Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

September 2009

Cybercrime legislation – country profile

SOCIALIST REPUBLIC of VIETNAM

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

Comments may be sent to:

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

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

Country:	**Socialist Republic of Vietman**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;	**Law on information technology (No. 67/2006/QH11)** **Article 4.- Interpretation of terms** 1. Information technology means a combination of scientific and technological methods and modern technical tools for the production, transmission, collection, processing, storage and exchange of digital information. 2. Digital information means information generated by the method of using digital signals. 3. Network environment means an environment in which information is supplied, transmitted,

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	collected, processed, stored and exchanged via information infrastructure. 4. Information infrastructure means a system of equipment in service of the production, transmission, collection, processing, storage and exchange of digital information, including telecommunications networks, the Internet, computer networks and databases. 5. Information technology application means the use of information technology in socio-economic, external, defense, security and other activities with a view to raising the productivity, quality and efficiency of these activities. 6. Information technology development means research and development activities relating to the process of production, transmission, collection, processing, storage and exchange of digital information; development of information technology human resources; development of the information technology industry and development of information technology services. 7. Digital gap means the difference in conditions and ability to use computer and information infrastructure to access sources of information and knowledge. 8. Venture investment in the information technology domain means investment in enterprises operating in such domain with prospect of bringing huge profits but also with high risks. 9. Information technology industry means a hi-tech econo-technical sector, which produces and supplies information technology products, including hardware and software products and digital information contents. 10. Hardware means complete digital equipment; component assemblies; components; parts of digital equipment, component assemblies or components. 11. Digital equipment means electronic, computer, telecommunications, transmission, radio-receiving and -transmitting equipment or other integrated equipment, which is used for the production, transmission, collection, processing, storage and exchange of digital information. 12. Software means a computer program which is described by a system of signs, codes or languages for controlling digital equipment to perform certain functions. 13. Source code means a pre-compilation product of a software, which is yet able to control digital equipment. 14. Computer language means a post-compilation product of a software, which is able to control digital equipment. 15. Spam means an email or a message sent to a recipient who does not wish or has no responsibility to receive it according to the provisions of law. 16. Computer virus means a computer program which can spread or cause malfunction of digital equipment, or which can copy, modify or delete information stored in digital equipment. 17. Website means a website or a collection of websites in the network environment in service of information supply and exchange. 18. Digitalization means the change of information of various types into digital information

Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Art. 226(a) of Penal Code of the Socialist Republic of Vietnam** **Article 226a. Illegally accessing others' computer networks, telecommunication networks, the internet or digital devices.** 1. Those who intentionally ignore warnings, access codes, firewalls, use of other's management position or by other means illegally access other's computer systems, telecommunication networks, the internet or digital devices in order to take over the control power; interfere with proper functioning of digital devices; steal, alter, destroy, falsify data or illegally use of services, shall be subject to a fine of between twenty million dong and two hundred million dong or a prison term of between one year and five years. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between three and seven years of imprisonment: a) In an organized manner; b) Abusing position and powers; c) Illegally gained a large amount of profit, d) Causing serious consequences; e) Dangerous recividism. 3. Committing the crime in one of the following circumstances, the offenders shall be sentenced between five and twelve years of imprisonment: a) Towards data of State secrecy, information system in service of national defense and security; b) Towards National Information Infrastructure, National Grid Operation Information System, Banking and Financial Information System, Traffic Control; c) Illegally gained a very large or particularly large amounts of profit; d) Causing very serious and particularly serious consequences. 4. The offenders may also be subject to a fine of between five million dong and fifty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years. **Article 226.- Illegally using information in computer networks** 1. Those who illegally use information in computer networks and computers as well as put information into computer networks in contravention of law provisions, causing serious consequences, who have already been disciplined, administratively sanctioned but continue to commit it, shall be subject to a fine of between five million dong and fifty million dong, non-custodial reform for up to three years or a prison term of between six months and three years. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced

	to between two and five years of imprisonment: a) In an organized manner; b) Causing very serious or particularly serious consequences. 3. The offenders may also be subject to a fine of between three million dong and thirty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Art. 125 "Transmitted by telecommunication means and computers" of Penal Code of the Socialist Republic of Vietnam** **Article 125- Infringement upon other persons privacy or safety of letters, telephone and/or telegraph** 1.Those who appropriate letters, telegrams, telex, facsimile or other documents transmitted by telecommunication means and computers or commit illegal acts of infringing upon the secrecy or safety of letters, telephone conversations or telegraphs of other persons and who have been disciplined or administratively sanctioned for such acts but continue to commit violations, shall be subject to warning, a fine of between one million and five million dong or non-custodial reform for up to one year. 2.Committing the crime in one of the following circumstances, the offenders shall be subject to non-custodial reform for one to two years or a prison term of between three months and two years: a) In an organized manner; b) Abusing their positions and/or powers; c) Committing the crime more than once; d) Causing serious consequences; e) Recidivism. 3. The offenders may also be subject to a fine of between two million and twenty million dong, to a ban from holding certain posts for one to five years.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Article 225. Obstructing or causing operation disorder of telecommunication networks, computer systems, the internet and digital devices** 1. Those who commit one of the following acts causing serious consequences, if not falling under the cases stipulated in Articles 224 and 226a of this Code, shall be subject to a fine of between 20 million dong and two hundred million dong or a prison term of between one and five years: **a) deletion, damage or alteration of software, data of digital devices without permission; or** **b) Illegal obstruction of data transmission of telecommunication networks, computer systems and of the internet, digital devices; or**

	c) Other acts which obstruct or cause disorder to the operation of telecommunication networks, computer systems, the internet, digital devices. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between three years and seven years of imprisonment: a) In an organized manner; b) Abusing management position of telecommunication networks, computer systems and of the internet; c) Causing very serious consequences. 3. Committing the crime in one of the following circumstances, the offenders shall be sentenced between five and twelve years of imprisonment: a) Towards data of State secrecy, information system in service of national defense and security; b) Towards National Information Infrastructure, National Grid Operation Information System, Banking and Financial Information System, Traffic Control System; c) Causing particularly serious consequences. 4. The offenders may also be subject to a fine of between five million dong and fifty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Art. 143(1 "Those who destroy or deliberately damage other persons' property…") of Penal Code of the Socialist Republic of Vietnam** **Article 224. Scattering viruses and informatic programs having harmful feature to computer systems, telecommunication networks, the internet and digital devices.** 1. Those who intentionally **scatter viruses and informatic programs having harmful feature to computer systems, telecommunication networks, the internet and digital devices causing serious consequences**, shall be subject to a fine of between 20 million dong and two hundred million dong or a prison term of between one year and five years. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between three years and seven years of imprisonment: a) In an organized manner; b) Causing very serious consequences; c) Dangerous recividism. 3. Committing the crime in one of the followings, the offenders shall be sentenced to between five years and twelve years of imprisonment: a) Towards data of State secrecy, information system in service of national defense and security; b) Towards National Information Infrastructure, National Grid Operation Information System, Banking and Financial Information System, Traffic Control System; c) Causing particularly serious consequences.

	4. The offenders may also be subject to a fine of between five million dong and fifty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years. **Article 225. Obstructing or causing operation disorder of telecommunication networks, computer systems, the internet and digital devices** 1. Those who commit one of the following acts causing serious consequences, if not falling under the cases stipulated in Articles 224 and 226a of this Code, shall be subject to a fine of between 20 million dong and two hundred million dong or a prison term of between one and five years: a) deletion, damage or alteration of sofwares, data of digital devices without permission; or b) Illegal obstruction of data transmission of telecommunication networks, computer systems and of the internet, digital devices; or c) **Other acts which obstruct or cause disorder to the operation of telecommunication networks, computer systems, the internet, digital devices.** 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between three years and seven years of imprisonment: a) In an organized manner; b) Abusing management position of telecommunication networks, computer systems and of the internet; c) Causing very serious consequences. 3. Committing the crime in one of the following circumstances, the offenders shall be sentenced between five and twelve years of imprisonment: a) Towards data of State secrecy, information system in service of national defense and security; b) Towards National Information Infrastructure, National Grid Operation Information System, Banking and Financial Information System, Traffic Control System; c) Causing particularly serious consequences. 4. The offenders may also be subject to a fine of between five million dong and fifty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of:	

