About the Budapest Convention on Cybercrime

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Council of Europe

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Council of Europe and cybercrime: WHY?

Hundreds of millions of incidents of theft of personal data every year

Online child sexual abuse

Cyberbullying, harassment and others forms of cyberviolence

Massive fraud generating massive amounts of crime proceeds

Attacks against critical information infrastructure

Ransomware

Interference in computer systems used in elections

Threats to

- **Human rights**
- **Democracy**
- **Rule of law**

2

Challenge: e-evidence on ANY crime

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

+

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

3

Rule of law in cyberspace and the 1% problem

Cybercrime and other offences involving evidence on computer systems (e-evidence):

WHO DID IT?

No data, no evidence, no justice

- Billions of users and devices
- Trillions of attacks
- Millions of offences
- Is there any type of crime without e-evidence?
- Investigations % ?
- Convictions % ?

= Cyberspace basically safe, crime the exception, offenders brought to justice, individuals and their rights protected?
= Rule of law in cyberspace?
= Do govs meet obligation to protect individuals against crime (ECtHR, K.U. v. Finland)?

4

Cybercrime and e-evidence: the problem of territory and jurisdiction

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?

- Transnational nature of cybercrime and e-evidence
- Crime and jurisdiction in cyberspace
- Need for public/private and international cooperation

5

The Budapest Convention on Cybercrime as a response

- Budapest Convention on Cybercrime
- Opened for signature in Budapest, Hungary, on 23 November 2001
- Negotiated by Council of Europe (47 members), Canada, Japan, South Africa and USA
- Currently 63 Parties
- Protocol on Xenophobia and Racism via computer systems (2003)
- Guidance Notes
- 2nd Additional under negotiation

6

The "mechanism" of the Budapest Convention

7

Convention backed up by …

Cybercrime Convention Committee (T-CY)

- 63 members (Parties to Convention), 8 observer States, 10 observer organisations (including EUROPOL and INTERPOL)
- Plenaries and working groups
- Assessing implementation of the Convention by the Parties
- Guidance Notes to use existing provision to address new challenges
- Preparation of new instruments ▶ Protocol to the Budapest Convention

8

Convention backed up by …

Capacity building

Dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania for worldwide capacity building:

- Support to implementation of Budapest Convention and follow up to T-CY decisions
- 250+ activities/year under several projects (priority to countries joining Convention)

9

Scope of the Budapest Convention

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

Limited by safeguards

+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

10

Scope of the Budapest Convention

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

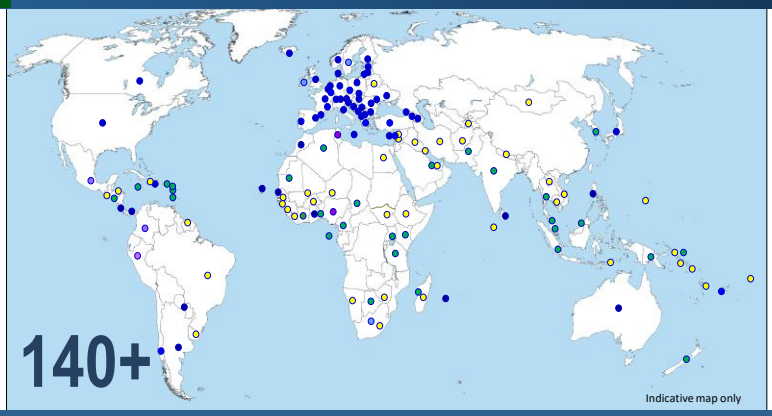
+

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

11

REACH of the Budapest Convention



Ratified/acceded: 63

Signed: 3

Invited to accede: 5

= 71

Other States with laws/draft laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 50+

12

Keeping the Budapest Convention up to date

- Protocol on Xenophobia and Racisms via Computer Systems (31 Parties + 13 Signatories)
- Guidance Notes on
  - Notion of computer systems
  - Botnets
  - Malware
  - Spam
  - Terrorism
  - Transborder access to data (Article 32)
  - Production Orders for Subscriber Information (Article 18)
  - Election interference [in preparation]
- Protocol on enhanced international cooperation under negotiation

= Budapest Convention remains up-to-date and relevant

13

Preparation of 2nd Additional Protocol

Issues to be addressed:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Possible solutions:

A. Provisions for more efficient MLA
- Emergency MLA
- Joint investigations
- Video conferencing
- Language of requests
- Etc.

