journal Officiel du 24 juin 1999)

S'il y a lieu de procéder à des constatations ou à des examens techniques ou scientifiques, l'officier de police judiciaire a recours à toutes personnes qualifiées.

Sauf si elles sont inscrites sur une des listes prévues à l'article 157, les personnes ainsi appelées prêtent, par écrit, serment d'apporter leur concours à la justice en leur honneur et en leur conscience.

Les personnes désignées pour procéder aux examens techniques ou scientifiques peuvent procéder à l'ouverture des scellés. Elles en dressent inventaire et en font mention dans un rapport établi conformément aux dispositions des articles 163 et 166. Elles peuvent communiquer oralement leurs conclusions aux enquêteurs en cas d'urgence.

Sur instructions du procureur de la République, l'officier de police judiciaire donne connaissance des résultats des examens techniques et scientifiques aux personnes à l'encontre desquelles il existe des indices faisant présumer qu'elles ont commis ou tenté de commettre une infraction, ainsi qu'aux victimes.

Article 60-1

(Loi nº 2003-239 du 18 mars 2003 art. 18 1º Journal Officiel du 19 mars 2003)

(Loi nº 2004-204 du 9 mars 2004 art. 80 I Journal Officiel du 10 mars 2004)

(Loi nº 2004-204 du 9 mars 2004 art. 80 II Journal Officiel du 10 mars 2004)

(Loi nº 2007-297 du 5 mars 2007 art. 69 1º Journal Officiel du 7 mars 2007)

Le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-3, la remise des documents ne peut intervenir qu'avec leur accord.

A l'exception des personnes mentionnées aux articles 56-1 à 56-3, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 Euros. Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, du délit prévu par le présent alinéa.

Article 60-2

(Loi nº 2004-204 du 9 mars 2004 art. 80 I Journal Officiel du 10 mars 2004)

(Loi nº 2004-575 du 21 juin 2004 art. 56 Journal Officiel du 22 juin 2004 en vigueur le 1er août 2004)

(Loi nº 2004-801 du 6 août 2004 art. 18 II Journal Officiel du 7 août 2004)

Sur demande de l'officier de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa du 3º du II de l'article 8 et au 2º de l'article 67 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 Euros. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du code pénal.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises.

CODE DE PROCEDURE PENALE
(Partie Législative)

Sous-section I : Des transports, des perquisitions et des saisies

Article 94

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

(Loi nº 2004-575 du 21 juin 2004 art. 42 Journal Officiel du 22 juin 2004)

Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité.

Article 96

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

(Loi nº 93-2 du 4 janvier 1993 art. 163 Journal Officiel du 5 janvier 1993 en vigueur le 1er mars 1993)

(Loi nº 2000-516 du 15 juin 2000 art. 44 Journal Officiel du 16 juin 2000)

(Loi nº 2004-204 du 9 mars 2004 art. 79 III Journal Officiel du 10 mars 2004)

Si la perquisition a lieu dans un domicile autre que celui de la personne mise en examen, la personne chez laquelle elle doit s'effectuer est invitée à y assister. Si cette personne est absente ou refuse d'y assister, la perquisition a lieu en présence de deux de ses parents ou alliés présents sur les lieux, ou à défaut, en présence de deux témoins.

Le juge d'instruction doit se conformer aux dispositions des articles 57 (alinéa 2) et 59.
Toutefois, il a l'obligation de provoquer préalablement toutes mesures utiles pour que soit assuré le respect du secret professionnel et des droits de la défense.

Les dispositions des articles 56, 56-1, 56-2 et 56-3 sont applicables aux perquisitions effectuées par le juge d'instruction.

Article 97

(ordonnance nº 58-1296 du 23 décembre 1958 art. 1 Journal Officiel du 24 décembre 1958)

(ordonnance nº 60-121 du 13 février 1960 art. 13 Journal Officiel du 14 février 1960)

(ordonnance nº 60-529 du 4 juin 1960 art. 2 Journal Officiel du 8 juin 1960)

(loi nº 85-1407 du 30 décembre 1985 art. 3 et art. 4 Journal Officiel du 31 décembre 1985 en vigueur le 1er février 1986)

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

(Loi nº 93-2 du 4 janvier 1993 art. 164 et 224 Journal Officiel du 5 janvier 1993 en vigueur le 1er mars 1993)

(Loi nº 2001-1168 du 11 décembre 2001 art. 18 Journal Officiel du 12 décembre 2001)

(Loi nº 2004-575 du 21 juin 2004 art. 43 Journal Officiel du 22 juin 2004)

Lorsqu'il y a lieu, en cours d'information, de rechercher des documents ou des données informatiques et sous réserve des nécessités de l'information et du respect, le cas échéant, de l'obligation stipulée par l'alinéa 3 de l'article précédent, le juge d'instruction ou l'officier de police judiciaire par lui commis a seul le droit d'en prendre connaissance avant de procéder à la saisie.
Tous les objets, documents ou données informatiques placés sous main de justice sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, l'officier de police judiciaire procède comme il est dit au quatrième alinéa de l'article 56.
Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur ordre du juge d'instruction, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Avec l'accord du juge d'instruction, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité.
Lorsque ces scellés sont fermés, ils ne peuvent être ouverts et les documents dépouillés qu'en présence de la personne, assistée de son avocat, ou eux dûment appelés. Le tiers chez lequel la saisie a été faite est également invité à assister à cette opération.

Si les nécessités de l'instruction ne s'y opposent pas, copie ou photocopie des documents ou des données informatiques placés sous main de justice peuvent être délivrées à leurs frais, dans le plus bref délai, aux intéressés qui en font la demande.

Si la saisie porte sur des espèces, lingots, effets ou valeurs dont la conservation en nature n'est pas nécessaire à la manifestation de la vérité ou à la sauvegarde des droits des parties, il peut autoriser le greffier à en faire le dépôt à la Caisse des dépôts et consignations ou à la Banque de France.

Lorsque la saisie porte sur des billets de banque ou pièces de monnaie libellés en euros contrefaits, le juge d'instruction ou l'officier de police judiciaire par lui commis doit transmettre, pour analyse et identification, au moins un exemplaire de chaque type de billets ou pièces suspectés faux au centre d'analyse national habilité à cette fin. Le centre d'analyse national peut procéder à l'ouverture des scellés. Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés entre les mains du greffier de la juridiction compétente. Ce dépôt est constaté par procès-verbal.

Les dispositions du précédent alinéa ne sont pas applicables lorsqu'il n'existe qu'un seul exemplaire d'un type de billets ou de pièces suspectés faux, tant que celui-ci est nécessaire à la manifestation de la vérité.

Article 99-3

(Loi nº 2004-204 du 9 mars 2004 art. 116 I Journal Officiel du 10 mars 2004)

(Loi nº 2007-297 du 5 mars 2007 art. 69 3º Journal Officiel du 7 mars 2007)

Le juge d'instruction ou l'officier de police judiciaire par lui commis peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'instruction, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-3, la remise des documents ne peut intervenir qu'avec leur accord.

En l'absence de réponse de la personne aux réquisitions, les dispositions du deuxième alinéa de l'article 60-1 sont applicables.

CODE DE PROCEDURE PENALE
(Partie Législative)

Sous-section II : Des interceptions de correspondances émises par la voie des télécommunications

Article 100

(Loi nº 85-1407 du 30 décembre 1985 art. 9 et art. 94 Journal Officiel du 31 décembre 1985 en vigueur le 1er février 1986)

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.
La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

Article 100-1

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci.

Article 100-2

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

Article 100-3

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des télécommunications ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécommunications autorisé, en vue de procéder à l'installation d'un dispositif d'interception.

Article 100-6

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Il est dressé procès-verbal de l'opération de destruction.

CODE DE PROCEDURE PENALE
(Partie Législative)

Section I : Transmission et exécution des demandes d'entraide

Article 694

(Loi nº 75-624 du 11 juillet 1975 art. 13 Journal Officiel du 13 juillet 1975 en vigueur le 1er janvier 1976)

(Loi nº 92-1336 du 16 décembre 1992 art. 64 Journal Officiel du 23 décembre 1992 en vigueur le 1er mars 1994)

(Loi nº 99-515 du 23 juin 1999 art. 30 Journal Officiel du 24 juin 1999)

(Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

En l'absence de convention internationale en stipulant autrement :

1º Les demandes d'entraide émanant des autorités judiciaires françaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du ministère de la justice. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie ;

2º Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises sont transmises par la voie diplomatique. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

En cas d'urgence, les demandes d'entraide sollicitées par les autorités françaises ou étrangères peuvent être transmises directement aux autorités de l'Etat requis compétentes pour les exécuter. Le renvoi des pièces d'exécution aux autorités compétentes de l'Etat

requérant est effectué selon les mêmes modalités. Toutefois, sauf convention internationale en stipulant autrement, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises doivent faire l'objet d'un avis donné par la voie diplomatique par le gouvernement étranger intéressé.

Article 694-1

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

En cas d'urgence, les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises, selon les distinctions prévues à l'article 694-2, au procureur de la République ou au juge d'instruction du tribunal de grande instance territorialement compétent. Elles peuvent également être adressées à ces magistrats par l'intermédiaire du procureur général.

Si le procureur de la République reçoit directement d'une autorité étrangère une demande d'entraide qui ne peut être exécutée que par le juge d'instruction, il la transmet pour exécution à ce dernier ou saisit le procureur général dans le cas prévu à l'article 694-4.

Avant de procéder à l'exécution d'une demande d'entraide dont il a été directement saisi, le juge d'instruction la communique immédiatement pour avis au procureur de la République.

Article 694-2

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées par le procureur de la République ou par les officiers ou agents de police judiciaire requis à cette fin par ce magistrat.

Elles sont exécutées par le juge d'instruction ou par des officiers de police judiciaire agissant sur commission rogatoire de ce magistrat lorsqu'elles nécessitent certains actes de procédure qui ne peuvent être ordonnés ou exécutés qu'au cours d'une instruction préparatoire.

Article 694-3

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées selon les règles de procédure prévues par le présent code.

Toutefois, si la demande d'entraide le précise, elle est exécutée selon les règles de procédure expressément indiquées par les autorités compétentes de l'Etat requérant, à condition, sous peine de nullité, que ces règles ne réduisent pas les droits des parties ou les garanties procédurales prévus par le présent code. Lorsque la demande d'entraide ne peut être exécutée conformément aux exigences de l'Etat requérant, les autorités compétentes françaises en informent sans délai les autorités de l'Etat requérant et indiquent dans quelles conditions la demande pourrait être exécutée. Les autorités françaises compétentes et celles de l'Etat requérant peuvent ultérieurement s'accorder sur la suite à réserver à la demande, le cas échéant, en la subordonnant au respect desdites conditions.

L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Article 694-4

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le procureur de la République saisi de cette demande ou avisé de cette demande en application du troisième alinéa de l'article 694-1 la transmet au procureur général qui détermine, s'il y a lieu, d'en saisir le ministre de la justice et donne, le cas échéant, avis de cette transmission au juge d'instruction.

S'il est saisi, le ministre de la justice informe l'autorité requérante, le cas échéant, de ce qu'il ne peut être donné suite, totalement ou partiellement, à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.

Article 694-9

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Lorsque, conformément aux stipulations prévues par les conventions internationales, le procureur de la République ou le juge d'instruction communique à des autorités judiciaires étrangères des informations issues d'une procédure pénale en cours, il peut soumettre l'utilisation de ces informations aux conditions qu'il détermine.

CODE DE PROCEDURE PENALE
(Partie Législative)

Chapitre III : Dispositions propres à l'entraide entre la France et certains Etats

Article 695-10

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Les dispositions des sections 1 et 2 du chapitre II sont applicables aux demandes d'entraide entre la France et les autres Etats parties à toute convention comportant des stipulations similaires à celles de la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne. (Voir annexe 2, p. 20).