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an	**Article 284.- Forgery in the course of employment** 1.Those who, for self-seeking or other personal motivation, abuse their positions and/or powers to commit one of the following acts, shall be sentenced to between one and five years of imprisonment: a) Amending or falsifying contents of papers, documents; b) Making and/or granting counterfeit papers; c) Forging signatures of persons with positions and powers. 2. Committing the offense in one of the following circumstances, the offenders shall be sentenced

intent to defraud, or similar dishonest intent, before criminal liability attaches.	to between three and ten years of imprisonment: a) In an organized manner; b) The offenders are persons responsible for making or granting the papers and/or documents; c) Committing the offense more than once; d) Causing serious consequences 3.Committing the crime and causing very serious consequences, the offenders shall be sentenced to between seven and fifteen years of imprisonment. 4. Committing the crime and causing particularly serious consequences, the offenders shall be sentenced to between twelve and twenty years of imprisonment. 5. The offenders shall also be banned from holding certain posts or doing certain jobs for one to five years, may be subject to a fine of between three million dong and thirty million dong.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**226b. Using of telecommunication networks, computer systems, the internet or digital devices for appropriation of property.** 1. Those who use computer systems, telecommunication network, internet or digital devices to conduct one of the following acts, shall be subject to a fine of between 10 million dong and one hundred million dong or a prison term of between one year and five years: a) Use of information on account and bank cards of individuals and organisations to appropriate or counterfeit bank cards to appropriate property of the card holders or for payment of goods purchase or services; b) Illegal access into bank account of individuals and organisations for appropriation of money; c) Fraud in electronic commerce, monatary dealing, credit fund mobilization, dealings and payment of shares over the internet or other kinds of fraud in order to appropriate property of individuals and organisations; d) Other acts to appropriate property of individuals and organisations. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between three and seven years of imprisonment: a) In an organized manner; b) Committing the crime more than once c) In a professional manner; d) Appropriating property valued between fifty million dong and under two hundred million dong; e) Causing serious consequences; f) Dangerous recividism. 3. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between seven and fifteen years of imprisonment: a) Appropriating property valued between two hundred million million dong and less than five hundred million dong;

	b) Causing very serious consequences; 4.Committing the crime in one of the following circumstances, the offenders shall be sentenced to between twelve and twenty years of imprisonment or life imprisonment: a) Appropriating property valued from five hundred million dong and above; b) Causing particularly serious consequences; 5.The offenders may also be subject to a fine of between five million dong and one hundred million dong, partial or whole confiscation of property, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however,	**Law on information technology** (No. 67/2006/QH11) ***Article 12.*- Prohibited acts** 1. Obstructing lawful activities or supporting illegal activities in information technology application and development; illegally obstructing the operation of the system of national domain-name servers; destroying the information infrastructure or destroying information in the network environment. 2. Supplying, exchanging, transmitting, storing or using digital information for the following purposes: a/ Opposing the State of the Socialist Republic of Vietnam or undermining the all-people unity bloc; b/ **Exciting violence, propagating wars of aggression; sowing hatred among nations and peoples, exciting obscene, depravation, crime, social evils or superstition; undermining the nation's fine traditions and customs;** c/ Revealing state secrets, military, security, economic, external relation or other secrets provided for by law; d/ Distorting, slandering, or offending the prestige of organizations or the honor, dignity or prestige of citizens; e/ Advertising for or propagating goods or services banned by law. 3. Infringing upon intellectual property rights in information technology activities; illegally producing or circulating information technology products; forging websites of other organizations or individuals; creating illegal links to domain names lawfully used by organizations or individuals. **Article 73.- Responsibility to protect children** 1. The State, society and schools have the following responsibilities: a/ To protect children against negative impacts of information in the network environment; b/ To take measures to prevent and combat information technology applications with violence-inciting or obscene contents.