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

14

Acceding to the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:

- If a country has legislation in place: Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit the instrument of accession at the Council of Europe

15

Benefits of joining Budapest Convention

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

"Cost": Commitment to cooperate

Disadvantages?

16

Starting point: Domestic legislation in line with the Convention

- Use as a checklist
- Compare provisions
- Use wording

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	?

17

Requirements in terms of legislation: substantive law

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 1	Definitions	Article 1
Art. 2	Illegal access	Articles 2 and 3
Art. 3	Illegal interception	Article 4
Art. 4	Data interference	Article 3
Art. 5	System interference	Article 3
Art. 6	Misuse of devices	
Art. 7	Computer-related forgery	Article 10
Art. 8	Computer-related fraud	Article 11
Art. 9	Child pornography	Article 7
Art. 10	IPR offences	Article 13
Art. 11	Attempt, aiding, abetting	Articles 49 and 50
Art. 12	Corporate liability	Article 48

18

Requirements in terms of legislation: procedural powers

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	Articles 21 and 46
Art. 17	Expedited preservation and partial disclosure of traffic data	Articles 17 and 21, possibly
Art. 18	Production order	Articles 18 and 21
Art. 19	Search and seizure	Articles 14 and 21
Art. 20	Real-time collection traffic data	Articles 17, 20, 21, and 46
Art. 21	Interception of content data	Articles 17 and 46
Art. 22	Jurisdiction	

19

Budapest Convention: International cooperation provisions

Combination: regular MLA + expedited and provisional measures

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 23	General principles	Article 23
Art. 24	Extradition	Articles 23, 24, 39, and 42
Art. 25	General rules	Articles 23-26 and 30-32
Art. 26	Spontaneous information	Article 38
Art. 27	MLA in absence of treaty	Articles 24 28, 29, and 31-33
Art. 28	Confidentiality	Article 28

20

Budapest Convention: International cooperation provisions

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 29	Expedited preservation	Articles 25, 30, and 31
Art. 30	Partial disclosure traffic data	
Art. 31	MLA accessing data	Article 30
Art. 32	Transborder access	
Art. 33	MLA collection traffic data	Article 30
Art. 34	MLA interception content	
Art. 35	24/7 point of contact	

21

Budapest Convention: Domestic legislation as the starting point

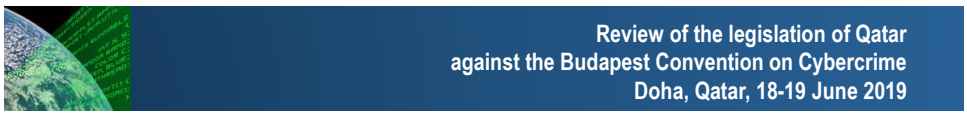
Preliminary review:

- Most (but not all) provisions of the Budapest Convention covered by Law no. 14 on Combating Cybercrime
- Clarification needed regarding specific aspects (e.g. standard of intent, specificity of procedural powers)
- Clarification needed regarding the scope of procedural powers (Article 14 Budapest Convention) and conditions and safeguards (Article 15 Budapest Convention)

▶ **This workshop is an opportunity for a more detailed review**

22

23



Compatibility of domestic legislation with the Budapest Convention

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

24

Requirements in terms of legislation: substantive law

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 1	Definitions	Article 1
Art. 2	Illegal access	Articles 2 and 3
Art. 3	Illegal interception	Article 4
Art. 4	Data interference	Article 3
Art. 5	System interference	Article 3
Art. 6	Misuse of devices	
Art. 7	Computer-related forgery	Article 10
Art. 8	Computer-related fraud	Article 11
Art. 9	Child pornography	Article 7
Art. 10	IPR offences	Article 13
Art. 11	Attempt, aiding, abetting	Articles 49 and 50
Art. 12	Corporate liability	Article 48

25

Budapest Convention: Use of terms

Article 1 – Definitions

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;

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.

