Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Draft (25 March 2008)

Cybercrime legislation – country profile

Indonesia

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:	Indonesia	
Signature of Convention:	Yes:_____ (Date)	No: _____No._____
Ratification/accession:	Yes:_____ (Date)	No: _____No._____
	If not yet signed/acceded to: *What measure are being undertaken in your country to become a Party?* Indonesia has not ratified the convention. The House of Representative, however, approved the Law on Information and Electronic Transaction. The Law shall come into force soon. Basically this draft has implemented Convention on Cybercrime, UNCITRAL Model Law on Electronic Signatures, and UNCITRAL Model Law on Electronic Commerce. *What specific obstacles (legislative or other) prevent ratification/accession?* Approval from House of Representatives is required to ratify the Convention. Such approval requires particular process and sufficient time.	
Provisions of the Convention	***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*	
Chapter I – Use of terms		
Article 1 – "Computer system", "computer data", "service provider", "traffic	Implemented in the Draft. Computer System is defined from definition of Computer and Electronic System.	

data"	Computer means a tool to process electronic data, magnetic, optic, or system to process functions of logics, arithmetic, and storing. Electronic System means a set of electronic tools and procedures which function is to prepare, collect, process, analyse, store, present, publish, transmit and/or disseminate Electronic Information. Computer data and traffic data are defined from definition of Electronic Information and Electronic Document. Electronic Information means one or a set of electronic data, include but not limited in writing, sound, drawing, map, plan, picture, electronic data interchange, electronic mail, telegram, telex, telecopy or the like, letter, mark, access code, symbol, or perforation processed and such has meaning or can be understood by particular person. Electronic Document means every Electronic Information made, transmitted, sent, received, or stored on analog, digital, electromagnetic, optical, or the like, which can be seen, presented, and/or heard by means of Computer or Electronic System, include but not limited in writing, sound, picture, map, plan, photo or the like, letter, mark, number, Access Code, symbol, or perforation which has meaning or which can be understood by particular person. Service Provider definition is implemented in definition of Electronic Service Provider which means government, a Person, an Entity or a Community who provides Electronic System.
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	Indonesia has Criminal Code at national Level
Article 2 – Illegal access	Implemented in the Draft. Anyone commits illegal access by any mean to an electronic system without right shall be liable to a prison maximum 12 years and/or a fine maximum 800 million rupiah.
Article 3 – Illegal interception	Implemented in the Draft. Any person commits interception to Electronic Information and/or Electronic Document in a Computer and/or Electronic System without right shall be liable to a prison maximum 10 years and/or a fine maximum 800 million rupiah.
Article 4 – Data interference	Implemented in the Draft. Anyone commits intentionally the damaging, deletion, alteration, and/or transmission of Electronic Information and/or Electronic Document by any means without right shall be liable to a prison maximum 10 years and/or a fine maximum 5 billion rupiah.
Article 5 – System interference	Implemented in the Draft. Anyone commits any activity without right damaging or disfuctioning Electronic System shall be liable to a prison maximum 10 years and/or a fine maximum 10 billion rupiah.
Article 6 – Misuse of	Implemented in the Draft. Anyone commits without right produces,