CODE DE PROCEDURE PENALE
(Partie Législative)

Section V : Des interceptions de correspondances émises par la voie des télécommunications

Article 706-95

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 1 Journal Officiel du 10 mars 2004 en vigueur le 1er octobre 2004)

Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de

correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention.

Pour l'application des dispositions des articles 100-3 à 100-5, les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui sont exercées par le procureur de la République ou l'officier de police judiciaire requis par ce magistrat.

Le juge des libertés et de la détention qui a autorisé l'interception est informé sans délai par le procureur de la République des actes accomplis en application de l'alinéa précédent.

CODE DE PROCEDURE PENALE
(Partie Législative)

Section I : Des conditions de l'extradition

Article 696-1

(Loi nº 99-515 du 23 juin 1999 art. 30 Journal Officiel du 24 juin 1999)

(Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Aucune remise ne pourra être faite à un gouvernement étranger de personnes n'ayant pas été l'objet de poursuites ou d'une condamnation pour une infraction prévue par la présente section.

Article 696-2

(Loi nº 99-515 du 23 juin 1999 art. 30 Journal Officiel du 24 juin 1999)

(Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Le gouvernement français peut remettre, sur leur demande, aux gouvernements étrangers, toute personne n'ayant pas la nationalité française qui, étant l'objet d'une poursuite intentée au nom de l'Etat requérant ou d'une condamnation prononcée par ses tribunaux, est trouvée sur le territoire de la République.

Néanmoins, l'extradition n'est accordée que si l'infraction cause de la demande a été commise :
- soit sur le territoire de l'Etat requérant par un ressortissant de cet Etat ou par un étranger ;
- soit en dehors de son territoire par un ressortissant de cet Etat ;

- soit en dehors de son territoire par une personne étrangère à cet Etat, quand l'infraction est au nombre de celles dont la loi française autorise la poursuite en France, alors même qu'elles ont été commises par un étranger à l'étranger.

Article 696-3

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Les faits qui peuvent donner lieu à l'extradition, qu'il s'agisse de la demander ou de l'accorder, sont les suivants :

1º Tous les faits punis de peines criminelles par la loi de l'Etat requérant ;

2º Les faits punis de peines correctionnelles par la loi de l'Etat requérant, quand le maximum de la peine d'emprisonnement encourue, aux termes de cette loi, est égal ou supérieur à deux ans, ou, s'il s'agit d'un condamné, quand la peine prononcée par la juridiction de l'Etat requérant est égale ou supérieure à deux mois d'emprisonnement.

En aucun cas l'extradition n'est accordée par le gouvernement français si le fait n'est pas puni par la loi française d'une peine criminelle ou correctionnelle.

Les faits constitutifs de tentative ou de complicité sont soumis aux règles précédentes, à condition qu'ils soient punissables d'après la loi de l'Etat requérant et d'après celle de l'Etat requis.

Si la demande a pour objet plusieurs infractions commises par la personne réclamée et qui n'ont pas encore été jugées, l'extradition n'est accordée que si le maximum de la peine encourue, d'après la loi de l'Etat requérant, pour l'ensemble de ces infractions, est égal ou supérieur à deux ans d'emprisonnement.

Article 696-4

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

L'extradition n'est pas accordée :

1º Lorsque la personne réclamée a la nationalité française, cette dernière étant appréciée à l'époque de l'infraction pour laquelle l'extradition est requise ;

2º Lorsque le crime ou le délit à un caractère politique ou lorsqu'il résulte des circonstances que l'extradition est demandée dans un but politique ;

3º Lorsque les crimes ou délits ont été commis sur le territoire de la République ;

4º Lorsque les crimes ou délits, quoique commis hors du territoire de la République, y ont été poursuivis et jugés définitivement ;

5º Lorsque, d'après la loi de l'Etat requérant ou la loi française, la prescription de l'action s'est trouvée acquise antérieurement à la demande d'extradition, ou la prescription de la peine antérieurement à l'arrestation de la personne réclamée et d'une façon générale toutes les fois que l'action publique de l'Etat requérant est éteinte ;

6º Lorsque le fait à raison duquel l'extradition a été demandée est puni par la législation de l'Etat requérant d'une peine ou d'une mesure de sûreté contraire à l'ordre public français ;

7º Lorsque la personne réclamée serait jugée dans l'Etat requérant par un tribunal n'assurant pas les garanties fondamentales de procédure et de protection des droits de la défense ;

8º Lorsque le crime ou le délit constitue une infraction militaire prévue par le livre III du code de justice militaire.

Article 696-5

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Si, pour une infraction unique, l'extradition est demandée concurremment par plusieurs Etats, elle est accordée de préférence à l'Etat contre les intérêts duquel l'infraction était dirigée, ou à celui sur le territoire duquel elle a été commise.

Si les demandes concurrentes ont pour cause des infractions différentes, il est tenu compte, pour décider de la priorité, de toutes circonstances de fait, et, notamment, de la gravité relative et du lieu des infractions, de la date respective des demandes, de l'engagement qui serait pris par l'un des Etats requérants de procéder à la réextradition.

Article 696-6

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Sous réserve des exceptions prévues à l'article 696-34, l'extradition n'est accordée qu'à la condition que la personne extradée ne sera ni poursuivie, ni condamnée pour une infraction autre que celle ayant motivé l'extradition et antérieure à la remise.

Article 696-7

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I, art. 198 V Journal Officiel du 10 mars 2004)

Dans le cas où une personne réclamée est poursuivie ou a été condamnée en France, et où son extradition est demandée au gouvernement français à raison d'une infraction différente, la remise n'est effectuée qu'après que la poursuite est terminée, et, en cas de condamnation, après que la peine a été exécutée.

Toutefois, cette disposition ne fait pas obstacle à ce que la personne réclamée puisse être envoyée temporairement pour comparaître devant les tribunaux de l'Etat requérant, sous la condition expresse qu'elle sera renvoyée dès que la justice étrangère aura statué.

Est régi par les dispositions du présent article le cas où la personne réclamée est soumise à la contrainte judiciaire par application des dispositions du titre VI du livre V du présent code.

Annexe 2. **Dispositions propres à l'entraide entre la France et les autres Etats membres de l'Union européenne.**

CODE DE PROCEDURE PENALE
(Partie Législative)

Section I : Transmission et exécution des demandes d'entraide

Article 695-1

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Sauf si une convention internationale en stipule autrement et sous réserve des dispositions de l'article 694-4, les demandes d'entraide sont transmises et les pièces d'exécution retournées directement entre les autorités judiciaires territorialement compétentes pour les délivrer et les exécuter, conformément aux dispositions des articles 694-1 à 694-3.

CODE DE PROCEDURE PENALE
(Partie Législative)

Paragraphe 2 : Effets du mandat d'arrêt européen

Article 695-18

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Lorsque le ministère public qui a émis le mandat d'arrêt européen a obtenu la remise de la personne recherchée, celle-ci ne peut être poursuivie, condamnée ou détenue en vue de l'exécution d'une peine privative de liberté pour un fait quelconque antérieur à la remise et autre que celui qui a motivé cette mesure, sauf dans l'un des cas suivants :

1º Lorsque la personne a renoncé expressément, en même temps qu'elle a consenti à sa remise, au bénéfice de la règle de la spécialité dans les conditions prévues par la loi de l'Etat membre d'exécution ;

2º Lorsque la personne renonce expressément, après sa remise, au bénéfice de la règle de la spécialité dans les conditions prévues à l'article 695-19 ;

3º Lorsque l'autorité judiciaire de l'Etat membre d'exécution, qui a remis la personne, y consent expressément ;

4º Lorsque, ayant eu la possibilité de le faire, la personne recherchée n'a pas quitté le territoire national dans les quarante-cinq jours suivant sa libération définitive, ou si elle y est retournée volontairement après l'avoir quitté ;

5º Lorsque l'infraction n'est pas punie d'une peine privative de liberté.

Article 695-19

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Pour le cas visé au 2º de l'article 695-18, la renonciation est donnée devant la juridiction d'instruction, de jugement ou d'application des peines dont la personne relève après sa remise et a un caractère irrévocable.

Lors de la comparution de la personne remise, la juridiction compétente constate l'identité et recueille les déclarations de cette personne. Il en est dressé procès-verbal. L'intéressé, assisté le cas échéant de son avocat et, s'il y a lieu, d'un interprète, est informé des conséquences juridiques de sa renonciation à la règle de la spécialité sur sa situation pénale et du caractère irrévocable de la renonciation donnée.

Si, lors de sa comparution, la personne remise déclare renoncer à la règle de la spécialité, la juridiction compétente, après avoir entendu le ministère public et l'avocat de la personne, en donne acte à celle-ci. La décision précise les faits pour lesquels la renonciation est intervenue.

Article 695-20

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

Pour les cas visés au 3º des articles 695-18 et 695-21, la demande de consentement est adressée par le ministère public à l'autorité judiciaire de l'Etat membre d'exécution. Elle doit contenir, dans les conditions prévues à l'article 695-14, les renseignements énumérés à l'article 695-13.

Pour le cas mentionné au 3º de l'article 695-18, elle est accompagnée d'un procès-verbal consignant les déclarations faites par la personne remise concernant l'infraction pour laquelle le consentement de l'autorité judiciaire de l'Etat membre d'exécution est demandé.

Article 695-21

(inséré par Loi nº 2004-204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

I. - Lorsque le ministère public qui a émis le mandat d'arrêt européen a obtenu la remise de la personne recherchée, celle-ci ne peut, sans le consentement de l'Etat membre d'exécution, être remise à un autre Etat membre en vue de l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté pour un fait quelconque antérieur à la remise et différent de l'infraction qui a motivé cette mesure, sauf dans l'un des cas suivants :

1º Lorsque la personne ne bénéficie pas de la règle de la spécialité conformément aux 1º à 4º de l'article 695-18 ;

2º Lorsque la personne accepte expressément, après sa remise, d'être livrée à un autre Etat membre dans les conditions prévues à l'article 695-19 ;

3º Lorsque l'autorité judiciaire de l'Etat membre d'exécution, qui a remis la personne, y consent expressément.

II. - Lorsque le ministère public qui a délivré un mandat d'arrêt européen a obtenu la remise de la personne recherchée, celle-ci ne peut être extradée vers un Etat non membre de l'Union européenne sans le consentement de l'autorité compétente de l'Etat membre qui l'a remise.

7.3 Country profile on cybercrime legislation – Germany

Project on Cybercrime
www.coe.int/cybercrime

Draft (1 June 2007)

Cybercrime legislation – country profile

Germany[225]

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

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

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

Country:	**Germany**	
Signature of Convention:	Yes: 23 November 2001	
Ratification/accession:	No If not yet signed/acceded to: What measures are being undertaken in your country to become a Party? What specific obstacles (legislative or other) prevent ratification/accession? The necessary legislation for ratification is currently being prepared. However, before the Convention can be ratified, the process of implementation must be completed. In this respect, German law largely complies with the requirements of the Council of Europe Convention. However, a few amendments and changes to national law remain necessary. The implementation of the	

[225] This profile was prepared in May/June 2007. In the meantime the amendments to the legislation have been adopted by the Federal Parliament. The only outstanding issue is the age-limit for child pornography. Once this has been amended, Germany will be able to ratify the Convention on Cybercrime.

