Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

First draft (8 June 2007)

Cybercrime legislation – country profile

Armenia

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:	**Armenia**
Signature of Convention:	23.11.2001
Ratification/accession:	12.10.2006
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"	
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	Article 251 of RA Criminal Code (access (penetration) into computer information system without permission) envisages a responsibility for illegal access. In accordance with point 1 of the mentioned article penetration into information stored in a computer system, network or on storage media, and part or the whole information system protected by law, without permission, committed with violation of the protection system and negligently caused change, copying, obliteration or isolation of information, or spoilage of computer equipment, computer system or other significant damage, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labor for 6 months to 1 year, or with imprisonment for the term of up to 2 years.
Article 3 – Illegal interception	In accordance with point 1 of the article 254 (Illegal appropriation of computer data) copying or appropriating in any other way, of computer data stored in the computer system, network or on storage

	media, interception of transmitted data by means of computer communication, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years. Point two of the above-mentioned article envisages that forcing the submission of data mentioned in part 1 of the Article stored in the computer system, network or on storage media, by threat of publicizing defamatory information concerning a person or his close relatives, facts which the aggrieved wishes to keep secret, or with a threat to use violence against the person or his relatives, or against the person who manages this information, with a threat to destroy or damage the property, is punished with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3, or with imprisonment for 2-5 years.
Article 4 – Data interference	Article 253 (Computer sabotage) defines that obliteration (sabotage) of computer data or software, isolation or making it unusable, spoilage of computer equipment or destruction of the computer system, network or on storage media, is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years. The same action: 1) accompanied with access (penetration) into a computer system or network without permission; 2) negligently caused grave consequences, is punished with correctional labor for the term of up to 2 years, or with imprisonment for the term of up to 4 years. The acts envisaged in part 1 or 2 of mentioned Article which willfully caused severe consequences are punished with imprisonment for 3-6 years.
Article 5 – System interference	See the answers of the article 4.
Article 6 – Misuse of devices	According to the Article 255 of the Code (Illegal appropriation of computer data) determines that manufacture of special hardware or software for the illegal penetration into a protected computer system or network for the purpose of sale, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years. Moreover, in accordance with article 256 (manufacture, use and dissemination of hazardous software) the development of computer software for the purpose of obliteration, isolation, changing of data stored in the computer system, network or on storage media, or for making changes in existing software, or developing software with special viruses, their use, or dissemination of storage media with such software, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years and a fine in the amount of 100 to 300 minimal salaries.
Article 7 – Computer-related forgery	Article 252 of the Criminal Code (change in computer information) envisages that change in information stored in a computer, computer

	system, network or on storage media, or entering obviously false information therein, in the absence of elements of property theft, or infliction of property damage by deception or abuse of confidence, which caused significant damage, is punished with a fine in the amount of 200 to 500 minimal salaries, or with correctional labor for the term of up to 1 year. The same action which was accompanied with access (penetration) into a computer system or network without permission is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3 months, or with imprisonment for the term of up to 2 years.
Article 8 – Computer-related fraud	See the answer to the article 7.
Article 9 – Offences related to child pornography	According to the Article 263 of the Code (Illegal dissemination of pornographic materials or items) forcing minors to get involved in creation of software, video or film materials, pictures or other items of pornographic nature, as well as presenting children's pornography through computer network, is punished with a fine in the amount of 400 to 800 minimal salaries, or with arrest for the term of up to 3 months, or with imprisonment for the term of up to 3 years.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	In accordance with article 158 of the Code (breach of copyright and adjacent rights) legal use of the object of copyright and adjacent rights or appropriation of authorship, if these actions caused large loss, is punished with a fine in the amount of 200 to 400 minimal salary, or with imprisonment for the term of up to 2 years. (By large loss, this Article means an amount exceeding 200 minimal salaries at the moment of crime committal)
Article 11 – Attempt and aiding or abetting	RA legislation envisages criminal responsibility for the attempt, the organizer, the abettor and the perpetrator of the crime. So, point 3 of the article 33 of the Criminal Code provides that the liability for attempts to commit a crime and the preparation for crime is under the same article of the Special Part of this Code as for complete crimes. In accordance with point two of the article 39 of the Code the organizer, the abettor and the perpetrator are subject to liability under the article which envisages the committed crime, except those cases when they were at the same time the co-perpetrators of the crime.
Article 12 – Corporate liability	Not Regulated yet.
Article 13 – Sanctions and measures	See sanctions on crimes envisaged in articles 2-11.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	The questions concerning the powers and procedures which are necessary for realization of specific criminal investigations or procedures mentioned in Article 14 of the Convention are regulated by Criminal Procedure Code of Republic of Armenia.

