European Commission
Commission européenne

Council of Europe
Conseil de l'Europe

CyberCrime@IPA project
www.coe.int/cybercrime

Version June 2010

Cybercrime legislation – country profile

BOSNIA AND HERZEGOVINA

This profile has been prepared within the framework of the EU/COE Joint Project on Regional Cooperation against Cybercrime in South-eastern Europe 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:

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:	**Bosnia and Herzegovina**			
	State Level	**Federation of Bosnia and Herzegovina**	**Republika Srpska**	**Brčko District**
Signature of Convention:	09/02/2005			
Ratification/accession:	19/05/2006			
Provisions of the	**Corrresponding provisions/solutions in national legislation**			

Convention	(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"	**CPC BiH CHAPTER II - DEFINITION OF TERMS** **Article 20 - Basic Terms:** The term **"Computer system"** is any device or a group of mutually connected or linked devices, out of which one or more are automatically processing data on the basis of a programme, The term **"Computer data"** denotes any presentation of facts, information or concepts in a form suitable for processing in a computer system, including any programme that is able to cause the computer system to execute certain function. The term **"original"** refers to an actual writing, recording or similar counterpart intended to have the same effect by a person writing, recording or issuing it. An "original" of a photograph includes the negative or any copy there from. If data is stored on a computer or a similar automatic data processing device, any printout or other output readable by sight is considered an "original"; The term "**duplicate**" refers to a copy generated by copying the original or matrix, including enlargements and miniatures, or by		**LAW ON TELECOMMUNICATIONS** **ART. 2 Provider of a service:** Legal or natural person who provides services through the public telecommunication operator. **RS CC - Article 147** (23) A movable object shall also include to mean any manufactured or accumulated energy used for producing light, heat or movement, and telephone impulses as well as any registered information that is the result of electronically processed information (computer data or program).	

	mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques that accurately reproduce the original; The term **"telecommunication address"** means any telephone number, either landline or cellular, or e-mail or internet address held or used by a person.				
Chapter II – Measures to be taken at the national level Section 1 – Substantive criminal law					
Article 2 – Illegal access		**ART. 397 - Unauthorised Access to the Electronic Data Processing Protected System and Network** **(1) Whoever,** without authorisation, logs on the electronic data processing system or network, by violating the protective measures; (2) Whoever **uses a datum** obtained in the manner referred to in paragraph 1 of this Article;	**ART. 238 - Unauthorized Access to Protected Computer Data Base:** Whoever, without authorization, **accesses another's protected <u>computer database</u>** and alters, destroys, copies, uses, conceals, publish or enters his data or computer virus or in some other manner renders useless or unavailable another's **computer data or programs…** **Article 292d Unauthorised Access to Protected Computer, Computer Network,**	ART. 387 (2): "**enters <u>computer data</u> or programs without authorization"** ART. 391 (1): **"accesses a system or network** for electronic data processing by violating measures for protection without authorization".

		ART. 393 - Damaging Computer Data and Programs: (2) Whoever, despite the protective measures, accesses without authorisation the computer data or programs **or intercepts their transmission without authorisation.**	**Telecommunication network and Electronic Data Processing** (1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorisation, or accesses electronic data processing without authorisation, shall be punished by fine or imprisonment up to six months. (2) Whoever records or uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years. (3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three years. **Article 292e** **Unauthorised Use of Computer of Computer Network** (1) Whoever uses	

			computer services or computer network with intent to acquire unlawful material benefit for himself or another, shall be punished by fine or imprisonment up to three months. (2) Prosecution for the offence specified in paragraph 1 of this Article shall be instigated by private action.	
Article 3 – Illegal interception		**ART. 393 - Damaging Computer Data and Programs:** (2) Whoever, despite the protective measures, access without authorisation the computer data or programs or **intercepts their transmission** without authorisation.		**ART. 387 (2):** "enters computer data or programs without authorization, despite security measures, or who intercepts transfer thereof without authorization".
Article 4 – Data interference		**ART. 393(1) - Damaging Computer Data and Programs:** Whoever	**ART.238- Unauthorized Access to Protected Computer Data Base:** Whoever, without	**ART. 387(1):** "who damages, changes, deletes, destroys or otherwise makes useless or unavailable another person's computer information or programs"