	Convention will be effected through the following amendments to German law: • The Council of Europe's provisions regarding substantive criminal law – excluding the provision on content-related offences (Title 3 of the Council of Europe Convention) – is addressed by the German draft law against computer crime (BT-Drs. 16/3656) which was adopted by the Bundestag on 24 May 2007 (draft law regarding substantive criminal law). This law is also intended to cover the modifications introduced by the EU Framework Decision on attacks against information systems. • The Convention's provision on content-related offences (Title 3 of the Council of Europe Convention) is addressed by the German draft law to implement the EU Framework Decision on combating the sexual exploitation of children and child pornography (BT-Drs. 16/3439), which is currently under consideration in the Bundestag. • The Convention's provision regarding procedural law is addressed by the German draft law revising provisions on telecommunications surveillance and other covert investigative measures and implementing EU Directive 2006/24/EC (draft law regarding criminal procedural law). The draft law was adopted by the Federal Cabinet on 18 April 2007.
Provisions of the Convention	***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	Computer data are covered by section 202a (2) of the German Criminal Code (*Strafgesetzbuch*, StGB).
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	Covered by section 202a (1) StGB.
Article 3 – Illegal interception	Currently covered in part by section 201 StGB as well as section 148 in connection with section 89 of the German Telecommunications Act (*Telekommunikationsgesetz*, TKG). Completely covered by the proposed section 202b of the draft law regarding substantive criminal law.
Article 4 – Data interference	Covered by section 303a StGB.
Article 5 – System interference	Covered in part by section 303b StGB. Amendment is necessary with regard to private computer systems and to the requirements of data input and transmission. This issue is addressed by the proposed amendment to section 303b in the draft law regarding

	substantive criminal law
Article 6 – Misuse of devices	Covered by the proposed section 202c in the draft law regarding substantive criminal law.
Article 7 – Computer-related forgery	Covered by section 269 StGB.
Article 8 – Computer-related fraud	Covered by section 263a StGB.
Article 9 – Offences related to child pornography	Covered in part by section 184b StGB. An amendment is necessary with respect to the age of the person involved (currently a person under the age of 14). This issue is addressed by the above-mentioned draft law to implement the EU Framework Decision on combating the sexual exploitation of children and child pornography.
Title 4 – Offences related to infringements of copyright and related rights	See below.
Article 10 – Offences related to infringements of copyright and related rights	Covered by sections 106 ff. of the German Copyright Act (*Urheberrechtsgesetz*, UrhG).
Article 11 – Attempt and aiding or abetting	Attempt is covered by sections 22-24 StGB. Aiding and abetting is covered by sections 26 and 27 StGB.
Article 12 – Corporate liability	Covered by sections 30 and 130 of the German Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OWiG).
Article 13 – Sanctions and measures	Article 13 (1) is covered by the above-mentioned articles (sections 202a, 202b, 202c, 263a, 269, 303a, 303a StGB and section 106 UrhG). Article 13 (2) is covered by section 30 OWiG.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	See below (Articles 16-21).
Article 15 – Conditions and safeguards	See below (Articles 16-21).
Article 16 – Expedited preservation of stored computer data	With respect to computer data, Article 16 is covered by sections 94, 95 and 98 of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO). With respect to traffic data, Article 16 is covered in part by sections 100g and 100h StPO. The necessary amendment is addressed by the proposed amendment to section 100g in the draft law regarding criminal procedural law.
Article 17 – Expedited preservation and partial disclosure of traffic data	Covered in part by sections 100g and 100h StPO. The necessary amendments are addressed by the proposed amendment to section 100g in the draft law regarding criminal procedural law.
Article 18 – Production order	Article 18 (1) lit. a is covered by section 95 StPO. Article 18 (1) lit. b is covered by sections 112 and 113 TKG.
Article 19 – Search and seizure of stored computer data	Article 19 (1) and (3) are covered by sections 94, 95, 102, 103, 105, 161 and 163 StPO. Article 19 (2) is covered by the proposed amendment to section 110 (3) StPO in the draft law regarding criminal procedural law.
Article 20 – Real-time collection of traffic data	Covered in part by section 100g StPO. The necessary amendments are addressed by the proposed amendment to section 100g in the

	draft law regarding criminal procedural law.
Article 21 – Interception of content data	Covered by sections 100a and 100b StPO.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	Covered by sections 3-9 StGB.
Chapter III – International co-operation	
Article 24 – Extradition	Covered by sections 2 and 3 of the Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, IRG) in the absence of applicable international agreements.
Article 25 – General principles relating to mutual assistance	Covered by provisions set forth in the IRG (e.g. sections 2 ff.: extradition; sections 59 ff.: other forms of mutual legal assistance).
Article 26 – Spontaneous information	Covered by sections 61a and 83j IRG in the absence of applicable international agreements.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 28 – Confidentiality and limitation on use	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 29 – Expedited preservation of stored computer data	Covered by sections 66 f. IRG in the absence of applicable international agreements.
Article 30 – Expedited disclosure of preserved traffic data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 31 – Mutual assistance regarding accessing of stored computer data	Covered by section 66 IRG in the absence of applicable international agreements.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Covered by section 94 StPO.
Article 33 – Mutual assistance in the real-time collection of traffic data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 34 – Mutual assistance regarding the interception of content data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 35 – 24/7 Network	Germany has established a 24/7 contact point within the Bundeskriminalamt. It is a member of the 24/7 Network of the "G8 High-Tech Crime Subgroup" and of the ICPO Interpol.

Article 42 – Reservations	

Appendix

A. German Criminal Code (*Strafgesetzbuch*, StGB):

Section 3 Applicability to Domestic Acts
German criminal law shall apply to acts which were committed domestically.

Section 4 Applicability to Acts on German Ships and Aircraft
German criminal law shall apply, regardless of the law of the place where the act was committed, to acts which are committed on a ship or in an aircraft that is entitled to fly the federal flag or the national insignia of the Federal Republic of Germany.

Section 5 Acts Abroad Against Domestic Legal Interests
German criminal law shall apply, regardless of the law of the place the act was committed, to the following acts committed abroad:

1. preparation of a war of aggression (section 80);
2. high treason (sections 81 to 83);
3. endangering the democratic rule of law:
a) in cases under sections 89 and 90a subsection (1), and section 90b, if the perpetrator is a German and has his livelihood in the territorial area of applicability of this law; and
b) in cases under sections 90 and 90a subsection (2);
4. treason and endangering external security (sections 94 to 100a);
5. crimes against the national defence:
a) in cases under sections 109 and 109e to109g; and
b) in cases under sections 109a, 109d and 109h, if the perpetrator is a German and has his livelihood in the territorial area of applicability of this law;
6. abduction and casting political suspicion on another (sections 234a, 241a), if the act is directed against a person who has his domicile or usual residence in Germany;
6a. child stealing in cases under section 235 subsection (2), number 2, if the act is directed against a person who has his domicile or usual residence in Germany;
7. violation of business or trade secrets of a business located within the territorial area of applicability of this law, an enterprise that has its registered place of business there, or an enterprise with its registered place of business abroad, which is dependent on an enterprise with its registered place of business within the territorial area of applicability of this law and constitutes with it a group;
8. crimes against sexual self-determination:
a) in cases under section 174 subsections (1) and (3), if the perpetrator and the person against whom the act was committed are Germans at the time of the act and have their livelihoods in Germany; and
b) in cases under sections 176 to 176b and 182, if the perpetrator is a German;
9. termination of pregnancy (section 218), if the perpetrator at the time of the act is a German and has his livelihood in the territorial area of applicability of this law;
10. false unsworn testimony, perjury and false affirmations in lieu of an oath (sections 153 to 156) in proceedings pending before a court or other German agency within the territorial area of applicability of this law, which is competent to administer oaths or affirmations in lieu of an oath;
11. crimes against the environment in cases under sections 324, 326, 330 and 330a, which were committed in the area of Germany's exclusive economic zone, to the extent that international conventions on the protection of the sea permit their prosecution as crimes;
11a. crimes under section 328 subsection (2), numbers 3 and 4 subsections (4) and (5), also

in conjunction with section 330, if the perpetrator is a German at the time of the act;
12. acts which a German public official or a person with special public service obligations commits during his official stay or in connection with his duties;
13. acts committed by a foreigner as a public official or as a person with special public service obligations;
14. acts which someone commits against a public official, a person with special public service obligations, or a soldier in the Federal Armed Forces during the discharge of his duties or in connection with his duties;
14a. bribery of a member of parliament (section 108e), if the perpetrator is a German at the time of the act or the act was committed in relation to a German;
15. trafficking in organs (section 18 of the Transplantation Law), if the perpetrator is a German at the time of the act.

Section 6 Acts Abroad Against Internationally Protected Legal Interests
German criminal law shall further apply, regardless of the law of the place of their commission, to the following acts committed abroad:
1. (deleted);
2. serious criminal offences involving nuclear energy, explosives and radiation in cases under sections 307 and 308 subsections (1) to (4), section 309 subsection (2) and section 310;
3. assaults against air and sea traffic (section 316c);
4. trafficking in human beings for the purpose of sexual exploitation and for the purpose of the exploitation of workers and promotion of trafficking in human beings (sections 232 to 233a);
5. unauthorised distribution of narcotics;
6. dissemination of pornographic writings in cases under sections 184a and 184b subsections (1) to (3), also in conjunction with section 184c, first sentence;
7. counterfeiting of money and securities (sections 146, 151 and152), guaranteed payment cards and blank Eurochecks (section 152b subsections (1) to (4)), as well as their preparation (sections 149,151,152 and 152b subsection (5));
8. subsidy fraud (section 264);
9. acts which, on the basis of an international agreement binding on the Federal Republic of Germany, shall also be prosecuted if they are committed abroad.

Section 7 Applicability to Acts Abroad in Other Cases
(1) German criminal law shall apply to acts which were committed abroad against a German, if the act is punishable at the place of its commission or the place of its commission is subject to no criminal law enforcement.
(2) German criminal law shall apply to other acts which were committed abroad, if the act is punishable at the place of its commission or the place of its commission is subject to no criminal law enforcement and if the perpetrator:
1. was a German at the time of the act or became one after the act; or
2. was a foreigner at the time of the act, was found to be in Germany and, although the Extradition Act would permit extradition for such an act, is not extradited, because a request for extradition within a reasonable period of time is not made, is rejected, or the extradition is not practicable.

Section 8 Time of the Act
An act is committed at the time the perpetrator or the inciter or accessory acted, or in case of an omission, should have acted. The time when the result occurs is not determinative.

Section 9 Place of the Act
(1) An act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or at which the result, which is an element of the offence, occurs or should occur according to the understanding of the perpetrator.
(2) Incitement or accessoryship is committed not only at the place where the act was

committed, but also at every place where the inciter or accessory acted or, in case of an omission, should have acted or where, according to his understanding, the act should have been committed. If the inciter or accessory in an act abroad acted domestically, then German criminal law shall apply to the incitement or accessoryship, even if the act is not punishable according to the law of the place of its commission.

Section 11 Terms Relating to Persons and Subject Matter

(1) Within the meaning of this law:

1. a relative is whoever belongs among the following persons:

a) relations by blood or marriage in direct line, the spouse, the same-sex partner, the fiancé, siblings, the spouses of siblings, siblings of spouses, even if the marriage or same-sex partnership upon which the relationship was based no longer exists, or when the relationship by blood or marriage has ceased to exist;

b) foster parents and foster children;

2. a public official is whoever, under German law:

a) is a civil servant or judge;

b) otherwise has an official relationship with public law functions; or

c) has been appointed to a public authority or other agency or has been commissioned to perform duties of public administration without prejudice to the organisational form chosen to fulfil such duties;

3. a judge is whoever under German law is a professional or honorary judge;

4. a person with special public service obligations is whoever, without being a public official, is employed by or is active for:

a) a public authority or other agency which performs duties of public administration; or

b) an association or other union, business or enterprise which carries out duties of public administration for a public authority or other agency,

and is formally obligated by law to fulfil duties in a conscientious manner;

5. an unlawful act is only one which fulfils all the elements of a penal norm;

6. the undertaking of an act is its attempt and completion;

7. a public authority is also a court;

8. a measure is every measure of reform and prevention, forfeiture, confiscation and rendering unusable;

9. compensation is every consideration consisting of a material benefit;

(2) An act is also intentional within the meaning of this law, if it fulfils the statutory elements of an offence which requires intent in relation to the conduct, even if only negligence is required as to the specific result caused thereby.