26

Budapest Convention: Use of terms

Budapest Convention Article 1 – Definitions

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 14 of Qatar

?

27

Budapest Convention: Use of terms

Budapest Convention Article 1 – Definitions

For the purposes of this Convention:

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;

Law 14 of Qatar

Article 1

….

Electronic Data and Information Any information that could be stored, processed, created or transmitted through means of Information Technology, specifically text, images, sound, digits, letters, symbols, signals, or others.

28

Budapest Convention: Use of terms

Budapest Convention Article 1 – Definitions

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;

Law 14 of Qatar

Service Provider: Any person, natural or legal, public or private, providing subscribers with services to communicate via Information Technology, or processing data storage.

29

Budapest Convention: Use of terms

Budapest Convention Article 1 – Definitions

For the purposes of this Convention:

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.

Law 14 of Qatar

Article 1

Traffic Data: Any electronic data or information created through an information technology means that describes the source of communication, the destination transmitted to its route, and time, date, volume, duration and type of the service.

30

Budapest Convention: Use of terms

Budapest Convention Article 18 – Production orders

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.

Law 14 of Qatar

Article 1

Subscriber Information: Any data available with the service provider that relates to the subscribers, including:

- Type of used communication service, technical conditions, and service duration.
- The subscriber's identity, postal or geographic address, or telephone number and available payment information based on an agreement or service arrangements.
- Any other information regarding the location where the communication equipment is installed according to the service agreement.

31

Substantive criminal law

Budapest Convention 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.

32

Law 14 of Qatar

Article (3)
Whoever intentionally and illegally accesses, by any method, an electronic site, Information System, Information Network, or any information technology means or part thereof, exceeds authorized access; or knowingly continues his/her visit or access thereof, shall be punished by imprisonment for a period not exceeding three years, and a fine not exceeding (500,000) five hundred thousand Riyals, or either of these two penalties.

The punishment set forth in the preceding paragraph shall be doubled, if the act of access resulted in cancelling, omitting, adding, disclosing, impairing, modifying, transmitting, capturing, copying, publishing, or republishing electronic information or data stored in an information system; harming users or beneficiaries, destroying, stopping or disabling an electronic Site, Information System, or Information Network; changing or cancelling, or modifying the content, designs, method of using an electronic Site, or impersonating the owner or the administrator of such electronic site.

33

Budapest Convention 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.

34

Substantive criminal law

Law 14 of Qatar

Article (4)
Whoever intentionally, with no right to do so, captures, intercepts, or eavesdrops, any traffic data or any data being transmitted via the information network or any means of information technology shall be punished by imprisonment for a period not exceeding two years and a fine not exceeding (100,000) one hundred thousand Riyals, or either of these two penalties.

35

Substantive criminal law

Budapest Convention 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.

36

Substantive criminal law

Law 14 of Qatar

Article (3)
Whoever intentionally and illegally accesses, by any method, an electronic site, Information System, Information Network, or any information technology means or part thereof, exceeds authorized access; or knowingly continues his/her visit or access thereof, shall be punished by imprisonment for a period not exceeding three years, and a fine not exceeding (500,000) five hundred thousand Riyals, or either of these two penalties.

The punishment set forth in the preceding paragraph shall be doubled, if the act of access resulted in cancelling, omitting, adding, disclosing, impairing, modifying, transmitting, capturing, copying, publishing, or republishing electronic information or data stored in an information system; harming users or beneficiaries, destroying, stopping or disabling an electronic Site, Information System, or Information Network; changing or cancelling, or modifying the content, designs, method of using an electronic Site, or impersonating the owner or the administrator of such electronic site.

37

Substantive criminal law

Budapest Convention Article 5 – System interference

Establish as criminal offences under 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.