		damages, alters, deletes, destroys or in some other way renders useless or unavailable computer data or computer programs of another**.**	authorization, **accesses another's protected <u>computer database</u>** and alters, destroys, copies, uses, conceals, publish or enters his data or computer virus or in some other manner renders useless or unavailable another's **computer data or programs…** **Article 292a** **Damaging Computer Data and Programs** (1) Whoever without authorisation deletes, alters, damages, conceals or otherwise makes unusable a computer datum or program, shall be punished by fine or imprisonment up to one year. (2) If the offence specified in paragraph 1 of this Article results in damages exceeding 10.000 KM, the offender shall be punished by imprisonment of three months to three years. (3) If the offence specified in paragraph 1 of this Article results in damages exceeding 30.000 KM, the offender shall be punished by imprisonment of three months to five years. (4) Equipment and	

			devices used for committing of the offence specified in paragraphs 1 and 2 of this Article, if they are property of offender, shall be seized. **Article 292b** **Computer Sabotage** Whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer datum or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, public services, institutions, enterprises or other entities, shall be punished by imprisonment of six months to five years.	
Article 5 – System interference		**ART. 398 - Computer sabotage:** Whoever enters, alters, deletes or conceals a		ART. 392: "who enters, changes, deletes or conceals computer information or program or in some other way interferes with a computer system, or destroys or damages devices for electronic data

		computer datum or program or in any other manner interferes in the computer system, or destroys or damages devices for the electronic data processing with an aim of **disabling or considerably disturbing the process of electronic data processing important** to the governmental bodies, public services, public institutions, business enterprises or other legal persons of special public interest, **and thereby causes damage exceeding 500.000 KM…** **ART. 393 - Damaging Computer Data and Programs:** (3) The punishment referred to in paragraph 2 of this Article shall be imposed on **whoever disables or renders more difficult the work or use of computer system,**		processing with the intention to **prevent or significantly obstruct the course of electronic data processing important** for governmental bodies, public services, public institutions, trading companies or other legal persons of special public importance

		computer data or programs or computer communication. **ART. 396 - Disturbing the Work of the Electronic Data Processing System and Network:** Whoever, **by an unauthorised access** to the electronic data processing system or network, causes the stoppage or disturbance of the work of such system or network.		
Article 6 – Misuse of devices	**CC BiH: Impermissible Use of Copyrights – ART. 243:** (3)… whomever, with an aim of **facilitating the unauthorized use** of the author's work or the performer's of art performance produces, imports, brings **across the state border, distributes, rents or allows to others the use and exploitation of any kind of equipment or device**	**Art. 393 (5) - Damaging Computer Data and Programs:** Whoever, <u>without authorisation</u>, manufactures, supplies, sells, possesses or makes available to another special devices, means, computer programs or computer data created for or adjusted for the perpetration of	**ART. 398 - Manufacturing and Purchasing Weapons and Items for the Purpose of Committing a Criminal Offence:** (3) The punishment referred to in Paragraph 2 of this Article shall be pronounced against a person who makes, purchases, sells or lends instructions or items that are to be used for accessing a computer system.	**ART. 387(4):** "who illicitly manufactures, purchases, sells, hold in possession, or makes available to another person special devices, computer programs or electronic data, made or adapted to commit the criminal offence from Paragraphs 1 through 3 of this Article".

	whose sole or main purpose is to facilitate the unauthorized removal or circumvention of any technical device or computer program that is used for protection of the author's and performer's of art rights against unauthorized use.	criminal offence referred to in paragraphs 1 through 3 of this Article. ART. 394 in paragraph 3 criminalizes the same act for computer forgery.	**Article 292v** **Creating and Introducing of Computer Viruses** (1) Whoever makes a computer virus with intent to introduce it into another's computer or computer network or telecomunication network, shall be punished by fine or imprisonment up to six months. (2) Whoever introduces a computer virus into another's computer or computer network thereby causing damage, shall be punished by fine or imprisonment up to two years. (3) Equipment and devices used for committing of the offence specified in paragraphs 1 and 2 of this Article shall be seized. **Article 292e** **Unauthorised Use of Computer of Computer Network** (1) Whoever uses computer services or computer network with intent to acquire unlawful material benefit for	

			himself or another, shall be punished by fine or imprisonment up to three months. (2) Prosecution for the offence specified in paragraph 1 of this Article shall be instigated by private action.	
Article 7 – Computer-related forgery		**ART. 394 (1) Electronic Forgery:"**Whoever, without authorisation, produces, enters, alters, deletes or renders useless **computer data** or programs that are of value for the legal relations, with an aim of using them as genuine, or uses such data or programs himself". **Covered.**	**Article 292g Computer Fraud** (1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another one unlawful material benefit and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years. (2) If the offence specified in paragraph 1 of this Article results in acquiring material benefit exceeding 10.000 KM, the offender shall be punished by imprisonment of one to eight years. (3) If the offence specified in paragraph 1 of this	**ART. 388 (1) Electronic Forgery:** "who illegally produces, enters, changes, deletes or makes useless **computer information** or programs relevant for legal affairs, with the intention to use such information or programs as valid or who uses himself such information or programs.