(3) Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection.

Section 22 Definition of Terms

Whoever, in accordance with his understanding of the act, takes an immediate step towards the realisation of the elements of the offence, attempts to commit a crime.

Section 23 Punishability for an Attempt

(1) An attempt to commit a serious criminal offence is always punishable, while an attempt to commit a less serious criminal offence is only punishable if expressly provided by law.

(2) An attempt may be punished more leniently than the completed act (section 49a subsection (1)).

(3) If the perpetrator, due to a gross lack of understanding, fails to recognise that the attempt could not possibly lead to completion due to the nature of the object on which or the means with which it was to be committed, the court may withhold punishment or in its own discretion mitigate the punishment (section 49 subsection(2)).

Section 24 Abandonment

(1) Whoever voluntarily renounces further execution of the act or prevents its

completion shall not be punished for an attempt. If the act is not completed due in no part to the contribution of the abandoning party, he shall not be punished if he makes voluntary and earnest efforts to prevent its completion.

(2) If more than one person participate in the act, whoever voluntarily prevents its completion will not be punished for an attempt. However his voluntary and earnest efforts to prevent the completion of the act shall suffice for exemption from punishment if the act is not completed due in no part to his contribution or is committed independently of his earlier contribution to the act.

Section 26 Incitement

Whoever intentionally induces another to intentionally commit an unlawful act shall, as an inciter, be punished the same as a perpetrator.

Section 27 Accessoryship

(1) Whoever intentionally renders aid to another in that person's intentional commission of an unlawful act shall be punished as an accessory.

(2) The punishment for the accessory corresponds to the punishment threatened for the perpetrator. It shall be mitigated pursuant to section 49 subsection (1).

Section 149 Preparation of the Counterfeiting of Money and Stamps

(1) Whoever prepares a counterfeiting of money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another:

1. plates, frames, type, blocks, negatives, stencils, computer programs or similar equipment which by its nature is suited to the commission of the act;
2. paper which is identical or confusingly similar to the type of paper which is designated for the production of money or official stamps and specially protected against imitation, or
3. holograms or other elements serving to afford protection against counterfeiting

shall be punished with imprisonment for not more than five years or a fine if he prepared the counterfeiting of money, otherwise with imprisonment for not more than two years or a fine.

(2) Whoever voluntarily:

1. renounces the execution of the prepared act and averts a danger caused by him that others continue to prepare the act or execute it, or prevents the completion of the act; and
2. destroys or renders useless the means for counterfeiting, to the extent they still exist and are useful for counterfeiting, or reports their existence to a public authority or surrenders them there,

shall not be punished under subsection (1).

(3) If the danger that others continue to prepare or execute the act is averted, or the completion of the act is prevented due in no part to the contribution of the perpetrator, then the voluntary and earnest efforts of the perpetrator to attain this goal shall suffice in lieu of the prerequisites of subsection (2), no 1.

Section 184b Dissemination, Purchase, and Possession of Pornographic Writings Involving Children

(1) Whoever, in relation to pornographic writings (section 11 subsection (3)) that have as their object the sexual abuse of children (sections 176 to 176b) (pornographic writings involving children):

1. disseminates them;
2. publicly displays, posts, presents or otherwise makes them accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends or undertakes to import or export them, in order to use them or copies made from them within the meaning of numbers 1 or 2 or makes such use possible by another,

shall be punished with imprisonment for three months to five years.

(2) Whoever undertakes to obtain possession for another of pornographic writings involving children that reproduce an actual or true to life event, shall be similarly punished.

(3) In cases under subsection (1) or subsection (2), imprisonment for six months to ten years shall be imposed if the perpetrator acts on a commercial basis or as a member of a

gang that has combined for the continued commission of such acts and the pornographic writings involving children reproduce an actual or true to life event.

(4) Whoever undertakes to obtain possession of pornographic writings involving children that reproduce an actual or true to life event shall be punished with imprisonment for up to two years or a fine. Whoever possesses the writings set forth in sentence 1 shall be similarly punished.

(5) Subsections (2) and (4) shall not apply to acts that exclusively serve the fulfilment of legal, official, or professional duties.

(6) In cases under subsection (3), section 73d shall be applicable. Objects to which a crime under subsection (2) or (4) relates shall be confiscated. Section 74a shall be applicable.

Section 201 Violation of the Confidentiality of the Spoken Word

(1) Whoever, without authorisation:

1. makes an audio recording of the privately spoken words of another; or
2. uses or makes a recording thus produced accessible to a third party,

shall be punished with imprisonment for not more than three years or a fine.

(2) Whoever, without authorisation:

1. listens with an eavesdropping device to privately spoken words not intended to come to his attention; or
2. publicly communicates, verbatim, or the essential content of the privately spoken words of another recorded pursuant to subsection (1), number 1, or listened to pursuant to subsection (2), number 1,

shall be similarly punished. The act under sentence 1, number 2, shall only be punishable if the public communication is capable of interfering with the legitimate interests of another. It is not unlawful if the public communication was made for the purpose of safeguarding pre-eminent public interests.

(3) Whoever, as a public official or a person with special public service obligations, violates the confidentiality of the spoken word (subsections (1) and (2)) shall be punished with imprisonment for not more than five years or a fine.

(4) An attempt shall be punishable.

(5) The audio recording media and eavesdropping devices which the perpetrator or the inciter or accessory used may be confiscated. Section 74a shall be applicable.

Section 202a Data Espionage

(1) Whoever, without authorisation, obtains data for himself or another, which were not intended for him and were specially protected against unauthorised access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall be only those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

Section 202a Data Espionage (draft law)

(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) Within the meaning of subsection (1), data shall be only those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

Section 202b Data Interception (draft law)

Whoever, without authorisation and through the use of technological means, obtains for himself or another party access to data not intended for him (section 202a subsection (2)) from non-public transmissions of data or from electromagnetic emissions of data processing equipment, shall be punished with imprisonment for no more than two years or a fine, provided that the offence is not subject to a more severe penalty under other provisions.

Section 202c Preparation of Data Espionage or Data Interception (draft law)

(1) Whoever prepares a criminal offence pursuant to section 202a or 202b by creating, procuring for himself or another party, selling, giving over to another party, disseminating or otherwise providing access to

1. passwords or other security codes that enable access to data (section 202a subsection (2)), or
2. computer programmes whose purpose is to commit such an act,

shall be punished with imprisonment for no more than one year or a fine.

(2) Section 149 subsections 2 and 3 shall apply accordingly.

Section 263 Fraud

(1) Whoever, with the intent of obtaining an unlawful material benefit for himself or a third person, damages the assets of another by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment for six months to ten years. An especially serious case exists, as a rule, if the perpetrator:

1. acts on a commercial basis or as a member of a gang which has combined for the continued commission of falsification of documents or fraud;
2. causes an asset loss of great magnitude or by the continued commission of fraud acts with the intent of placing a large number of human beings in danger of loss of assets;
3. places another person in financial need;
4. abuses his powers or his position as a public official; or
5. feigns an insured event after he or another have, to this end, set fire to a thing of significant value or destroyed it, in whole or in part, through the setting of a fire or caused the sinking or wrecking of a ship.

(4) Section 243 subsection (2) as well as sections 247 and 248a shall apply accordingly.

(5) Whoever on a commercial basis commits fraud as a member of a gang which has combined for the continued commission of crimes under sections 263 to264 or 267 to 269, shall be punished with imprisonment for one year to ten years, in less serious cases with imprisonment for six months to five years.

(6) The court may order supervision of conduct (section 68 subsection (1)).

(7) Sections 43a, 73d shall be applicable if the perpetrator acted as a member of a gang which has combined for the continued commission of crimes under sections 263 to 264 or 267 to 269. Section 73d shall also be applicable if the perpetrator acted on a commercial basis.

Section 263a Computer Fraud

(1) Whoever, with the intent of obtaining an unlawful material benefit for himself or a third person, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the order of events, shall be punished with imprisonment for not more than five years or a fine.

(2) Section 263 subsections (2) to (7) shall apply accordingly.

(3) Whoever prepares a criminal offence under subsection (1) by manufacturing computer programs, the purpose of which is to commit such an act, or for himself or another, obtains offers for sale, holds, or gives to another, shall be punished with imprisonment for not more than three years or a fine.

(4) in cases under subsection (3), section 149 subsections (2) and (3) shall apply accordingly.

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment for six months to ten years. An especially serious case exists, as a rule, if the perpetrator:

1. acts on a commercial basis or as a member of a gang which has combined for the

continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents on a commercial basis as a member of a gang which has combined for the continued commission of crimes under sections 263 to 264 or 267 to 269 shall be punished with imprisonment for one year to ten years, in less serious cases with imprisonment for six months to five years.

Section 269 Falsification of Legally Relevant Data

(1) Whoever, for purposes of deception in legal relations, stores or modifies legally relevant data in such a way that a counterfeit or falsified document would exist upon its retrieval, or uses data stored or modified in such a manner, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) Section 267 subsections (3) and (4), shall apply accordingly.

Section 303a Alteration of Data (draft law concerning subsection 3 only)

(1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a subsection (2)) shall be punished with imprisonment for not more than two years or a fine.

(2) An attempt shall be punishable.

(3) Section 202c shall apply accordingly with respect to the preparation of a criminal offence under subsection (1).

Section 303b Computer Sabotage

(1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another party or a public authority by:
1. committing an act under section 303a subsection (1); or
2. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

Section 303b Computer Sabotage (draft law)

(1) Whoever seriously interferes with data processing which is of substantial significance to another party by
1. committing an act under section 303a subsection (1),
2. enters or transmits data (section 202a subsection (2)) with the intention of causing harm to another party or
3. Destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be punished with imprisonment of no more than three years or a fine.

(2) If such interference involves data processing that is of substantial significance to the business or enterprise of another party or to a public authority, the penalty shall consist of imprisonment of no more than five years or a fine.

(3) An attempt shall be punishable.

(4) In particularly serious cases under subsection (2), the punishment shall consist of imprisonment from six months to ten years. As a rule, a case is to be considered particularly serious when the perpetrator
1. causes a loss of assets of great magnitude,
2. acts on a commercial basis or as a member of a gang established to commit recurrent acts of computer sabotage,
3. interferes with the provision of goods or services vital to the population or compromises the security of the Federal Republic of Germany

(5) Section 202c shall apply accordingly with respect to the preparation of a criminal offence under subsection (1).

B. Copyright Act (*Gesetz über Urheberrecht und verwandte Schutzrechte Urheberrechtsgesetz*, UrhG)

Section 106 Unauthorised Exploitation of Copyrighted Works

(1) Whoever reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, other than in a manner allowed by law and without the right holder's consent, shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 107 Unlawful Affixing of Designation of Author

(1) Whoever

1. without the author's consent, affixes a designation of author (section 10 subsection (1)) to the original of a work of fine art or distributes an original bearing such designation,
2. affixes a designation of author (section 10 subsection (1)) on a copy, adaptation or transformation of a work of fine art in such manner as to give to the copy, adaptation or transformation the appearance of an original or distributes a copy, adaptation or transformation bearing such designation,

shall be punished with imprisonment for up to three years or a fine provided the offence is not subject to a more severe penalty under other provisions.