38

Substantive criminal law

Law 14 of Qatar

Article (3)
Whoever intentionally and illegally accesses, by any method, an electronic site, Information System, Information Network, or any information technology means or part thereof, exceeds authorized access; or knowingly continues his/her visit or access thereof, shall be punished by imprisonment for a period not exceeding three years, and a fine not exceeding (500,000) five hundred thousand Riyals, or either of these two penalties.

The punishment set forth in the preceding paragraph shall be doubled, if the act of access resulted in cancelling, omitting, adding, disclosing, impairing, modifying, transmitting, capturing, copying, publishing, or republishing electronic information or data stored in an information system; harming users or beneficiaries, destroying, stopping or disabling an electronic Site, Information System, or Information Network; changing or cancelling, or modifying the content, designs, method of using an electronic Site, or impersonating the owner or the administrator of such electronic site.

39

Substantive criminal law

Budapest Convention 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.

40

Substantive criminal law

Misuse of devices

[Domestic law?]

41

Substantive criminal law

Budapest Convention 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 intent to defraud, or similar dishonest intent, before criminal liability attaches.

42

Substantive criminal law

Law 14 of Qatar

Article (10)
Whoever forges of an official electronic document and knowingly uses it shall be punished by imprisonment for a period not exceeding ten years and a fine not exceeding (200,000) two hundred thousand Riyals.

And whoever forges an unofficial electronic document and knowingly uses it shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding (100,000) one hundred thousand Riyals or either of these two penalties.

43

Substantive criminal law

Budapest Convention 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.

44

Substantive criminal law

Law 14 of Qatar

Article (11)
A punishment of imprisonment for a period not exceeding three years and a fine not exceeding (100,000) one hundred thousand Riyals or either of these two penalties, shall be imposed on whoever commits any of the following acts:

1. Using information network or any means of information technology to impersonate a legal or natural person.
2. Managing through information network of any means of information technology to seize, whether for himself or for other persons, movable properties, a deed or secures signature on a deed by resorting to any fraudulent method, or adoption of a false name or false identity.

45

Substantive criminal law

Budapest Convention Article 9 – Child pornography

1 Establish as criminal offences 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.

46

Substantive criminal law

Budapest Convention Article 9 – Child pornography

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, require a lower age-limit, which shall be not less than 16 years.

47

Substantive criminal law

Law 14 of Qatar

Article (7)
Whoever produces child pornography materials by means of Information Technology, imports, sells, offers for the purpose of sale or use, circulates, distributes, transmits, publishes, makes available, or broadcasts child pornography materials by any means of information Technology shall be punished by imprisonment for a period not exceeding five years and a fine not exceeding (500,000) five hundred thousand Riyals.

And whoever possesses child pornography shall be punished by imprisonment for a period not exceeding one year and a fine not exceeding two hundred fifty thousand (250,000) Riyals, or either of these two penalties.

The child's consent is insignificant regarding crimes punishable under this Article.

Under this Article, However did not complete the age of 18 calendar years, shall be considered as a child.

48

Substantive criminal law

Budapest Convention 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.

.....

49

Substantive criminal law

Law 14 of Qatar

Article (13)
Whoever uses Information network or any Information Technology means, by any method and in any manner, to infringe or facilitate the infringement of, any copyright or author's related rights, patents, trade secrets, trademarks, trade data, commercial names, geographical indications, industrial designs, or designs of integrated circuits protected under the law shall be punished by imprisonment for a period not exceeding three years, and a fine not exceeding five hundred thousand (500,000) Riyals, or either of these two penalties.

50

Substantive criminal law

Budapest Convention 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.

51

Substantive criminal law

Budapest Convention 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.

…..

52

Substantive criminal law

Budapest Convention 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.

53

Substantive criminal law

Law 14 of Qatar – Other provisions not covered by Budapest Convention

Article (5)

Whoever sets up or manages an electronic site for the interest of a terrorist group or a terrorist organization via the information network or any other information Technology means, or facilitates communication with the leaders of these groups or any of its members; or promotes their ideas, or finances them, or publishes methods for manufacturing incendiary devices or explosives or any other devices used in terrorism acts, shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding (500,000) five hundred thousand Riyals.