			Article results in acquiring material benefit exceeding 30.000 KM, the offender shall be punished by imprisonment of two to ten years. (4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months.	
Article 8 – Computer-related fraud		**Art. 395 (1) Computer Fraud:** "Whoever, without authorisation, enters, damages, alters or conceals computer datum or program or otherwise influences the result of the electronic data processing with an aim of acquiring unlawful material gain for himself or for another, and thus causes material damage to somebody else,	**ART. 271 - Unauthorized Entry into Computer System:** (1) Whoever **in the course of business activities,** without authorization, alters, deletes, publishes, conceals or destroys another's computer data or program in order to obtain unlawful property gain for himself or a third party or to cause damage to another,	**ART. 389 (1) Computer Fraud:** "who unlawfully enters, damages, changes or conceals computer information or program, or in some other way influences the output of electronic data processing, with the intention to acquire a property gain for himself or another and in that way causes a property damage to another,
Article 9 – Offences related to child pornography	**ART. 1 - CC** (10) A **child,** as referred to in this Code, is a person who has not	**ART. 230 Showing Obscene (Pornographic) Material**	**ART. 199 - Abuse of a Child or Juvenile for Pornography:** Article 199: Whoever	**ART. 208 Abuse of a Child or a Minor for Pornographic Purposes: "**who abuses a child or a minor for taking photographs, audio-visual material or

	reached fourteen years of age. (11) A **juvenile,** as referred to in this Code, is a person who has not reached eighteen years of age.		**photographs or films a child** with a view to developing photographs, audio-visual tapes or other pornographic materials or incites such persons to play in pornographic shows... **ART. 200 - Production and Screening Child Pornography:** Whoever **sells, shows or renders available through a public display or in any other way writings, pictures, audio-visual and other items containing child pornography or whoever produces, purchase, keeps or screens a child pornographic show for the same reasons..**. (2) If the offence referred to in Paragraph 1 is committed against a **minor who is under 16**, (3) If the offence referred to in preceding Paragraphs is committed **through the mass media or internet,** the perpetrator shall be punished by imprisonment for a term between six months and five years. (4)**Child pornography** in	other material with pornographic contents, or possesses, or imports, or sells, or distributes, or presents such material, or induces such persons to take part in a pornographic performance". **ART. 186 (3) Unauthorized Optical Recording:** "who photographs a child or a juvenile in order to develop photographs, audio and visual material or other articles containing pornographic elements, or possesses, imports, sells, distributes or presents such material ".

			terms of this provision shall be understood to mean any pornographic material that visually shows: (a) a child or a minor involved in an obvious sexual act, and (b) realistic photographs that show a child or a minor involved in an obvious sexual act. **Article 292g** **Computer Fraud** (1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another one unlawful material benefit and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years. (2) If the offence specified in paragraph 1 of this Article results in acquiring material benefit exceeding 10.000 KM, the offender shall be punished by	

			imprisonment of one to eight years. (3) If the offence specified in paragraph 1 of this Article results in acquiring material benefit exceeding 30.000 KM, the offender shall be punished by imprisonment of two to ten years. (4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months.		
Title 4 – Offences related to infringements of copyright and related rights					
Article 10 – Offences related to infringements of copyright and related rights	**CC BiH: Impermissible Use of Copyrights – ART. 243:** (1) Whoever, without the authorization of the author or other holder of copyright, or the person entitled to give authorization, where such authorization is required under the provisions of the law of Bosnia and Herzegovina, or contrary to their prohibition, **fixes on a**				

	material surface, reproduces, multiplies, distributes, rents, imports, brings across the state border, presents, performs, broadcasts, transmits, makes available to the public, translates, adapts, arranges, alters <u>or uses the in any other form the work of an author…</u> (2)… whomever, without the authorization of the performer of art or the person entitled to give authorization, where such authorization is required under the provisions of the law of Bosnia and Herzegovina, or, contrary to their prohibition, **records, reproduces, multiplies, distributes, rents, imports, brings across the state border, presents, performs, broadcasts, transmits, makes available to the public or uses his performance in another way.** **Law on copyright and related rights in**			