(2) An attempt shall be punishable.

Section 108 Infringement of Neighbouring Rights

(1) Whoever, other than in a manner allowed by law and without the right holder's consent:

1. reproduces, distributes or publicly communicates a scientific edition (section 70) or an adaptation or transformation of such edition;
2. exploits a posthumous work or an adaptation or transformation of such work contrary to section 71;
3. reproduces, distributes or publicly communicates a photograph (section 72) or an adaptation or transformation of a photograph;
4. exploits a performance contrary to section 77 subsection (1) or (2) or section 78 subsection (1);
5. exploits an audio recording contrary to section 85;
6. exploits a broadcast contrary to section 87;
7. exploits a video or video and audio recording contrary to section 94 or section 95 in conjunction with section 94;
8. uses a database contrary to section 87b (1),

shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 108a Unlawful Exploitation on a Commercial Basis

(1) Where the person committing the acts referred to in sections 106 to 108 does so on a commercial basis, the penalty shall be imprisonment for up to five years or a fine.

(2) An attempt shall be punishable.

Section 108b Unauthorised interference with technical protection measures and information necessary for rights management

(1) Any person who,

1. with the intention of enabling access to or use of a work protected under this Act or other subject matter protected under this Act, circumvents an effective technical measure without the consent of the right holder, or
2. knowingly without authorisation

a) removes or alters rights management information originating from right holders, if any such information is affixed to a reproduction of a work or other protected subject matter or is published in connection with the public communication of such a work or other protected subject matter, or

(b) disseminates, prepares for dissemination, broadcasts, publicly communicates or makes available to the public a work or other protected subject matter where rights management information has been removed or altered without authorisation

and in so doing has at least recklessly induced, enabled, facilitated or concealed the

infringement of copyright or related rights
shall, if the offence was not committed for the exclusive private use of the perpetrator or persons personally associated with the perpetrator or is not related to such use, be punished with imprisonment for no more than one year or a fine.

(2) Punishment shall also be imposed upon any person who, in violation of section 95a subsection (3), produces, imports, disseminates, sells or rents a device, product or component for commercial purposes.

(3) Where the person committing the acts referred to in subsection (1) does so on a commercial basis, the penalty shall be imprisonment for no more than three years or a fine.

C. Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OWiG)

Section 30 Regulatory Fine Imposed on Legal Persons and on Associations of Persons

(1) Where a person acting

1. as an entity authorised to represent a legal person or as a member of such an entity,
2. as chairman of the executive committee of an association without legal capacity or as a member of such committee,
3. as a partner authorised to represent a partnership with legal capacity, or
4. as the authorised representative with full power of attorney or in a managerial position as procura holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3,
5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position,

has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association.

(2)The regulatory fine shall amount

1. in the case of a criminal offence committed with intent, to not more than one million Euros,
2. in the case of a criminal offence committed negligently, to not more than five hundred thousand Euros.

Where a regulatory offence has been committed, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence at issue. The second sentence shall also apply where an act simultaneously constituting a criminal offence and a regulatory offence has been committed, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the maximum pursuant to the first sentence.

(3) Section 17 subsection 4 and section 18 shall apply *mutatis mutandis*.

(4) If criminal proceedings or proceedings to impose a regulatory fine are not instituted in respect of the criminal offence or the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. However, independent assessment of a regulatory fine against the legal person or association of persons shall be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1, second sentence, shall remain unaffected.

(5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a forfeiture order, pursuant to sections 73 or 73a of the Criminal Code or pursuant to section 29a, against such person or association of persons.

Section 130

(1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner as such and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel.

(2) An operation or undertaking within the meaning of subsection 1 shall include a public enterprise.

(3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum regulatory fine imposable for the breach of duty. The second sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine imposable for the breach of duty exceeds the maximum pursuant to the first sentence.

D. German Code of Criminal Procedure (*Strafprozessordnung*, StPO)

Section 94 Objects Which May Be Seized

(1) Objects which may have importance as evidence for the investigation shall be impounded or be secured in another manner.

(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.

(3) Subsections (1) and (2) shall also apply to driver's licenses which are subject to confiscation.

Section 95 Obligation to Surrender

(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce and to deliver it upon request.

(2) In the case of non-compliance, the coercive measures provided under section 70 may be used against such person. This shall not apply to persons entitled to refuse to testify.

Section 98 Order of Seizure

(1) Seizures shall be ordered only by the judge and, in exigent circumstances, by the public prosecution office and officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the judge.

(2) An official who seized an object without judicial order shall within three days apply for judicial approval if neither the person concerned nor an adult relative was present at the seizure, or if the person concerned and, if he was absent, an adult relative of that person raised express objection to the seizure. The person concerned may at any time apply for a judicial decision. To the extent that public charges are not preferred, the decision shall be made by the Local Court in whose district the seizure took place. If a seizure, seizure of mail or a search has already been made in another district, the Local Court in the district in which the public prosecution office conducting the preliminary proceedings has its seat shall issue a decision. In this case, the person concerned may also submit the application to the Local Court in whose district the seizure took place. If this Local Court is not competent pursuant to the fourth sentence, the judge shall forward the application to the competent Local Court. The person concerned shall be informed of his rights.

(3) The judge shall be notified of the seizure within three days if the seizure was made by the public prosecution office or by one of the officials assisting it after the public charges were preferred; the objects seized shall be put at his disposal.

(4) If it is necessary to make a seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior authority of the Federal Armed Forces shall be requested to carry out such seizure. The requesting agency

shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 100a Conditions Regarding Interception of Telecommunications
Interception and recording of telecommunications may be ordered if certain facts substantiate the suspicion that a person was the perpetrator or inciter of, or accessory to

1. a) criminal offences against peace, of high treason, of endangering the democratic state based on the rule of law, or of treason and of endangering external security (sections 80 to 82, 84 to 86, 87 to 89, 94 to 100a of the Criminal Code, section 20 subsection (1), numbers 1 to 4 of the Associations Act);

   b) criminal offences against national defence (sections 109d to 109h of the Criminal Code);

   c) criminal offences against public order (sections 129 to 130 of the Criminal Code, section 92 subsection (1), number 7 of the Residence Act),

   d) incitement or accessoryship to desertion or incitement to disobedience (sections 16, 19 in conjunction with section 1 subsection (3) of the Military Criminal Code) without being a member of the Federal Armed Forces;

   e) criminal offences against the security of the troops of the non-German contracting parties to the North Atlantic Treaty stationed in the Federal Republic of Germany or of the troops of one of the Three Powers present in *Land* Berlin (sections 89, 94 to 97, 98 to 100, 109d to 109g of the Criminal Code, sections 16 and 19 of the Military Criminal Code in conjunction with Article 7 of the Fourth Criminal Law Amendment Act);

2. counterfeiting money or shares or bonds (sections 146, 151, 152 of the Criminal Code),

   aggravated trafficking in human beings pursuant to section 181, numbers 2 and 3 of the Criminal Code,

   murder, manslaughter or genocide (sections 211, 212, 220a of the Criminal Code),

   a criminal offence against personal liberty (sections 234, 234a, 239a, 239b of the Criminal Code),

   gang theft (section 244 subsection (1), number 2 of the Criminal Code) or aggravated gang theft (section 244a of the Criminal Code),

   robbery or extortion resembling robbery (sections 249 to 251, 255 of the Criminal Code),

   extortion (section 253 of the Criminal Code),

   commercial handling of stolen goods or gang handling of stolen goods (section 260 of the Criminal Code) or commercial gang handling (section 260a of the Criminal Code),

   money laundering or concealment of unlawfully obtained assets pursuant to section 261 subsection (1), (2) or (4) of the Criminal Code,

   a criminal offence endangering the general public in the cases of sections 306 to 306c, or section 307 subsection (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314 or section 315 subsection (3), section 315b subsection (3) or sections 316a or 316c of the Criminal Code,

3. a criminal offence pursuant to section 52a subsections (1) to (3), section 53 subsection (1), first sentence, numbers 1, 2, second sentence of the Weapons Act, section 34 subsections (1) to (6) of the Foreign Trade and Payments Act or pursuant to section 19 subsections (1) to (3), section 20 subsection (1) or (2), each also in conjunction with section 21 or section 22a subsections (1) to (3) of the War Weapons Control Act,

4. a criminal offence pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, of the Narcotics Act under the conditions set forth therein or a criminal offence pursuant to sections 29a, 30 subsection (1), numbers 1, 2, 4, section 30a or section 30b of the Narcotics Act, or

5. a criminal offence pursuant to section 92a subsection (2) or section 92b of the Residence Act or pursuant to section 84 subsection (3) or section 84a of the Asylum Procedure Act

or, in cases in which the attempt is punishable, has attempted to perpetrate or participate in such offences or has prepared such offences by committing a criminal offence and if other means of establishing the facts or determining the accused's whereabouts offer no prospect of success or are considerably more difficult. The order may be made only against the accused or against persons in respect of whom it can be assumed, on the basis of particular facts, that they are receiving messages intended for the accused or receiving or transmitting messages from the accused or that the accused is using their connection.

Section 100b Order to Intercept Telecommunications

(1) The interception and recording of telecommunications (section 100a) may be ordered only by a judge. In exigent circumstances, the order may also be given by the public prosecution office. The order of the public prosecution office shall become ineffective if it is not confirmed by the judge within three days.

(2) The order shall be given in writing. It must indicate the name and address of the person against whom it is directed as well as the telephone number or other identification of the person's telecommunications access line. The type, extent and time of the measures shall be specified in the order. The order shall be limited to a maximum duration of three months. An extension of not more than three months shall be admissible if the prerequisites designated under section 100a continue to exist.

(3) On the basis of this order all persons providing, or collaborating in the provision of, telecommunications services on a commercial basis shall enable the judge, the public prosecution office and officials assisting it working in the police force (section 152 of the Courts Constitution Act) to intercept and record telephone calls. Whether and to what extent measures are to be taken in this respect shall follow from section 88 of the Telecommunications Act and from the Ordinance issued thereunder for the technical and organisational implementation of interception measures. Section 95 subsection (2) shall apply *mutatis mutandis*.

(4) If the prerequisites provided under section 100a no longer prevail, the measures resulting from the order shall be terminated without delay. The judge and the person bound by subsection (3) shall be informed of the termination.

(5) The personal information obtained by the measure may be used as evidence in other criminal proceedings only insofar as during its evaluation information was obtained which is required to clear up one of the criminal offences listed in Section 100a.

(6) If the records obtained by the measures are no longer required for criminal prosecution purposes, they shall be destroyed without delay under the control of the public prosecution office. The destruction shall be recorded in writing.

Section 100g

(1) If certain facts substantiate the suspicion that a person, as a perpetrator, inciter or accessory, or using terminal equipment (section 3, number 3, of the Telecommunications Act), has committed a criminal offence of substantial significance, particularly one of the offences referred to in section 100a, first sentence, or, in cases where an attempt is punishable, has attempted to perpetrate or participate in such offences or has prepared such offences by committing a criminal offence, an order may be made to the effect that commercial providers of telecommunications services or those who are involved in the provision of such services shall, without delay, give information on the telecommunications traffic data referred to in subsection (3) to the extent that the information is necessary for the investigation. This shall only apply insofar as such traffic data concern the accused or the other persons referred to in Section 100a, second sentence. The order may also be made in respect of information concerning future telecommunications traffic.

(2) An order may only be made for the provision of information on whether telecommunications traffic has been established from a telecommunications access line to the persons referred to in subsection (1), second sentence, if other means of establishing the facts or determining the accused's whereabouts offer no prospect of success or are considerably more difficult.