require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	2. Families shall prevent children from accessing harmful information. 3. Competent state agencies shall take the following measures to prevent children from accessing harmful information in the network environment: a/ Building, and disseminating the use of, content filter; b/ Creating and disseminating tools to prevent children from accessing information harmful to them; c/ Guiding the establishment and management of websites exclusively for children with a view to promoting the establishment of websites with information contents suitable and not harmful to children; raising the capability to manage information contents in the network environment, which are suitable and not harmful to children. 4. Service providers shall take measures to prevent children from accessing harmful information in the network environment. 5. Information technology products and services with contents harmful to children must bear warning signs.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty,	**Article 131.- Infringement upon copyright** 1. Those who commit one of the following acts thus causing serious consequences or who have been administratively sanctioned for one of the acts stipulated in this Article or have been sentenced for such crime, not yet entitled to criminal record remission but repeat their violations, shall be subject to a fine of between two million and twenty million dong or non-custodial reform for up to two years: a) Appropriating the copyright of literary, art, scientific, journalistic works, audio tapes or disc, video tapes or disc; b) Wrongfully assuming authors? names on literary, art, scientific or journalistic works, audio tapes or disc, video tapes or disc; c) Illegally amending the contents of literary, art, scientific, journalistic works, programs on audio tapes or disc, video tapes or disc; d) Illegally announcing or disseminating literary, art, scientific or journalistic works, programs on audio tapes or disc, video tapes or disc. 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between six months and three years of imprisonment: a) In an organized manner; b) Committing the crime more than once; c) Causing very serious or particularly serious consequences. 3. The offenders may also be subject to a fine of between ten million and one hundred million

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.	dong, to a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years. **Law on information technology (No. 67/2006/QH11)** **Article 69.- Protection of intellectual property rights in the information technology domain** The protection of intellectual property rights in the information technology domain shall comply with the law on intellectual property and the following regulations: 1.Organizations and individuals that transmit information in the network environment may make a temporary copy of a protected work according to the technical requirements of information transmission and that temporary copy shall be stored in a period of time which is long enough for information transmission; 2.Lawful users of protected software may reproduce that software for standby storage and replacement of the damaged software without asking for permission or paying copyright royalties.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Article 20.- Complicity** 1. Complicity is where two or more persons intentionally commit a crime. 2. The organizers, executors, instigators and helpers are all accomplices. The executors are those who actually carry out the crimes. The organizers are those who mastermind, lead and direct the execution of crimes. The instigators are those who incite, induce and encourage other persons to commit crimes. The helpers are those who create spiritual or material conditions for the commission of crimes. 3. The organized commission of a crime is a form of complicity with close collusion among persons who jointly commit the crime. **Article 21.- Concealment of crimes** Any person who, though having not earlier promised anything, knows a crime has been committed and conceals the offender, traces and/or exhibits of the crime or commits the act of obstructing the detection, investigation and/or handling of the offender, shall bear penal liability for the concealment of crime as provided for by this Code. **Article 53.- Deciding penalties in cases of complicity** When deciding penalties for accomplices, the court shall take into account the nature of complicity and the nature and extent of involvement of each accomplice. Extenuating, aggravating or penal liability exemption circumstances of any accomplice shall only apply to such accomplice.

Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in	

this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of	**CRIMINAL PROCEDURE CODE** **Chapter II - FUNDAMENTAL PRINCIPLES**

human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to	

preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or	

any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data;	**Chapter XII SEARCH, FORFEITURE, SEIZURE, DISTRAINMENT OF PROPERTY** **Article 140.- Grounds for body search, search of residences, working places, premises, objects, correspondence, telegraphs, postal parcels and matters** 1.Body search, search of residences, working places and premises shall be conducted only when there are grounds to judge that on the bodies, in the residences, working places and/or premises of persons there are instruments and means of offense commission, objects and property acquired from offense commission or other objects and documents related to the cases. Search of residences, working places or premises shall also be conducted in case of necessity to detect wanted persons. 2.In case of necessity to collect documents and objects related to the cases, correspondence, telegraphs, postal parcels and matters may be searched. **Article 144.- Forfeiture of correspondence, telegraphs, postal parcels and matters at post offices** In case of necessity to forfeit correspondence, telegraphs, postal parcels and matters at post offices, the investigating bodies shall issue forfeiture warrants. These warrants must be approved by the procuracies of the same level before they are executed, except for cases where the execution thereof cannot be delayed, provided that the reasons therefor must be clearly stated in the minutes and the forfeiture, once completed, be immediately notified to the procuracies of the same level. Before effecting the forfeiture, the executors of forfeiture warrants must notify such to the persons in charge of the post offices concerned. The persons in charge of the post offices concerned must assist the executors of seizure warrants in fulfilling their tasks. The forfeiture of correspondence, telegraphs, postal parcels and matters must be witnessed by