54

Substantive criminal law

Law 14 of Qatar – Other provisions not covered by Budapest Convention

Article (6)
Whoever sets up or manages an electronic Site via information Network or any other Information Technology means to publish false news with the aim to jeopardize the State safety, its public order, or its internal and external security, shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding (500,000) five hundred thousand Riyals or either of these two penalties.

And whoever promotes, broadcasts, or publishes false news by any means for the same intent shall be punished by imprisonment for a period not exceeding one year and a fine not exceeding (250,000) two hundred fifty thousand Riyals or either of these two penalties.

55

Substantive criminal law

Law 14 of Qatar – Other provisions not covered by Budapest Convention

Article (8)
Whoever violates social principles or values; or otherwise publishes news, picture photos, audio or visual recordings connected to the sanctity of the personal or family life of any person, even if it is true; or infringes on others by libel or slander via Information Network or any other information Technology means shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding (100,000) one hundred thousand Riyals or either of these two penalties.

56

Substantive criminal law

Law 14 of Qatar – Other provisions not covered by Budapest Convention

Article (12)
A punishment of imprisonment for a period not exceeding three years and a fine not exceeding (200,000) two hundred thousand Riyals or either of these two penalties, shall be imposed on whoever commits any of the following acts:
1. Using, obtaining, or facilitating unlawfully, data or numbers of electronic transaction card by using the information network or any means of information technology;
2. Forging electronic transaction card by any means;
3. Manufacturing or obtaining, without authorization, devices or materials used to issue or forge electronic transaction cards;
4. Knowingly using or facilitating the use of forged electronic transaction cards;
5. Knowingly accepting invalid, forged, or stolen electronic transaction card.

57

Requirements in terms of legislation: procedural powers

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 14	Scope of procedural provisions	
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	Articles 21 and 46
Art. 17	Expedited preservation and partial disclosure of traffic data	Articles 17 and 21, possibly
Art. 18	Production order	Articles 18 and 21
Art. 19	Search and seizure	Articles 14 and 21
Art. 20	Real-time collection traffic data	Articles 17, 20, 21, and 46
Art. 21	Interception of content data	Articles 17 and 46
Art. 22	Jurisdiction	

58

Budapest Convention 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.

59

Law 14 of Qatar: 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.

60

Budapest Convention 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 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.

Law 14 of Qatar – Conditions and safeguards

Procedural law

Budapest Convention 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.

…..

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

63

Procedural law

Law 14 of Qatar

Article (21)
According to the prescribed legal procedures, service provider shall be committed to the following:

1. Providing the competent authority or the judicial and investigation authorities with all data and information necessary to uncover the truth where so is ordered by the public prosecution;
2. Taking the necessary procedures to block information network links, according to orders issued by the judicial authorities;
3. Retaining the information of the subscriber for a period of one year;
4. Urgently and temporarily preserve information, technology data , traffic data, or content information for ninety renewable days, based on a request from the competent authority, investigation bodies, or court;
5. Cooperate with and assist the competent authority in collecting or recording electronic information, electronic data and traffic data according to orders issued by the judicial authorities.

64

Budapest Convention 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

65

Law 14 of Qatar

Article (21)
According to the prescribed legal procedures, service provider shall be committed to the following:
1. Providing the competent authority or the judicial and investigation authorities with all data and information necessary to uncover the truth where so is ordered by the public prosecution;
2. Taking the necessary procedures to block information network links, according to orders issued by the judicial authorities;
3. Retaining the information of the subscriber for a period of one year;
4. Urgently and temporarily preserve information, technology data , traffic data, or content information for ninety renewable days, based on a request from the competent authority, investigation bodies, or court;
5. Cooperate with and assist the competent authority in collecting or recording electronic information, electronic data and traffic data according to orders issued by the judicial authorities

66

Budapest Convention Article 18 - Production order

1 ...measures to empower 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.

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.