devices	sales, procures, imports, distributes, facilitates, or possesses hardware or software of a computer designed primarily to facilitate criminal offence conducts (mentioned above) shall be liable to a prison maximum 10 years and/or a fine maximum 10 billion rupiah.
Article 7 – Computer-related forgery	Implemented in the Draft. Any person commits and without right or unlawfully manipulates, creates, alters, and/or deletes Electronic Information and/or Electronic Document resulting in inauthentic one shall be liable to a prison maximum 12 years and/or a fine maximum 12 billion rupiah.
Article 8 – Computer-related fraud	Implemented in the Draft. Anyone commits without right causing a loss to another person because any conducts mentioned before shall be liable to a prison maximum 12 years and/or a fine maximum 12 billion rupiah.
Article 9 – Offences related to child pornography	Implemented in the Draft. Anyone commits and without right distributes and/or transmits Electronic Information and/or Electronic Document related to child pornography or sexual exploitation shall be liable to a prison maximum 8 years and/or a fine maximum 1.3 billion rupiah.
Title 4 – Offences related to infringements of copyright and related rights	Implemented in the Draft. Utilization of Information concerning private data of a person through electronic media shall be based on his consent. Similar provision regulated on Indonesian Copy Right Law.
Article 10 – Offences related to infringements of copyright and related rights	no
Article 11 – Attempt and aiding or abetting	Provided on Indonesian Criminal Code.
Article 12 – Corporate liability	Implemented in the Draft. Criminal sanction for any criminal offence mentioned above conducted by a corporation shall be added 2/3 more of the basic sanction.
Article 13 – Sanctions and measures	Implemented in the draft. Sanctions and measures mentioned above.
Section 2 – Procedural law	Investigation of criminal offence mentioned above shall be conducted based on Indonesian Criminal Procedure Code and the provisions of the draft.
Article 14 – Scope of procedural provisions	Investigators are The Police of the Republic of Indonesia and Special Civil Servant responsible for Information Technology and Electronic Transaction thus responsible to investigate any criminal offence related to Information Technology and Electronic Transaction.
Article 15 – Conditions and safeguards	The Investigation shall take into account and/or consider protection of privacy, confidentiality, uninterrupted of public services, and data integrity pursuant to prevailing laws and regulations.
Article 16 – Expedited preservation of stored computer data	Confiscation and search warrant concerning criminal offence related to Information Technology and Electronic Transaction shall be conducted based on permission from head of district court.

	In conducting such confiscation and search warrant, investigator shall maintain and/keep the continuity of public services.
Article 17 – Expedited preservation and partial disclosure of traffic data	The Investigation shall take into account and/or consider protection of privacy, confidentiality, uninterrupted of public services, and data integrity pursuant to prevailing laws and regulations.
Article 18 – Production order	Confiscation and search warrant concerning criminal offence related to Information Technology and Electronic Transaction shall be conducted based on permission from head of district court.
Article 19 – Search and seizure of stored computer data	Confiscation and search warrant concerning criminal offence related to Information Technology and Electronic Transaction shall be conducted based on permission from head of district court.
Article 20 – Real-time collection of traffic data	no
Article 21 – Interception of content data	Interception requested by Police, Prosecutor and/or other law enforcement officer related to law enforcement is not criminal offence.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	The Draft stipulates that the Law applicable to every individual conducts legal action within or outside jurisdiction of Indonesia, that causing legal impact within or outside jurisdiction of Indonesia and damaging Indonesia's interests.
Chapter III – International co-operation	Indonesian Investigators can cooperate with foreign investigators to unravel criminal offence by sharing Information and evidence.
Article 24 – Extradition	-
Article 25 – General principles relating to mutual assistance	Indonesian Investigators can cooperate with foreign investigators to unravel criminal offence by sharing Information and evidence.
Article 26 – Spontaneous information	Implemented in definition of Electronic Information. Electronic Information means one or a set of electronic data, include but not limited to writing, sound, drawing, map, plan, picture, electronic data interchange, electronic mail, telegram, telex, telecopy or the like, letter, mark, access code, symbol, or perforation processed and has meaning or can be understood by particular person.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	no
Article 28 – Confidentiality and limitation on use	The Investigation shall take into account and/or consider protection of privacy, confidentiality, uninterrupted of public services, and data integrity pursuant to prevailing laws and regulations.
Article 29 – Expedited preservation of stored computer data	The Investigation shall take into account and/or consider protection of privacy, confidentiality, uninterrupted of public services, and data integrity pursuant to prevailing laws and regulations.

Article 30 – Expedited disclosure of preserved traffic data	The Investigation shall take into account and/or consider protection of privacy, confidentiality, uninterrupted of public services, and data integrity pursuant to prevailing laws and regulations.
Article 31 – Mutual assistance regarding accessing of stored computer data	Indonesian Investigators can cooperate with foreign investigators to unravel criminal offence by sharing Information and evidence.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	no
Article 33 – Mutual assistance in the real-time collection of traffic data	Indonesian Investigators can cooperate with foreign investigators to unravel criminal offence by sharing Information and evidence.
Article 34 – Mutual assistance regarding the interception of content data	Indonesian Investigators can cooperate with foreign investigators to unravel criminal offence by sharing Information and evidence.
Article 35 – 24/7 Network	no
Article 42 – Reservations	*No need to fill in this information as it will be copied from the Council of Europe treaty data base*