c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	the representatives of the post offices, who shall sign for certification the minutes thereof. The forfeiture warrant-issuing bodies must notify the persons having the to be forfeited correspondence, telegraphs, postal parcels and/or matters of the forfeiture warrants. If such notification will impede the investigation, immediately after such impediment no longer exists, the forfeiture warrant-issuing bodies must make such notification. **Article 145.- Seizure of objects and documents during a search** While conducting search, investigators may seize objects which are exhibits as well as documents directly related to the cases. For objects falling into the categories banned from storage or circulation, they must be forfeited and immediately delivered to competent management bodies. In case of necessity to seal objects up, such sealing must be conducted in the presence of the owners of such objects or their families' representatives, the administration's representatives as well as witnesses. The seizure of objects and documents during a search must be recorded in a minutes. Seizure minutes must be made in four copies, one of which to be handed to the owner of the objects and/or documents, one to be put in the case files; one to be sent to the procuracy of the same level, and one to the agency managing the seized objects and/or documents.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that	

territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Section 3 – Jurisdiction	

Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Article 5.- The effect of the Penal Code on criminal acts committed in the territory of the Socialist Republic of Vietnam** 1. The Penal Code applies to all acts of criminal offenses committed in the territory of the Socialist Republic of Vietnam. 2. For foreigners who commit offense in the territory of the Socialist Republic of Vietnam but are entitled to diplomatic immunities or consular privileges and immunities under Vietnamese laws, international treaties which the Socialist Republic of Vietnam has signed or acceded to or the international practices, their criminal liabilities shall be settled through diplomatic channels. **Article 6.- The effect of the Penal Code on criminal acts committed outside the territory of the Socialist Republic of Vietnam** 1. Vietnamese citizens who commit offenses outside the territory of the Socialist Republic of Vietnam may be examined for penal liability in Vietnam according to this Code. This provision also applies to stateless persons who permanently reside in the Socialist Republic of Vietnam. 2. Foreigners who commit offenses outside the territory of the Socialist Republic of Vietnam may be examined for penal liability according to the Penal Code of Vietnam in circumstances provided for in the international treaties which the Socialist Republic of Vietnam has signed or acceded to.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an	**Chapter XXXVII - EXTRADITION AND TRANSFER OF DOSSIERS, DOCUMENTS AND EXHIBITS OF CASES** **Article 343.- Extradition in order to examine penal liability or execute judgments** Basing themselves on the international agreements which the Socialist Republic of Vietnam has signed or acceded to on the principle of reciprocity, the bodies with procedure-conducting competence of the Socialist Republic of Vietnam may: 1. Request the foreign authorities with corresponding competence to extradite persons who have committed criminal acts or convicted under legally valid judgments to the Socialist Republic of

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	Vietnam for being examined for penal liability or serving their penalties. 2. Extradite foreigners who have committed criminal acts or convicted under legally valid judgments, who are being in the territory of the Socialist Republic of Vietnam, to the requesting nations for being examined for penal liability or serving their penalties. **Article 344.- Refusal to extradite** 1. The bodies with procedure-conducting competence of the Socialist Republic of Vietnam may refuse to extradite persons in one of the following cases: a) The persons requested to be extradited are citizens of the Socialist Republic of Vietnam b) Under the provisions of the laws of the Socialist Republic of Vietnam, the persons requested to be extradited cannot be examined for penal liability or serve penalties as the statute of limitations therefor has expired or for other lawful reasons. c) The persons requested to be extradited for penal liability examination have been convicted by the courts of the Socialist Republic of Vietnam under legally valid judgements for the criminal acts stated in the extradition requests or the cases have been ceased under the provisions of this Code; d) The persons requested to be extradited are residing in Vietnam for reasons of being possibly ill-treated in the extradition-requesting countries on the grounds of racial discrimination, religion, nationality, ethnicity, social status or political views. 2. The bodies with procedure-conducting competence of the Socialist Republic of Vietnam may refuse to extradite in one of the following cases: a) Under the criminal legislation of the Socialist Republic of Vietnam, the acts taken by the persons requested to be extradited do not constitute offenses; b) The persons requested to be extradited are being examined for penal liability in Vietnam for the acts stated in the extradition requests. 3. The bodies with procedure-conducting competence of the Socialist Republic of Vietnam which refuse to extradite under the provisions of Clause 1 and Clause 2 of this Article shall have to notify such to the foreign authorities with corresponding competence, which have sent the extradition requests. **Article 33. Extraditable offenses** 1. Extraditable offences are offences punishable under the criminal laws of both Vietnam and the requesting state in force at the time of extradition by imprisonment for a period of at least one year, for life imprisonment, or for death, or has been sentenced by the court of the requesting State to imprisonment and the remaining term of imprisonment to be served is at least six months. 2. It shall not matter whether the laws of both Vietnam and the requesting state place the

of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	conduct referred to in paragraph 1 of this Article within the same category of offense or denominate the offense by the same terminology; 3. Where the offence referred to in paragraph 1 of this Article has been committed outside the territory of the requesting state, extradition shall be granted if it is a criminal offence under the Penal Code of Vietnam
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional	**Part Eight INTERNATIONAL COOPERATION** **Chapter XXXVI GENERAL PROVISIONS ON INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS** **Article 340.- Principles for international cooperation in criminal proceedings** International cooperation in criminal proceedings between the bodies with procedure-conducting competence of the Socialist Republic of Vietnam and foreign authorities with corresponding competence shall be effected on the principles of respect for each other's national independence, sovereignty and territorial integrity, non-intervention in each other's internal affairs, equality and mutual benefit, compliance with the Constitution of the Socialist Republic of Vietnam and fundamental principles of international laws. International cooperation in criminal proceedings shall be carried out in conformity with the international agreements which the Socialist Republic of Vietnam has signed or acceded to and the laws of the Socialist Republic of Vietnam. Where the Socialist Republic of Vietnam has not yet signed or acceded to relevant international agreements, the international cooperation in criminal proceedings shall be effected on the principle of reciprocity but in contravention of the laws of the Socialist Republic of Vietnam, international laws and international practices. **Article 341.- Provision of judicial assistance** When rendering judicial assistance, the bodies as well as persons with procedure-conducting competence of the Socialist Republic of Vietnam shall apply the provisions of relevant international agreements which the Socialist Republic of Vietnam has signed or acceded to and the provisions of this Code. **Article 342.- Refusal to implement judicial assistance requests** The bodies with procedure-conducting competence of the Socialist Republic of Vietnam may refuse to implement judicial assistance requests in criminal proceedings in one of the following cases: 1.Judicial assistance requests fail to comply with the international agreements which the Socialist Republic of Vietnam has signed or acceded to and the laws of the Socialist Republic of Vietnam; 2.The implementation of judicial assistance requests is detrimental to the national sovereignty,

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.	security or other important interests of the Socialist Republic of Vietnam. **Law No. 08/2007/QH12 on Mutual Legal Assistance** **Article 4. Principles on mutual legal assistance** 1.Mutual legal assistance shall be carried out on the principle of respect for each other's independence, sovereignty and national territorial integrity, non-intervention in each other's internal affairs, equality and mutual benefit in compliance with the Constitution and law of Vietnam, and international treaties to which Vietnam is a party. 2.In case Vietnam and the foreign state concerned has not yet signed or acceded to any international treaty concerning mutual legal assistance, the legal assistance shall be performed on the principle of reciprocity, provided that this does not contradict Vietnamese laws and in compliance with international law and practice.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists,	

unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The	

requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article	

shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and	

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data	

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects.	

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	