Article 15 – Conditions and safeguards	Republic of Armenia ensures that the establishment, implementation and application of the powers and procedures mentioned in Article 15 of the Convention are performed in compliance with conditions and safeguards provided for under its domestic law, which guarantee the adequate protection of human rights and liberties, including rights arising from International treaties acting with the participation of Republic of Armenia, in particular pursuant to obligations of RA undertaken under the Convention and the Protocol mentioned in that article.
Article 16 – Expedited preservation of stored computer data	The question of the point 1 of Article 16 is regulated by the law of the Republic of Armenia on freedom of information which regulates the relations connected with freedom of information, defines the powers of persons holding (possessing) information, as well as the procedures, ways and conditions to get information. Article 5 of the above-mentioned law defines that the recording, classification and maintenance of elaborated or delivered data on the part of the information holder is implemented as defined by the Government of the Republic of Armenia. Moreover point 2 of article 12 of the mentioned law envisages that as defined by the law, information holders are responsible to record, categorize and maintain information possessed. Point 2 of the above-mentioned article is regulated by Criminal Procedure Code of RA article 226 of which provides that when necessary to take articles and documents significant for the case, and provided it is known for sure where they find themselves and in whose possession, the investigator conducts seizure. The seizure of documents which contain state secrets is conducted only by permission of the prosecutor and in agreement with the administration of the given institution. No enterprise, institution or organization, no official or citizen has the right to refuse to give the investigator the articles, documents or their copies which we would demand. The point 3 of article 16 of the Convention also is regulated by the mentioned Code. The point one of the article 172 of the Code stipulates that during a criminal proceeding measures prescribed by law shall be taken to secure the confidentiality of the information which constitutes an official, commercial or any other secret protected by law.
Article 17 – Expedited preservation and partial disclosure of traffic data	As questions mentioned in articles 17-21 of the Convention are directly interconnected questions, we would like to provide the common information on them. Thus, according to the article 225 (Grounds for seizure) of the Criminal Procedure Code the investigator, having sufficient ground to suspect that in some premises or in some other place or in possession of some person, there are instruments of crime, articles and valuables acquired by criminal way, as well as other items or documents, which can be significant for the case, conducts a search in order to find and take the latter. Point one of the article 239 of the Code provides that when there are sufficient grounds to believe that there is probatory value data in the mail or other correspondence, mail, telegrams and other communications sent by the suspect or the accused or to them by other persons, the investigator can make a grounded decision to impose monitoring on the correspondence of these people. Point 3 of the same article stipulates that the correspondence which can be arrested, in particular, concerns the following items: letter, telegrams, radiograms, parcels, cases, post containers, transmissions, fax and e-mail massages. Moreover, in compliance with article 240 the investigator familiarizes the director of the post office, and when necessary, other

	employees of the given office, with the seizure decree, with subscription, and with participation of selected attested witnesses from the employees of the office, opens up and examines the correspondence. When revealing documents and items which can be significant for the case, the investigator seizes the appropriate articles or confines him self to copying them. Also, article 241 stipulates that if there are sufficient grounds to suspect that the telephone conversations of the suspect or the accused or the conversations conducted by other means of communications can contain significant information for the case, the court makes a decision to permit the supervision and recording of these conversations.
Article 18 – Production order	As above. See article 17.
Article 19 – Search and seizure of stored computer data	As above. See article 17.
Article 20 – Real-time collection of traffic data	As above. See article 17.
Article 21 – Interception of content data	As above. See article 17.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	Article 14 of Criminal Code of RA envisages that the person who committed a crime in the territory of the Republic of Armenia is subject to liability under the Criminal Code of the Republic of Armenia. The crime is considered committed in the territory of the Republic of Armenia when: 1) it started, continued or finished in the territory of the Republic of Armenia; 2) it was committed in complicity with the persons who committed crimes in other countries. In case of crimes committed in the territory of the Republic of Armenia and other states, the person's liability arises under the Criminal Code of the Republic of Armenia, if the person was subjected to criminal liability in the territory of the Republic of Armenia and unless an international treaty of the Republic of Armenia prescribes otherwise. The person who committed a crime on board of a ship or flying aircraft bearing the flag or the identification of the Republic of Armenia is subject to criminal liability, regardless of their whereabouts, under the Criminal Code of the Republic of Armenia, unless otherwise stipulated in an international treaty of the Republic of Armenia. Also subject to liability under the Criminal Code of the Republic of Armenia, is the person who committed a crime on board of a military ship or aircraft of the Republic of Armenia, regardless of their location. Point 1 of article 15 stipulates that the citizens of the Republic of Armenia who committed crime outside the territory of the Republic of

	Armenia, as well as stateless persons permanently residing in the Republic of Armenia, are subject to criminal liability under the Criminal Code of the Republic of Armenia, if the act committed by them is recognized as a crime in the legislation of the state where the crime was committed, and if they were not convicted in another state. When convicting the above mentioned persons, the punishment can not exceed the upper limit for punishment in the state where the crime was committed. Moreover, according to the point 5 of article 16 of the Code, in case of refusal to extradite the person who committed a crime, the prosecution for the crime committed in the territory of a foreign country is done in accordance with the legislation of the Republic of Armenia.
Chapter III – International co-operation	
Article 24 – Extradition	
Article 25 – General principles relating to mutual assistance	
Article 26 – Spontaneous information	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	
Article 28 – Confidentiality and limitation on use	
Article 29 – Expedited preservation of stored computer data	
Article 30 – Expedited disclosure of preserved traffic data	
Article 31 – Mutual assistance regarding accessing of stored computer data	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	
Article 33 – Mutual assistance in the real-time collection of traffic data	
Article 34 – Mutual assistance regarding the interception of content data	
Article 35 – 24/7 Network	
Article 42 – Reservations	