	Bosnia and Herzegovina			
Article 11 – Attempt and aiding or abetting	**CC BiH - ART. 29, ART. 30- 31**	**ART. 20, ART. 23-25**	**ART. 21, ART. 23- 25**	**ART. 28, ART. 31- 33**
Article 12 – Corporate liability	**CC BiH - ART. 122** (1) This Chapter regulates criminal liability of a legal person, with the exclusion of Bosnia and Herzegovina, the Federation of Bosnia and Herzegovina, the Republika Srpska, the Brčko District of Bosnia and Herzegovina, canton, city, municipality and local community, for a criminal offence perpetrated by the		**XIV LIABILITY OF LEGAL PERSONS FOR CRIMINAL OFFENCES**	**Chapter XIV- LIABILITY OF LEGAL PERSONS FOR CRIMINAL OFFENCES**

	perpetrator in the name of, for account of or in favour of the legal person.			
Article 13 – Sanctions and measures	CC BiH – ART. 131 - Punishment for Legal Persons: The following types of punishment may be imposed upon the legal persons: a) Fines; b) Seizure of property; c) Dissolution of the legal person.			
Section 2 – Procedural law				
Article 14 – Scope of procedural provisions				
Article 15 – Conditions and safeguards	**Constitution of Bosnia and Herzegovina** **Article II: Human Rights and Fundamental Freedoms:** 6. The right to private and family life, home, and correspondence.			
Article 16 – Expedited preservation of stored computer data	**CPC BiH - ART. 72a (1) Order to the telecommunication operator:** If there are grounds for suspicion that a person has committed a criminal			

	offence, on the basis of motion of the Prosecutor or officials authorized by Prosecutor, the Court may issue an order to a telecommunication operator or another legal person performing telecommunication services to turn over information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or be useful in collection of information that could be useful to the criminal proceedings.			
Article 17 – Expedited preservation and partial disclosure of traffic data				
Article 18 – Production order				
Article 19 – Search and seizure of stored computer data	**CPC BiH - ART. 51** (2) - **Search of dwellings, other premises and personal property -** Search of personal property pursuant to Paragraph (1) of this Article shall include a **search of the computer systems,**		**Chapter XV** **ACTIONS TO OBTAIN EVIDENCE** **1. Search of dwellings or other premises and persons** **Article 115** **Search of dwellings, other premises and personal property** (2) The search of personal property pursuant to Paragraph 1 of this article shall include a search of the computer and	**ART. 28 (1)** - **Search of dwellings, other premises and personal property -** Search of personal property pursuant to Paragraph 1 of this Article shall include a **search of the computer and similar devices** for automated

	devices for automated and electronic data processing and mobile phone devices. Persons using such devices shall be obligated to allow access to them**, to hand over the media with saved data, as well as to provide necessary information concerning the use of the devices.** A person, who refuses to do so, may be punished under the provision of Article 65 Paragraph (5) of this Code. **ART. 65 (4) -(6) - Order for Seizure of Objects** –The authorized official shall seize objects on the basis of the issued warrant. Anyone in possession of such objects must turn them over at the request of the preliminary proceedings judge. A person who refuses to surrender articles may be fined in an amount up to 50.000 KM, and may be imprisoned if he persists in his refusal… The provisions of Paragraph 5 of this Article shall also **apply to the data stored in**		similar devices for automatic data processing connected with it. At the request of the court, the person using such devices is obliged to allow access to them, to hand over diskettes and magnetic tapes or other forms of saved data, as well as to provide necessary information concerning the use of the devices. A person, who refuses to do so, without cause for reasons that are referred to in Article 148 of this Code, may be punished under the provision of Article 129 Paragraph 5 of this Code. (3) The search of computers and similar devices under paragraph 2 of this article shall be conducted by an information technology expert. **Article 129 (1) (5) (6) Warrant for Seizure of Objects:** "(1) Objects that are the subject of seizure pursuant to the Criminal Code or that may be used as evidence in the criminal proceedings shall be seized temporarily and their custody shall be secured pursuant to a court decision. (5)Anyone in possession of such objects must turn them over at the request of the preliminary proceedings judge. A person who refuses to surrender articles may be fined in an amount up to 50,000 KM, and may be imprisoned if he persists in his refusal… The same provisions shall apply to an official or responsible person in a state body or a legal entity. (6) The provisions of Paragraph 5 of this Article shall also apply to the data stored in devices for automated or electronic data processing. In obtaining such data, special	data processing connected with it. At the request of the Court, the persons using such devices shall be obligated to allow them access, **to hand over diskettes and magnetic tapes or some other forms of saved data**, **as well as to provide necessary information concerning the use of the devices**. A person who refuses to do so, although the reasons from Article 84 of this Law do not exist, may be punished under the provision of Article 65 Paragraph 5 of this Law. **Section 2 – TEMPORARY SEIZURE OF OBJECTS AND PROPERTY** **ART. (5)(6) -Order for Seizure of Objects:** Anyone in possession of such objects must turn them over upon the order of the Court. A person who refuses to hand out articles may be fined 50.000 KM, and may be imprisoned if he persists in his refusal…. The provisions of Paragraph 5 of this

