www.coe.int/cybercrime

The Convention on Cybercrime: Benefits for Indonesia

Jakarta, Philippines, October 2007

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

1 About the Council of Europe ... www.coe.int

Strategy against economic crime
THE RATIONALE

in order to promote

democracy
rule of law
human rights

Measures against economic and organised crime

Established in 1949
Currently 47 member States

2

2

2 The legislative response to cybercrime

- Criminalise certain conduct ▶ substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▶ criminal procedure law
- Allow for efficient international cooperation ▶ harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements

3

3

Substantive law

Legislation to deal with – as a minimum:

- Illegal access to a computer system ("hacking", circumventing password protection, key-logging, exploiting software loopholes etc)
- Illegal interception (violating privacy of data communication)
- Data interference (malicious codes, viruses, trojan horses etc)
- System interference (hindering the lawful use of computer systems)
- Misuse of devices (tools to commit cyber-offences)
- Computer-related forgery (similar to forgery of tangible documents)
- Computer-related fraud
- Child pornography
- Hate speech, xenophobia and racism
- Infringement of copyright and related rights

Criminalising specific techniques/technologies or a certain conduct?

4

Procedural law

Legislation to provide for – as a minimum:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

5

5

3 The Convention on Cybercrime

- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- Opened for signature in Budapest in November 2001
- In force since July 2004

The Protocol on Xenophobia and Racism Committed through Computer Systems

- Opened for signature in January 2003
- In force since March 2006

6

6

Structure and content of the Convention

Chapter I: Definitions

Chapter II: Measures at national level
- Section 1 - Substantive criminal law (offences to be criminalised)
- Section 2 - Procedural law
- Section 3 - Jurisdiction

Chapter III: International cooperation
- Section 1 - General principles
- Section 2 - Specific provisions

Chapter IV: Final provisions

7

7

Chapter II – Measures at national level

Section 1 – Substantive criminal law

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Title 2 – Computer-related offences (forgery, fraud)
- Title 3 – Content-related offences (child pornography)
- Title 4 – Infringements of copyright and related rights
- Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)

8

8

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

Chapter III - International cooperation
Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

Chapter III - International cooperation...
Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data
- Art 35 - 24/7 network

Chapter IV – Final provisions

- Art 36 Signature and entry into force (open to member States and non-members which have participated in its elaboration)
- Art 37 Accession (any State may accede following majority vote in Committee of Ministers and unanimous vote by the parties entitled to sit on the Committee of Ministers)
- Art 40 – 43 Declarations, reservations
- Art 46 – Consultations of the parties

Protocol on racism and xenophobia committed through computer systems (ETS 189)

- Art 3 Dissemination of racist and xenophobic material through computer systems
- Art 4 Racist and xenophobic motivated threat
- Art 5 Racist and xenophobic motivated insult
- Art 6 Denial, gross minimisation, approval or justification of genocide or crimes against humanity

13

Implementation – current status

- The Convention entered into force in July 2004
- 21 ratifications + 22 signatures (as of 31 August 2007)
- Signed by Canada, Japan, South Africa, ratified by USA
- Costa Rica and Mexico have been invited to accede
- Legislative amendments and ratification process underway in many other countries

14

4 The Convention on Cybercrime: Benefits for Indonesia

The Convention serves as a guideline for the development of national cybercrime legislation

- Coherent approach to national legislation that helps protect society from cybercrime challenges
- Helps create a basis for public-private cooperation
- Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries
- Procedural measures for more efficient investigations
- Tools for the gathering of electronic evidence, including tools for the investigation of cyberlaundering, cyberterrorism and other serious crime

15

15

Benefits for Indonesia (2)

"Model law" function of the Convention

- Use as a checklist
- Compare provisions

Provision of Convention	Provision in national law
Art 4 System interference	?
Art 6 Misuse of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?
Art 18 Production order	?

16

16

Benefits for Indonesia (3)

The Convention serves as a framework for international cooperation against cybercrime

- Harmonisation of legislation
- Chapter 3 of the Convention provides the legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention
- Tools and obligations to cooperate
- Participation in the Consultations of the Parties (Cybercrime Convention Committee, T-CY) = participation in future work on the Convention

By becoming a party to this treaty, Indonesia can make use of this framework

17

17

Thank you.

Alexander.seger@coe.int

18

18