67

Law 14 of Qatar

Article (18)

Public Prosecution may order every relevant person to hand over devices, tools, means, electronic information or data, traffic data, or content information relevant to the subject of the crime or whatever is useful to unveiling the truth.

Public prosecution may also order the seizure of devices, tools, or means used in committing the crime.

Article (21)

According to the prescribed legal procedures, service provider shall be committed to the following:

1. Providing the competent authority or the judicial and investigation authorities with all data and information necessary to uncover the truth where so is ordered by the public prosecution;
2. Taking the necessary procedures to block information network links, according to orders issued by the judicial authorities;
3. Retaining the information of the subscriber for a period of one year;
4. Urgently and temporarily preserve information, technology data , traffic data, or content information for ninety renewable days, based on a request from the competent authority, investigation bodies, or court;
5. Cooperate with and assist the competent authority in collecting or recording electronic information, electronic data and traffic data according to orders issued by the judicial authorities.

68

Procedural law

Budapest Convention 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.

69

Procedural law

Budapest Convention Article 19 – Search and seizure of stored computer data …

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;
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.

70

Law 14 of Qatar

Article (14)

Public Prosecution or its delegated judicial officers thereby may inspect individuals, premises, and information systems which are relevant to the crime. Search warrants shall be reasoned and specific and may be renewed more than one time as long as the reasons of such act exist. If the inspection results in seizing devices, tools, or means related to the crime, judicial officers shall present them to the Public Prosecution to take necessary measures.

Article (21)

According to the prescribed legal procedures, service provider shall be committed to the following:

1. Providing the competent authority or the judicial and investigation authorities with all data and information necessary to uncover the truth where so is ordered by the public prosecution;

2. Taking the necessary procedures to block information network links, according to orders issued by the judicial authorities;

3. Retaining the information of the subscriber for a period of one year;

4. Urgently and temporarily preserve information, technology data , traffic data, or content information for ninety renewable days, based on a request from the competent authority, investigation bodies, or court;

5. Cooperate with and assist the competent authority in collecting or recording electronic information, electronic data and traffic data according to orders issued by the judicial authorities.

71

Budapest Convention 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.

…..

72

Law 14 of Qatar

Article (17)
Public prosecution may order the collection and immediate recording of any electronic information or data, traffic data, or content information which it deems so necessary for the interest of investigation.

Article (21)
According to the prescribed legal procedures, service provider shall be committed to the following:
1. Providing the competent authority or the judicial and investigation authorities with all data and information necessary to uncover the truth where so is ordered by the public prosecution;
2. Taking the necessary procedures to block information network links, according to orders issued by the judicial authorities;
3. Retaining the information of the subscriber for a period of one year;
4. Urgently and temporarily preserve information, technology data , traffic data, or content information for ninety renewable days, based on a request from the competent authority, investigation bodies, or court;
5. Cooperate with and assist the competent authority in collecting or recording electronic information, electronic data and traffic data according to orders issued by the judicial authorities.

73

Budapest Convention 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.

….

74

Procedural law

Law 14 of Qatar

Article (17)

Public prosecution may order the collection and immediate recording of any electronic information or data, traffic data, or content information which it deems so necessary for the interest of investigation.

75

Budapest Convention: International cooperation provisions

Combination: regular MLA + expedited and provisional measures

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 23	General principles	Article 23
Art. 24	Extradition	Articles 23, 24, 39, and 42
Art. 25	General rules	Articles 23-26 and 30-32
Art. 26	Spontaneous information	Article 38
Art. 27	MLA in absence of treaty	Articles 24 28, 29, and 31-33
Art. 28	Confidentiality	Article 28

76

Budapest Convention: International cooperation provisions

Article	Budapest Convention	Domestic Law No 14 on Combating Cybercrime
Art. 29	Expedited preservation	Articles 25, 30, and 31
Art. 30	Partial disclosure traffic data	
Art. 31	MLA accessing data	Article 30
Art. 32	Transborder access	
Art. 33	MLA collection traffic data	Article 30
Art. 34	MLA interception content	
Art. 35	24/7 point of contact	

77

78