	devices for automated or electronic data processing. In obtaining such data, special care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data.		care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data.	Article shall also **apply to the data stored in computers or similar devices for automated data processing.** In obtaining such data, special care shall be taken with respect to regulations on confidentiality of certain data.
Article 20 – Real-time collection of traffic data				
Article 21 – Interception of content data	**CPC BiH - ART. 116 - Types of Special Investigative Actions and Conditions of Their Application:** (1) If evidence cannot be obtained in another way or its obtaining would be accompanied by disproportional difficulties, special investigative measures may be ordered against a person against whom there are grounds for suspicion that he has committed or has along with other persons taken part in committing or is participating in the commission of an offense referred to in Article 117 of this Code.		**Article 226 Types of Special Investigative Actions and Conditions of Their Application:** (1) If evidence cannot be obtained in another way or its obtaining would be accompanied by disproportional difficulties, special investigative actions may be ordered against a person against whom there are grounds for suspicion that he has committed or has along with other persons taken part in committing or is participating in the commission of an offense referred to in Article 227 of this Code. (2) The investigative actions under Paragraph 1 of this Article are as follows: **a) surveillance and technical recording of telecommunications;** **b) access to the computer systems and computerized data processing;**	**ART. 116 - Types of Special Investigative Actions and Conditions for Their Taking:** If evidence cannot be obtained in another way or its obtaining would be accompanied by disproportionate difficulties, special investigative actions may be ordered against a person against whom there are grounds for suspicion that he has committed, along with other persons, taken part in committing or participated in the commission of an offense referred to in Article 117 of this Law.

	Measures referred to in Paragraph 1 of this Article are as follows: **- surveillance and technical recording of telecommunications;** **- access to the computer systems and computerized data processing;** ……			The investigative actions referred to in Paragraph 1 of this Article are as follows: **a) surveillance and technical recording of telecommunications;** **b) access to the computer systems and computerized data processing;** ……
Section 3 – Jurisdiction				
Article 22 – Jurisdiction				
Chapter III – International co-operation				
Article 24 – Extradition				
Article 25 – General principles relating to mutual assistance	**(Chapter XXX - PROCEDURE TO RENDER INTERNATIONAL LEGAL AID AND TO ENFORCE INTERNATIONAL AGREEMENTS IN CRIMINAL MATTERS of the Criminal Proceeding Code of**			

	Bosnia and Herzegovina) ART. 407 - General provisions: International aid in criminal matters shall be rendered under the provisions of this Code, **unless otherwise prescribed by the legislation of Bosnia and Herzegovina or an international agreement.**			
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	**Declaration transmitted by a communication from the Permanent Representation of Bosnia and Herzegovina, dated 6 August 2008, and confirmed by a letter from the Chargée d'Affaires a.i. of Bosnia and Herzegovina, dated 28 October 2008, registered at the Secretariat General on 29 October 2008 - Or. Fr.** **In accordance with Article 24, paragraph 7, Article 27, paragraph 2, and Article 35, paragraph 1, of the Convention on Cybercrime, Bosnia and Herzegovina designated as the competent authority for the purposes of the Convention : the State Investigation and Protection Agency of Bosnia and Herzegovina. The point of contact is Mr Jasmin GOGIC, Director of Sarajevo's regional office of the State Investigation and Protection Agency of Bosnia and Herzegovina** **Period covered: 29/10/2008 -** **The preceding statement concerns Article(s) : 24, 27, 35**			