(3) Telecommunications traffic data shall be:

1. in the case of a connection, authorisation codes, personal access numbers, identifications of position as well as the subscriber number or the identification of the calling and called access line or the terminal equipment,

2. the beginning and the end of the connection according to the date and the time of day,

3. telecommunication services used by the customer,

4. termination points of non-switched connections, their beginning and their end according to the date and the time of day.

Section 100g (draft law)

(1) If certain facts substantiate the suspicion that a person, as a perpetrator, inciter or accessory
1. has committed, even in a single case, a criminal offence of substantial significance, particularly one of the offences specified in section 100a subsection (2), has attempted to commit a criminal offence in cases where an attempt is punishable, or has prepared a criminal offence by committing a criminal offence or
2. has committed a criminal offence through the use of telecommunications,
traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be collected without the knowledge of the person concerned, to the extent that this is necessary for ascertaining the facts or for determining the whereabouts of the accused. In cases under the first sentence number 2, the measure shall be admissible only where other means of ascertaining the facts or determining the whereabouts of the accused offer no prospect of success and where the collection of such data is proportionate to the significance of the case. The collection of location data in real time is permitted only in cases where the first sentence number 1 applies.

(2) Section 100a subsection (3) and section 100b subsections (1) to (4), first sentence, shall apply accordingly. In derogation of section 100b subsection (2), second sentence number 2, in the case of a criminal offence of substantial significance, a sufficiently precise designation of the locality and time of the telecommunication shall suffice if other means of ascertaining the facts would offer no prospect of success or be considerably more difficult.

(3) If the traffic data are not collected from a telecommunications service provider, such collection shall, following the conclusion of the communication activity, be determined pursuant to general provisions.

(4) In accordance with section 100b subsection (5), an annual overview of measures conducted pursuant to subsection (1) shall be compiled which contains the following information:
1. the number of cases in which measures were conducted pursuant to subsection (1);
2. the number of orders to conduct measures pursuant to subsection (1), differentiated according to initial orders and extension orders;
3. the criminal offence that occasioned the respective order, differentiated according to subsection (1), first sentence, numbers 1 and 2;
4. the number of past months for which traffic data were retrieved pursuant to subsection (1), starting from the time the order was issued;
5. the number of measures that produced no results because the requested data were not available either in whole or in part.

Section 100h

(1) The order must contain the name and the address of the person against whom the order is directed, as well as the subscriber number or other identification of his telecommunications access line. In the case of a criminal offence of substantial significance it shall be sufficient if there is adequate designation of the locality and time of the telecommunication, in regard to which the information is to be provided, if other means of establishing the facts would offer no prospect of success or be much more difficult. Section 100b subsection (1) and subsection (2), first and third sentences, subsection (6) and section 95 subsection (2) shall apply *mutatis mutandis*; section 100b subsection (2), fourth and fifth sentences, and subsection (4) shall also apply *mutatis mutandis* in the case of an order for information on future telecommunications traffic.

(2) Where the right of refusal to testify applies in the cases referred to under section 53 subsection (1), numbers 1, 2 and 4, a request for information on telecommunications traffic established by or with the person entitled to refuse to testify shall be inadmissible; any information acquired nonetheless shall not be used. This shall not apply if the person

entitled to refuse to testify is suspected of incitement, accessoryship, obstruction of justice or handling stolen goods.

(3) The personal data obtained from the information provided may be used for the purposes of evidence in other criminal proceedings only insofar as during their evaluation information emerges which is required to clear up a criminal offence referred to in section 100g subsection (1), first sentence, or if the accused gives his consent thereto.

Section 102 Search in Respect of the Suspect

A body search, a search of the property and of the private and other premises of a person who, as a perpetrator or as an inciter or accessory before the fact, is suspected of committing a criminal offence, or is suspected of accessoryship after the fact or of obstruction of justice or of handling stolen goods, may be made for the purpose of his apprehension and in cases where it may be presumed that the search will lead to the discovery of evidence.

Section 103 Searches in Respect of Other Persons

(1) Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to pursue the traces of a criminal offence or to seize certain objects, and only if facts are present which support the conclusion that the person, trace, or object looked for is in the premises which are to be searched. For the purpose of apprehending an accused who is strongly suspected of having committed an offence pursuant to section 129a of the Criminal Code, or one of the offences designated in this provision, a search of private and other premises shall also be admissible if they are in a building where, on the basis of certain facts, the accused is presumed to be.

(2) The restrictions of subsection 1, first sentence, do not apply to premises where the accused was apprehended or which he entered during the pursuit.

Section 105 Search Order; Execution

(1) Searches shall be ordered by the judge only and, in exigent circumstances, also by the public prosecution office and officials assisting it (section 152, Courts Constitution Act). Searches pursuant to Section 103 subsection 1, second sentence, shall be ordered by the judge; the public prosecution office shall be authorised to order searches in exigent circumstances.

(2) A municipal official or two members of the community in the district where the search is made shall be called in, if possible, to assist, if private premises, business premises, or fenced-in property are to be searched without the judge or the public prosecutor being present. The persons called in as members of the community shall not be police officers or officials assisting the public prosecution office.

(3) If it is necessary to make a search in an official building or in an installation or establishment of the Federal Armed Forces which is not open to the general public, the superior authority of the Federal Armed Forces shall be requested to carry out such search. The requesting authority shall be entitled to participate. No such request shall be necessary if the search is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 110 Examination of Papers (draft law)

(1) The public prosecution office shall have the authority to examine the papers of the person with respect to whom the search was conducted (section 152 of the Courts Constitution Act).

(2) Otherwise, officials shall be authorised to examine found papers only if the holder approves such examination. In all other cases they shall deliver any papers, the examination of which they deem necessary, to the public prosecution office in an envelope that shall be sealed with the official seal in the presence of the holder.

(3) The examination of electronic storage media may be extended to storage media in separate locations, to which storage media the person with respect to whom the search was conducted is authorised to provide access. Data that could be of significance for the investigation may be stored if there is concern that such data may be lost prior to the securing of the data carrier; such data shall be deleted as soon as they are no longer required for criminal prosecution purposes.

Section 161 Information and Investigations

(1) For the purpose indicated in section 160 subsections (1) to (3), the public prosecution office shall be entitled to request information from all authorities and to make investigations of any kind, either itself or through the authorities and officials in the police force, provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with the request or order of the public prosecution office, and they shall be entitled in this case to request information from all authorities.

(2) Where personal information has been obtained as a result of a measure taken under police law, corresponding to the measure pursuant to section 98a, it may be used as evidence only insofar as during its evaluation information was obtained which is required to clear up one of the criminal offences listed in Section 98a subsection (1). The first sentence shall apply *mutatis mutandis* so far as measures taken under police law correspond to the measures referred to in section 100c subsection (1), number 2, and in section 110a.

(3) Personal information obtained in or from private premises by technical means for the purpose of personal protection in a clandestine investigation based on police law may be used as evidence where the offence concerned is murder or manslaughter (sections 211 and 212 of the Criminal Code), kidnapping for extortion or hostage taking (sections 239a and 239b of the Criminal Code), an assault on air and sea traffic (section 316c of the Criminal Code), or one of the offences pursuant to the Narcotics Act and referred to in section 100a, first sentence, number 4. Such use shall only be admissible after determination of its lawfulness by the presiding judge of a penal chamber of the Regional Court in whose district the authority making the order is located.

Section 163 Duties of the Police

(1) The authorities and officials in the police force shall investigate criminal offences and shall take all measures where there should be no delay, in order to prevent concealment of facts. To this end they shall be entitled to request all authorities for information, and in exigent circumstances to demand such information, and they shall be entitled to conduct investigations of any kind unless there are other statutory provisions specifically regulating their powers.

(2) The authorities and officials in the police force shall transmit, without delay, their records to the public prosecution office. Direct transmission to the Local Court shall be possible if it appears that a judicial investigation needs to be performed promptly.

E. Telecommunications Act (*Telekommunikationsgesetz*, TKG)

Section 89 Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy

Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others. Section 88 subsection (4) applies accordingly. The interception and forwarding of communications on the basis of special legal authorisation remain unaffected.

Section 112 Automated Information Procedure

(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111 subsection (1), first and third

sentences, and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111 subsection (1), third and fourth sentences, apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that

1. the Federal Network Agency can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.

The requesting authority is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice.

(2) Information from the customer data files pursuant to subsection (1) shall be provided to

1. the courts and criminal prosecution authorities;
2. federal and state police enforcement authorities for purposes of averting danger;
3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;
4. federal and state authorities for the protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service;
5. the emergency service centres pursuant to section 108 and the service centre for the maritime mobile emergency number 124124;
6. the Federal Financial Supervisory Authority; and
7. the Customs Administration authorities for the purposes set forth in section 2 subsection (1) of the Undeclared Work Act

via central inquiry offices, as stipulated in subsection (4), at all times, insofar as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures.

(3) The Federal Ministry of Economics and Technology shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, and with the consent of the German Bundesrat, a statutory order in which the following matters are regulated

1. the essential requirements in respect of the technical procedures for
   a) the transmission of requests to the Federal Network Agency;
   b) the retrieval of data by the Federal Network Agency from persons with obligations, including the data types to be used for the queries; and
   c) transmission by the Federal Network Agency to the requesting authorities of the data retrieved;
2. the security requirements to be observed; and
3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the statutory order,
   a) the minimum requirements in respect of the scope of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;
   b) the permitted number of hits to be transmitted to the requesting authority; and
   c) the requirements in respect of the erasure of data not needed.

In other respects, the statutory order may also restrict the query facility for the authorities referred to in subsection (2) numbers 5 to 7 to the extent that is required for such

authorities. The Federal Network Agency shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorised bodies and to be brought into line with the state of the art, where required, and published by the Federal Network Agency in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defect-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.

(4) At the request of the authorities referred to in subsection (2), the Federal Network Agency shall retrieve and transmit to the requesting authority the relevant data sets from the customer data files pursuant to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.

(5) The person with obligations according to subsection (1) shall make all such technical arrangements in his area of responsibility as are required for the provision of information under this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the statutory order and the technical directive pursuant to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.

Section 113 Manual Information Procedure

(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent authorities, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or regulatory offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Military Counterintelligence Service. The person with obligations pursuant to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request pursuant to section 161 subsection (1), first sentence, or section 163 subsection (1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8 subsection (1) of the Federal Act on the Protection of the Constitution, the corresponding provisions of legislation to protect the constitutions of the *Länder*, section 2 subsection (1) of the Federal Intelligence Service Act or section 4 subsection (1) of the Military Counterintelligence Service Act; such data shall not be transmitted to any other public or private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.

(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 23 of the Court Remuneration and Compensation Act, is determined by the statutory order referred to in section 110 subsection (9). Sentence 2 also applies in those cases in which,

under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure under section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or correctly under the automated information procedure under section 112.

Section 148 Penal Provisions

(1) Any person who,

1. in violation of section 89, first or second sentence, intercepts a communication or imparts to others the content of a communication or the fact of its reception; or
2. in violation of section 90 subsection (1), first sentence,

a) owns, or

b) manufactures, markets, imports or otherwise introduces in the area of application of this Act

transmitting equipment as referred to there,

shall be punished with imprisonment for not more than two years or a fine.

(2) Where action in the cases of subsection (1) number 2 letter b arises through negligence, the offender shall be punished with imprisonment for not more than one year or a fine.

F. Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, IRG)

Section 2 Principle

(1) A foreign national who is being prosecuted or who has been sentenced in a foreign country because of an act punishable there may be extradited to such foreign country at the request of the competent authorities for the purpose of prosecution or execution of a sentence given because of that act or because of the imposition of another penalty.

(2) A foreign national who has been sentenced in a foreign country because of an act punishable there may be extradited to another foreign country, which has taken over enforcement, at the request of the competent authorities of that country, for the purpose of executing the sentence imposed because of the act, or for the imposition of another penalty.

(3) Foreign nationals pursuant to this law shall be persons who are not German nationals pursuant to Article 116 (1) of the Basic Law.

Section 3 Extradition for the Purpose of Prosecution or Execution

(1) Extradition shall be admissible only if the act contains the elements of a criminal offence under German law or if, after analogous conversion of the facts, the act would under German law constitute an offence.

(2) Extradition for the purpose of prosecution shall be admissible only if the act is punishable under German law by a maximum of at least one year of imprisonment or if, after analogous conversion of the facts, the act would, under German law, be punishable by such a penalty.

(3) Extradition for the purpose of execution shall be admissible only if extradition for the purpose of prosecution because of the act would have been allowed and if a penalty involving imprisonment is to be executed. It shall further be granted on condition if it is to be expected that the period of imprisonment to be served, or the sum of the periods of imprisonment still to be served, is at least four months.

Section 59 Admissibility of Assistance

(1) At the request of a competent authority of a foreign state, other legal assistance in a criminal matter may be provided.

(2) Legal assistance within the meaning of subsection (1) shall be every type of aid given to foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by a governmental authority and whether the legal assistance is to

be provided by a court or by a governmental authority.

(3) Legal assistance may be provided only under circumstances under which German courts and governmental authorities could render legal assistance to each other.

Section 60 Rendering Assistance

If the governmental authority responsible for authorising legal assistance determines that the requirements for rendering legal assistance have been met, the governmental authority responsible for rendering the legal assistance shall be bound by such determination. Section 61 shall remain unaffected.

Section 61 Court Decision

(1) If a court decision that is responsible for rendering legal assistance considers that the requirements for rendering legal assistance have not been met, it shall give reasons for ist opinion and shall request a ruling by the Higher Regional Court. The Higher Regional Court shall also rule upon application of the public prosecution office at the Higher Regional Court, or in the case of section 66, upon application of a person claiming that his rights would be violated if assistance were rendered, whether the requirements for rendering legal assistance have been met. For such proceedings before the Higher Regional Court, sections 30 and 31 subsections (1), (2) and (4), sections 32 and 33 subsections (1), (2) and (4), section 38 subsection (4), second sentence, and section 40 subsection (1), as well as the provisions of Chapter 11, Vol. 1 of the Code of Criminal Procedure, with the exception of sections 140-143, shall apply accordingly. For any subsequent proceedings, section 42 shall apply accordingly.

(2) Jurisdiction ratione loci shall lie with the Higher Regional Court and the public prosecution office at the Higher Regional Court in whose district the legal assistance is to be or has been rendered. If acts of legal assistance are to be or have been carried out in the districts of different Higher Regional Courts, jurisdiction shall depend on which Higher Regional Court or, where no Higher Regional Court is yet involved in the case, which public prosecution office at a Higher Regional Court was first to deal with the case.

(3) The decision of the Higher Regional Court shall be binding on those courts and authorities which are responsible for rendering the legal assistance.

(4) Legal assistance may not be granted if the court has ruled that the requirements for rendering legal assistance have not been met.

Section 61a Transmission of Personal Data without Request

(1) Courts and public prosecution offices may transmit personal data from criminal proceedings to the public authorities of another state as well as to interstate and supranational authorities without request by the latter if

1. transmission without request to a German court or to a German public prosecution office would have been admissible,
2. there are facts which warrant the expectation that the transmission is necessary

a) in order to prepare a request by the receiving state for legal assistance for the purpose of prosecution or execution of a sentence for a crime that is punishable by a maximum of more than five years of imprisonment in the area of application of this law, and the conditions for granting assistance upon request would be met if such request were made, or

b) in the individual case, to avert a danger to the existence or security of the state, or to the life, limb or freedom of a person, or to property of significant value, maintenance of which is demanded by the public interest, or to prevent a crime as described under letter a), and

3. the public authority to which the data are transmitted is competent to implement appropriate measures pursuant to number 2.

If adequate data protection is ensured in the receiving state, number 2 letter a), first sentence, applies with the provision that a crime which is punishable by a maximum of more than five years of imprisonment at a place within the scope of application of this law is substituted by a crime of significant gravity.

(2) Transmission is to be conducted under the condition that

1. time limits pursuant to German law for deletion and for review of deletion of transmitted

data will be observed,
2. transmitted data will be used only for the purposes for which they were transferred, and
3. transmitted data will be deleted or corrected immediately upon information in accordance with subsection 4.

Section 62 Temporary Transfer to a Foreign Country for Foreign Proceedings

(1) A person who is held in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty within the territory to which this Act applies, may, on request by the competent authority of a foreign country, be temporarily transferred to that country to attend proceedings pending there to be examined as a witness, for the purpose of confrontation or for inspection by the court, if

1. after having been advised, he states that he consents and this is recorded by a judge,
2. it is not to be anticipated that the duration of deprivation of liberty will be extended or the purpose of the criminal proceedings will be prejudiced as a result of the transfer,
3. an assurance is given that during the period of his transfer, the person concerned will not be subjected to a penalty or other sanction or proceeded against by virtue of measures which could not also have been taken during his absence and that in the event of his release he may leave the requesting State, and
4. an assurance is given that the person concerned will be returned without delay following the taking of evidence unless this has been waived.

The consent (first sentence no. 1) cannot be revoked.

(2) The public prosecution office at the Higher Regional Court shall prepare and carry out the transfer. The public prosecution office at the Higher Regional Court in whose region the deprivation of liberty is being enforced shall have local jurisdiction.

(3) The period of deprivation of liberty served in the requesting State shall be deducted from the period of deprivation of liberty to be enforced within the territory to which this Act applies. Section 37 subsection (4) shall apply accordingly.

Section 63 Temporary Transfer from a Foreign Country for Foreign Proceedings

(1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by the competent authority of that country, be temporarily transferred to the territory within which this law applies to give evidence for proceedings pending in that country and, after the evidence has been taken, be returned. The person concerned shall be kept in detention to ensure his return.

(2) Detention shall be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information:

1. the person concerned,
2. the request for the taking of evidence in the presence of the person concerned and
3. the reason for detention.

(3) The decision concerning detention shall be taken by the judge responsible for rendering legal assistance or by the judge at the Local Court in whose district the authority responsible for rendering legal assistance is located. This decision is not open to appeal.

(4) Sections 27, 45 subsection (4) and 62 subsection (2), first sentence, shall apply accordingly.

Section 64 Transit of Witnesses

(1) A foreign national who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by a competent authority, be transported to a third state through the territory to which this law applies as a witness for examination, confrontation or inspection and be returned after the taking of evidence.

(2) The person concerned will be kept in detention to ensure secure transit. Sections 27, 30 subsection (1), 42, 44, 45 subsections (3) and (4), 47, 63 subsection (2) shall apply accordingly.

Section 65 Transit for Enforcement Purposes

The transit of a foreign national, for purposes of enforcing a sentence or other sanction, from the state in which he was sentenced through the territory to which this law applies to a foreign country that has taken over such enforcement, shall be governed by sections 43 subsections (2) to (4) and sections 44, 45 and 47 as appropriate, provided that the request may also be submitted by a competent authority of the state in which the judgment was issued.

Section 66. Surrender of objects

(1) Upon request by the competent authority of a foreign country, objects may be surrendered

1. which may serve as evidence for foreign proceedings or
2. which the person concerned or a participant acquired as a result of the offence on which the request is based or as consideration for such objects.

(2) Surrender shall be admissible only if

1. the act giving rise to the request constitutes an unlawful act also under German law which fulfils the elements of an offence contained in a penal act or an act which permits punishment by non-criminal fine, or if it would constitute such an act also under German law if the facts were transposed to an analogous context,
2. a seizure order issued by a competent authority of the requesting state has been submitted or such an authority has made a declaration stating that the requirements for seizure would be fulfilled if the objects were located in the requesting state, and
3. an assurance is given that the rights of third parties will remain unaffected and that objects surrendered subject to reservation will be returned immediately upon request.

(3) The public prosecution office at the Regional Court shall prepare the decision on surrender and carry out surrender once it has been authorised. The public prosecution office at the Regional Court in whose region the objects are located shall have local jurisdiction. Section 61 subsection (2), second sentence, shall apply accordingly.

Section 67 Search and seizure

(1) Objects that may become the subject of surrender to a foreign state may be seized or otherwise secured even prior to the receipt of the request for surrender. A search may also be conducted for this purpose.

(2) Subject to the conditions set forth in section 66 subsection (1) number 1 and subsection (2) number 1, objects may also be seized or otherwise secured if necessary for the execution of a request which is not directed toward the surrender of the objects. Subsection (1), second sentence, shall apply accordingly.

(3) The search and seizure shall be ordered by the Local Court in whose district the actions are to be conducted. Section 61 subsection (2), second sentence, shall apply accordingly.

(4) In case of imminent danger, the public prosecution office and its investigative personnel (section 152 of the Courts Constitution Act) shall be authorised to order the search and seizure.

Section 68 Return

(1) A person sought who, on request and subject to his subsequent return, has been temporarily extradited to face criminal proceedings brought against him within the territory to which this law applies, shall be returned to the requested state at the agreed time unless that state waives his return. The public prosecution office involved in the criminal proceedings referred to in the first sentence shall be responsible for ordering and effecting the return of the person sought.

(2) If the return of the person sought would not otherwise be guaranteed, his detention may be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information:

1. the person sought,
2. the state to which the person sought is to be returned, and
3. the reasons justifying the order for detention.

(3) The decision concerning detention shall be taken by the respective court competent for ordering measures involving deprivation of liberty in the criminal proceedings referred to in subsection (1), first sentence. The decision shall not be open to appeal.

(4) Sections 18, 19, 24, 25, 27 and 45 subsection (4) shall apply accordingly.

Section 69 Temporary Transfer from a Foreign Country for German Proceedings

(1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty and who, on request, has been temporarily transferred to a German court or German authority for examination, confrontation or inspection shall, during his stay in the territory to which this law applies, be held in detention in order to ensure his return to that country.

(2) The decision concerning detention shall be taken by the court seised with the case and, in respect of preparatory proceedings, by the judge at the Local Court in whose district the public prosecution office conducting the proceedings is located. The decision is not open to appeal.

(3) Sections 27 and 45 subsection (4), section 62 subsection (2), first sentence and section 63 subsection (2) shall apply accordingly.

Section 83j Transmission of Data without Request

(1) To the extent provided by an international agreement, personal data that substantiate the suspicion that a criminal offence has been committed may be transmitted by public authorities to the public authorities of another European Union Member State as well as to organs and institutions of the European Communities, without request, provided that

1. a transmission, without request, to a German court or German public prosecution office would also be admissible and
2. the transmission is suited for
a) the institution of criminal proceedings in that other Member State or
b) the furthering of criminal proceedings already instituted in that Member State, and
3. the authority to which the data are transmitted is competent to undertake the measures under number 2.

(2) section 61a subsections (2) to (4) shall apply accordingly.

7.4 Country profile on cybercrime legislation – Romania

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Project on Cybercrime
www.coe.int/cybercrime

Provisional (13 April 2007)

Cybercrime legislation – country profile

Romania

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

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

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

Country:	**Romania**
Signature of Convention:	Yes: 23.11.2001
Ratification/accession:	Yes: 12.05.2004
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	ART.35 (1) of Romania Law no 161/2003
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	ART.42 of Romania Law no 161/2003
Article 3 – Illegal interception	ART.43 of Romania Law no 161/2003
Article 4 – Data interference	ART.44 of Romania Law no 161/2003
Article 5 – System interference	ART.45 of Romania Law no 161/2003
Article 6 – Misuse of devices	ART.46 of Romania Law no 161/2003

Article 7 – Computer-related forgery	ART.48 of Romania Law no 161/2003
Article 8 – Computer-related fraud	ART.49 of Romania Law no 161/2003
Article 9 – Offences related to child pornography	ART.51(1) of Romania Law no 161/2003
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	ART. 139^{8} - 139^{9} and art. 143 of Law on copyright no.8/1996
Article 11 – Attempt and aiding or abetting	For art.11(2) of Convention on Cybercrime - ART.50 and ART.51(2) of Romania Law no 161/2003
Article 12 – Corporate liability	ART. 19^{1} of Criminal Code (amended by Law no 278/2006)
Article 13 – Sanctions and measures	For art. 13(1) of Convention on Cybercrime - ART. 42-46, ART.48-49 and ART. 51 of Romania Law no 161/2003 For art. 13(2) of Convention on Cybercrime – ART. 53^{1} of Criminal Code (amended by Law no 278/2006)
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	ART. 58 of Romania Law no 161/2003
Article 15 – Conditions and safeguards	ART. 26 (1), 27 (3), 28 of Romania Constitution, ART. 91^{1} Criminal procedure Code, ART. 57 (1), (2) of Romania Law no 161/2003, ART. 3 (3), (5) of Romania Law no 365/2002 on electronic commerce (amended by Law no 121/2006)
Article 16 – Expedited preservation of stored computer data	ART.54 of Romania Law no 161/2003
Article 17 – Expedited preservation and partial disclosure of traffic data	ART.54 of Romania Law no 161/2003
Article 18 – Production order	ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences
Article 19 – Search and seizure of stored computer data	For art. 19 (3) of Convention on Cybercrime - ART. 96 and Art.99 of Criminal procedure Code. For art.19 (1-2) of Convention on Cybercrime - ART.56 (1) (3) of Romania Law no 161/2003.
Article 20 – Real-time collection of traffic data	ART.54 of Romania Law no 161/2003
Article 21 – Interception of content data	ART.57 of Romania Law no 161/2003
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	ART. 3-4 and art.142-143 Criminal Code

Chapter III – International co-operation	
Article 24 – Extradition	Art.23-24 (1) of Convention on cybercrime - ART.60 of Romania Law no 161/2003 and Title II of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 25 – General principles relating to mutual assistance	ART.61 of Romania Law no 161/2003
Article 26 – Spontaneous information	ART.66 of Romania Law no 161/2003 and ART. 166 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	Single article (2) b) of Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime
Article 28 – Confidentiality and limitation on use	ART. 12 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 29 – Expedited preservation of stored computer data	ART.63 of Romania Law no 161/2003
Article 30 – Expedited disclosure of preserved traffic data	ART.64 of Romania Law no 161/2003
Article 31 – Mutual assistance regarding accessing of stored computer data	ART. 60 of Romania Law no 161/2003
Article 32 – Trans-border access to stored computer data with consent or where publicly available	ART.65 of Romania Law no 161/2003
Article 33 – Mutual assistance in the real-time collection of traffic data	ART. 60 of Romania Law no 161/2003
Article 34 – Mutual assistance regarding the interception of content data	ART. 60 of Romania Law no 161/2003
Article 35 – 24/7 Network	ART.62 of Romania Law no 161/2003
Article 42 – Reservations	*[copied from the CoE treaty database]* **Declaration contained in the instrument of ratification deposited on 12 May 2004 - Or. Engl.** In accordance with Article 24, paragraph 7.a, of the Convention, Romania declares that the central authority responsible for making or receiving requests for extradition or provisional arrest is the Ministry of Justice (address: Str. Apollodor nr. 17, sector 5, Bucuresti). **Period covered: 1/9/2004 -**

	The preceding statement concerns Article(s) : 24 **Declaration contained in the instrument of ratification deposited on 12 May 2004 - Or. Engl.** In accordance with Article 27, paragraph 2.c, of the Convention, Romania declares that the central authorities responsible for sending and answering requests for mutual assistance are : a) the Prosecutor's Office to the High Court of Cassation and Justice for the requests of judicial assistance formulated in pre-trial investigation (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti); b) the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment. **Period covered: 1/9/2004 -** The preceding statement concerns Article(s) : 27 **Declaration contained in the instrument of ratification deposited on 12 May 2004 - Or. Engl.** In accordance with Article 35, paragraph 1, of the Convention, Romania declares that the point of contact designated to ensure the immediate and permanent international co-operation in the field of combating cybercrime is the Service of Combating Cybercrime within the Section for Combating Organised Crime and Drugs Trafficking to the High Court of Cassation and Justice (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti). **Period covered: 1/9/2004 -** The preceding statement concerns Article(s) : 35

Appendix 1: Solutions in national legislation

Romania Law no 161/2003

Title III on preventing and fighting cybercrime[226]

Chapter I

General Provisions

Art. 34 – The present title regulates the prevention and fighting of cybercrime by specific measures to prevent, discover and sanction the infringements through the computer systems, providing the observance of the human rights and the protection of personal data.

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 at item 1 and for the users of the services offered by these;

f) *„traffic data"* are any computer data related to a communication achieved through a computer system and its products, representing a part of the communication chain, indicating the communication 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;

---

[226] The cybercrime related provisions are incorporated in Title III of the Anticorruption Law no 161/2003 published in the Official Gazette no 279 from 21 April 2003

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 explicit behaviour or an adult person presented as a minor with an explicit sexual explicit behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual explicit 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 qualified 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.

Chapter II

Prevention of cybercrime

Art. 36 – In order to ensure the security of the computer systems and the protection of the personal data, the authorities and public institutions with competence in the domain, the service providers, the non-governmental organisations and other representatives of the civil society carry out common activities and programs for the prevention of cybercrime.

Art. 37 – The authorities and public institutions with competence in the domain, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society promote policies, practices, measures, procedures and minimum standards for the security of the computer systems.

Art. 38 - The authorities and public institutions with competence in the area, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society organise informing campaigns on cybercrime and the risks the users of the computer systems.

Art. 39 – (1) The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department establish and permanent up-date a database on cybercrime.
(2) The National Institute of Criminology under the subordination of the Ministry of Justice carries out periodic studies in order to identify the causes determining and the conditions favouring the cybercrime.

Art. 40 - The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department carry out special training programs for the personnel with attributions in preventing and fighting cybercrime.

Art. 41 – The owners or administrators of computer systems for which access is forbidden or restricted to certain categories of users are obliged to warn the users on the legal access and use conditions, as well as on the legal consequences of access without right to these computer systems.

Chapter III

Crimes and contraventions

Section 1

Offences against the confidentiality and integrity of computer data and systems

Art. 42 – (1) The illegal access to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years.

(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. 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.

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.

Art. 45 – 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. 46 – (1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years.

a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45;
b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42 - 45;

2) The same penalty shall sanction the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45.

Art. 47 – The intent to commit the offences provided in Articles 42-43 shall be punished.

Section 2

Computer-related offences

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.

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.

Art. 50 – The intent to commit the offences provided in Articles 48 and 49 shall be punished.

Section 3

Child pornography through computer systems

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.

(2) The intent is punished.

Section 4

Contraventions

Art. 52 – The non-observance of the obligation stipulated by art. 41 is a contravention and shall be sanctioned by a fee between 5.000.000 lei and 50.000.000 lei.

Art. 53 – (1) Finding a contravention provided in art. 52 and the application of the sanction are performed by the personnel authorised for this purpose by the minister of communications and IT as well as by the specially authorised personnel within the Ministry of Interior.

(2) The provisions of Government Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments by Law no.180/2002 are applicable.

Chapter IV

Procedural provisions

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) is bound to immediately make available for the criminal investigation body 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. 55 – (1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, data regarding data traffic or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.

(2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.

(3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

Art.56 – (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.

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.58 – The provisions of this chapter are applicable to criminal investigations or during the trial for the offences stipulated in this title or any other offences committed by means of computer systems.

Art.59 – For the criminal offences stipulated in this title and any criminal offences committed by means of computer systems, in order to ensure the special seizure stipulated at art.118 of the Criminal Code it can be performed the prevention measures provided for by the Criminal Procedure Code.

Chapter V

International Cooperation

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 part 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.

Art.61 – (1) At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cybercrime.

(2) The common investigations referred to at paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities.

(3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation.

Art.62 - (1) In order to ensure an immediate and permanent international cooperation in the cybercrime area, within the Organised Crime Fighting and Anti-drug Section of the prosecutor's Office belonging to the Supreme Court, a service for combating cybercrime is established as a contact point permanently available.

(2) The Service for combating cybercrime has the following attributions:

a) provides specialised assistance and gives information on the Romanian legislation in the domain to similar contact points in other states;

b) orders the expeditious preservation of data as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority;

c) executes or facilitates the execution, according to the law, of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities.

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;

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.

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.

Art. 66 – The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.

Art.67 – Art.29 of Law no.365/2002 on e-commerce, published in the Official Journal of Romania, Part I, no.483 of May 7, 2002 is abrogated.

Constitution of Romania is available also in English on http://www.cdep.ro

The Romanian Copyright Law No.8/1996 (extract)

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.

THE CRIMINAL CODE amended by Law no 278/2006 (extract)

Conditions for the criminal liability of legal persons	ART. 19^1 Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence."
Types of penalties applicable to	ART. 53^1 The penalties are: main and complementary. The main penalty is a fine from RON 2.500 to RON 2.000.000.

legal persons	Complementary penalties are: a) dissolution of the legal person; b) suspension of the activity of the legal person for a period from 3 months to one year or suspension of that of the activities of the legal person which served in the perpetration of the offence, for a period from 3 months to 3 years; c) closing of working locations belonging to the legal person, for a period from 3 months to 3 years; d) prohibition to participate in public procurement for a period from one to 3 years; e) display or broadcasting of the sentencing judgement.

CRIMINAL PROCEDURE CODE (extract)
Section V[1]
Audio or video interception and recording

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.

Law no. 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.

CRIMINAL PROCEDURE CODE (extract)

Confiscation of objects and writings	**Art. 96 -** The criminal investigation body or the court must take away the objects or writings that may serve as means of evidence in the criminal trial.
Confiscation by force of objects or writings	**Art. 99 –** If the object or writing required is not delivered voluntarily, the criminal investigation body or the court order confiscation by force. During the trial, the order of confiscation by force of objects or writings is communicated to the prosecutor, who takes enforcement measures through the criminal investigation body.

THE CRIMINAL CODE (extract)

Criminal Law personality	**Art.4.** Criminal law shall apply to offences perpetrated outside the Romanian territory, if the perpetrator is a Romanian citizen or if he/she, while having no citizenship, domiciles in this country. Decisions of the Constitutional Court:
Territorial nature of Criminal Law	**Art.3.** Criminal Law shall apply to offences committed on Romanian territory.
Territory	**Art. 142.** The term "territory" in the phrases "Romanian territory" and "the territory of our country" means the surface of land and water that is comprised by the borders, with the subsoil and the aerial space, as well as the territorial sea with its soil, subsoil and aerial space.
Offence committed on the territory of our country	**Art. 143.** (1) "Offence committed on the territory of our country" means any offence committed on the territory shown in Art. 142 or on Romanian ships or aircraft. (2) An offence shall be deemed as committed on the territory of

	our country also when only an act of realisation was performed or only the result of the offence occurred on this territory or on Romanian ships or aircraft.

Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime

In accordance with Article 27, paragraph 2.c, of the Convention, Romania declares that the central authorities responsible for sending and answering requests for mutual assistance are:

a) the Prosecutor's Office to the High Court of Cassation and Justice for the requests of judicial assistance formulated in pre-trial investigation (address: Blvd. Libertatii nr. 12-14, sector 5, Bucharest);

b) the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment