

Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE:  
INCLUDING CASE STUDIES AND LESSONS LEARNED

25-27 March 2015

Data Protection and Cybercrime

By

Eva Ignatuschtschenko

United Nations Office on Drugs and Crime

The views reflected are those of the author and do not necessarily reflect the views of UNCTAD



**UNODC**

United Nations Office on Drugs and Crime

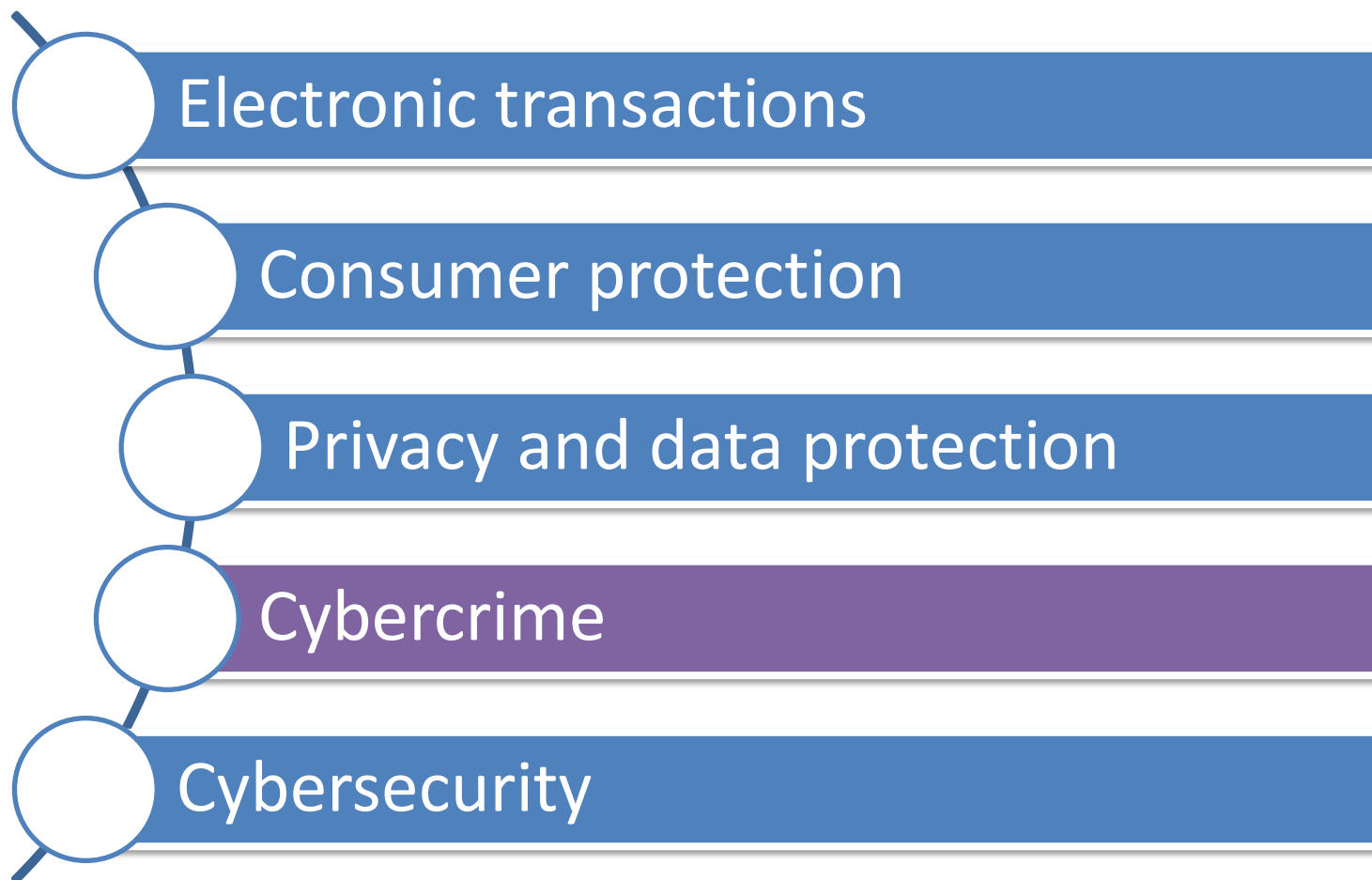
# Data protection and cybercrime

Eva Ignatuschtschenko  
Organized Crime Branch  
UNODC



[cybercrime@unodc.org](mailto:cybercrime@unodc.org)

# E-commerce regulation



# UNODC Global Programme on Cybercrime



**UNODC**

United Nations Office on Drugs and Crime

UNODC Global Programme on Cybercrime  
[cybercrime@unodc.org](mailto:cybercrime@unodc.org)

# Cybercrime Repository

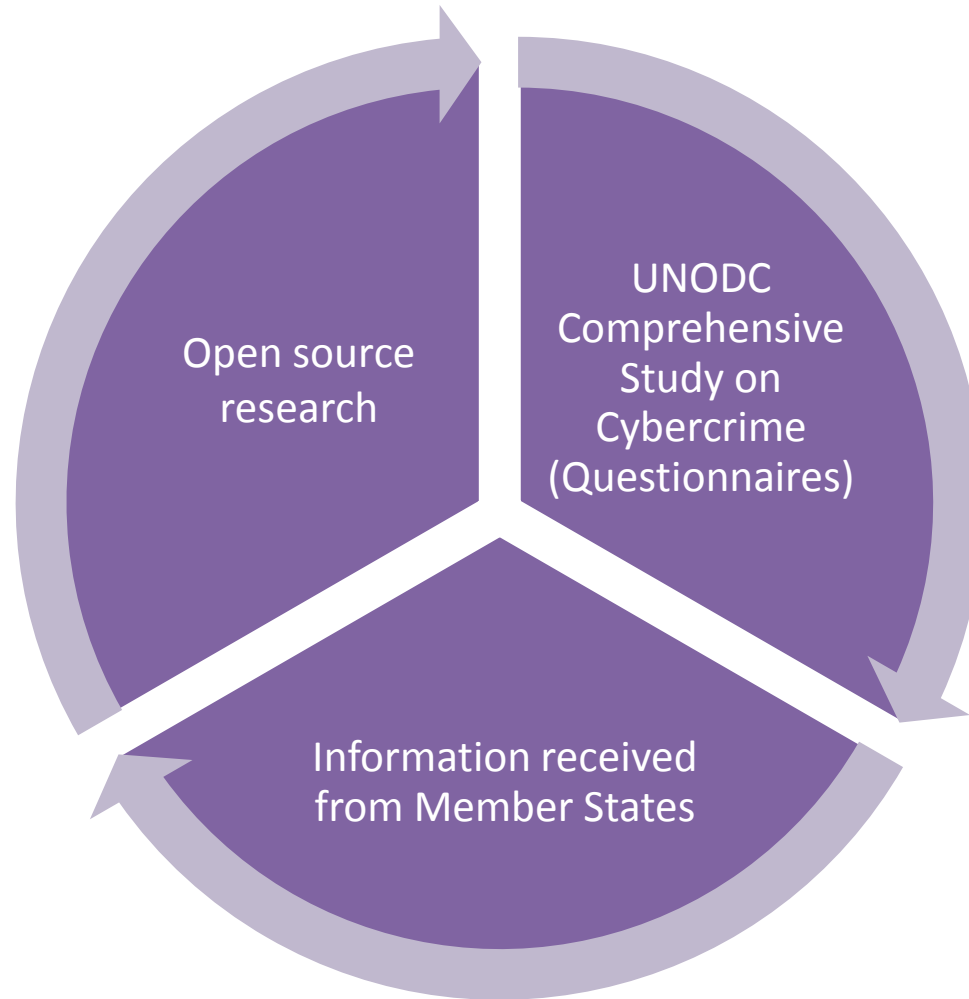
Commission on Crime Prevention and Criminal Justice  
(CCPCJ) 2013

## Resolution 22/8

*Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime*

5. *Further requests* the United Nations Office on Drugs and Crime to serve as a **central data repository of cybercrime laws and lessons learned** with a view to facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance;

# Cybercrime Repository - Sources



<http://cybrepo.unodc.org>



# REPOSITORY CYBERCRIME

The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.



## Case Law Database

Database of cybercrime case law.



## Lessons Learned

Database of lessons learned, containing national practices and strategies in preventing and combating cybercrime.



## Database of Legislation

Database of legislative provisions on cybercrime and electronic evidence.

[Acknowledgements](#)

[About us](#)

[Contact Us](#)

Copyright©2015 UNODC, All Rights Reserved, [Legal Notice](#)

The repository was made possible through the generous support of the government of the United Kingdom of Great Britain and Northern Ireland.



**UNODC**

United Nations Office on Drugs and Crime

is employed and the presentation of material in this web site do not imply the expression of any opinion whatsoever on the part of the Secretariat of the legal status of any country, territory, city, area or of its authorities, or concerning the delimitation of its frontiers or boundaries."

ercrime  
odc.org

# Database of Legislation

REPOSITORY  CYBERCRIME


 **UNODC**  
United Nations Office on Drugs and Crime

🏠 > DATABASE OF LEGISLATION


## Database of Legislation

Search Legislation Database












































... or start browsing by

 **Country**

 **Offences**

 **Procedural Aspects**

Filter Countries

<b>A</b>	 <b>Afghanistan</b> (0)	 <b>Albania</b> (8)	 <b>Algeria</b> (3)
	 <b>Andorra</b> (10)	 <b>Angola</b> (11)	 <b>Antigua and Barbuda</b> (13)
	 <b>Argentina</b> (9)	 <b>Armenia</b> (9)	 <b>Australia</b> (10)
	 <b>Austria</b> (9)	 <b>Azerbaijan</b> (5)	
<b>B</b>	 <b>Bahamas</b> (6)	 <b>Bahrain</b> (0)	 <b>Bangladesh</b> (4)
	 <b>Barbados</b> (10)	 <b>Belarus</b> (7)	 <b>Belgium</b> (13)
	 <b>Belize</b> (3)	 <b>Benin</b> (9)	 <b>Bhutan</b> (3)
	 <b>Bolivia (Plurinational State of)</b> (8)	 <b>Bosnia and Herzegovina</b> (11)	 <b>Botswana</b> (11)
	 <b>Bulgaria</b> (10)	 <b>Brazil</b> (7)	 <b>Brunei Darussalam</b> (7)
<b>C</b>	 <b>Cambodia</b> (0)	 <b>Burkina Faso</b> (2)	 <b>Burundi</b> (2)
	 <b>Cape Verde</b> (8)	 <b>Cameroon</b> (10)	 <b>Canada</b> (12)
	 <b>Chile</b> (6)	 <b>Central African Republic</b> (1)	 <b>Chad</b> (0)
	 <b>Comoros</b> (0)	 <b>China</b> (5)	 <b>Colombia</b> (7)
	 <b>Costa Rica</b> (9)	 <b>Congo</b> (0)	 <b>Cook Islands</b> (0)
		 <b>Cote d'Ivoire</b> (0)	 <b>Croatia</b> (10)



# Database of Legislation

REPOSITORY  CYBERCRIME



 **UNODC**  
United Nations Office on Drugs and Crime

🏠 > DATABASE OF LEGISLATION

## Database of Legislation

Search Legislation Database

... or start browsing by

 Country  Offences  Procedural Aspects

**Acts against the confidentiality, integrity and availability of computer data, and systems**

- Illegal access to a computer system
- Illegal access of computer data
- Interception of computer data
- Acquisition of computer data
- Illegal data/system interference
- Production/distribution/possession of computer misuse tools
- Breach of privacy/data protection measures

Computer related acts for personal or financial gain

Computer related specific acts

# Database of Legislation

REPOSITORY  CYBERCRIME

UNODC  
United Nations Office on Drugs and Crime

🏠 > DATABASE OF LEGISLATION > SEARCH



Additional criteria:  
Acts against the confidentiality, integrity and availability of computer data and systems:  
**Breach of privacy /data protection measures** ✕

Found 168 pieces of legislation Clear all search criteria ✕

- ▶ Country (105)
- ▶ National Law Title (87)
- ▶ Chapter (116)
- ▶ Article (163)
- ▼ Paragraph (1)
  - unknown (71)
- ▼ Subparagraph (1)
  - unknown (44)
- ▶ Acts against the confidentiality, integrity and availability of computer data and systems (7)
  - ▼ Computer related acts for personal or financial gain (3)
    - Forgery (4)
    - Fraud (3)
    - Identity offences (6)
  - ▼ Computer-related specific acts (3)
    - Acts causing personal harm (11)
    - Acts involving Racism/xenophobia (1)
    - Incitement to discrimination/hostility/violence (1)
- ▶ Investigative Measures (6)
- ▼ Electronic Evidence (1)
  - Admissibility of Electronic Evidence (1)
- ▼ International Cooperation (1)
  - Extradition (1)
- ▼ Liability of Legal Person (1)
  - Criminal (1)

 **Finland**

- ▶ The Criminal Code of Finland

 **France**

- ▶ Code Pénal

 **Gambia**

- ▶ Information and Communications Act

 **Georgia**

- ▶ Criminal Code of Georgia

 **Germany**

- ▶ Federal Data Protection Act
- ▶ German Criminal Code

 **Ghana**

- ▶ Electronic Communications Act

# Database of Legislation

🏠 > DATABASE OF LEGISLATION > SEARCH

- ▶ Country (105)
- ▶ National Law Title (87)
- ▶ Chapter (116)
- ▶ Article (163)
- ▼ Paragraph (1)
  - unknown (71)
- ▼ Subparagraph (1)
  - unknown (44)
- ▶ Acts against the confidentiality, integrity and availability of computer data and systems (7)
- ▼ Computer related acts for personal or financial gain (3)
  - Forgery (4)
  - Fraud (3)
  - Identity offences (6)
- ▼ Computer-related specific acts (3)
  - Acts causing personal harm (11)
  - Acts involving Racism/xenophobia (1)
  - Incitement to discrimination/hostility/violence (1)
- ▶ Investigative Measures (6)
- ▼ Electronic Evidence (1)
  - Admissibility of Electronic Evidence (1)

Search Legislation Database ✕ 🔍

Additional criteria:

Acts against the confidentiality, integrity and availability of computer data and systems:  
**Breach of privacy /data protection measures** ✕

Found 168 pieces of legislation

[Clear all search criteria ✕](#)



## Finland

### ▶ The Criminal Code of Finland

▶ Chapter 38: Data and communications offences (578/1995) ▶ Sections 1-2-9: Secrecy offence, Secrecy violation, Data protection offence

▶ Chapter 38: Data and communications offences (578/1995) ▶ Sections 8 - 8a: Computer break-in, Aggravated computer break-in



## France

### ▶ Code Pénal



## Gambia

### ▶ Information and Communications Act



## Georgia

### ▶ Criminal Code of Georgia



# Database of Legislation

## Cybercrime

Acts against the Confidentiality, Integrity and Availability of Computer, Data and Systems

- Breach of privacy/data protection measures

## Finland

### The Criminal Code of Finland

- ▶ Chapter 38
- ▶ Sections 1-2-9

## Original Text

### Section 1 - Secrecy offence (578/1995)

A person who in violation of a secrecy duty provided by an Act or Decree or specifically ordered by an authority pursuant to an Act

(1) discloses information which should be kept secret and which he or she has learnt by virtue of his or her position or task or in the performance of a duty, or

(2) makes use of such a secret for the gain of himself or herself or another shall be sentenced, unless the act is punishable under chapter 40, section 5, for a secrecy offence to a fine or to imprisonment for at most one year.

### Section 2 - Secrecy violation (578/1995)

(1) If the secrecy offence, in view of the significance of the act as concerns the protection of privacy or confidentiality, or the other relevant circumstances, is petty when assessed as a whole, the offender shall be sentenced for a secrecy violation to a fine.

(2) Also a person who has violated a secrecy duty referred to in section 1 and it is specifically provided that such violation is punishable as a secrecy violation, shall also be sentenced for a secrecy violation.

### Section 9 - Data protection offence (525/1999)

A person who intentionally or grossly negligently

(1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of data, sensitive data, identification codes or the processing of personal data for specific purposes, or violates a specific provision on the processing of personal data, (480/2001)

(2) by giving false or misleading information prevents or attempts to prevent a data subject from using his or her right of inspection, or

(3) conveys personal data to states outside the European Union or the European Economic Area in violation of chapter 5 of the Personal Data Act, and thereby violates the privacy of the data subject or causes him or her other damage or significant inconvenience, shall be sentenced for a data protection offence to a fine or to imprisonment for at most one year.

## Details

Source:

<http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf>

## Attachments

Criminal Code of Finland as of 2012



**UNODC**

United Nations Office on Drugs and Crime

UNODC Global Programme on Cybercrime  
[cybercrime@unodc.org](mailto:cybercrime@unodc.org)

# Database of Legislation

...with, whereby the data subject approves the processing of his/her personal data;

(8) *personal credit data* means the personal data intended for the assessment of the financial situation, ability to keep a commitment or credibility of a private individual; and

(9) *credit data file* means a file containing personal credit data.

## Section 4 — *Application of Finnish law*

(1) This Act applies to processing of personal data where the controller is established in the territory of Finland or otherwise subject to Finnish law.

(2) This Act applies also if the controller is not established in the territory of a Member State of the European Union, but it uses equipment located in Finland in the processing of personal data, except where the equipment is used solely for the transfer of data through the territory. In this case the controller shall designate a representative established in Finland.

## Chapter 2 — **General rules on the processing of personal data**

### Section 5 — *Duty of care*

The controller shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject's private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an Act. Anyone operating on the behalf of the controller, in the form of an independent trade or business, is subject to the same duty of care.

### Section 6 — *Defined purpose of processing*

It must be appropriate and justified to process personal data in the operations of the controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data

## ***Personal Data Act (523/1999)***

vessel or aircraft or a member of its crew.

### **Section 3 - *Offence directed at Finland***

(1) Finnish law applies to an offence committed outside of Finland that has been directed at Finland.

(2) An offence is deemed to have been directed at Finland

- (1) if it is an offence of treason or high treason,
- (2) if the act has otherwise seriously violated or endangered the national, military or economic rights or interests of Finland, or

(3) if it has been directed at a Finnish authority.

### **Section 4 - *Offence in public office and military offence***

(1) Finnish law applies to an offence referred to in chapter 40 of this Code that has been committed outside of Finland by a person referred to in chapter 40, section 11, paragraphs (1), (2), (3) and (5) (604/2002).

(2) Finnish law also applies to an offence referred to in chapter 45 that has been committed outside of Finland by a person subject to the provisions of that chapter.

### **Section 5 - *Offence directed at a Finn***

Finnish law applies to an offence committed outside of Finland that has been directed at a Finnish citizen, a Finnish corporation, foundation or other legal entity, or a foreigner permanently resident in Finland if, under Finnish law, the act may be punishable by imprisonment for more than six months.

### **Section 6 - *Offence committed by a Finn***

(1) Finnish law applies to an offence committed outside of Finland by a Finnish citizen. If the offence was committed in territory not belonging to any State, a precondition for the imposition of punishment is that, under Finnish law, the act is punishable by imprisonment for more than six months.

(2) A person who was a Finnish citizen at the time of the offence or is a Finnish citizen at the beginning of the court proceedings is deemed to be a Finnish citizen.



# Case Law Database



## REPOSITORY CYBERCRIME

The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.



### Case Law Database

Database of cybercrime case law.



### Database of Legislation

Database of legislative provisions on cybercrime and electronic evidence.



### Lessons Learned

Database of lessons learned, containing national practices and strategies in preventing and combating cybercrime.

[Acknowledgements](#)

[About us](#)

[Contact Us](#)

# Case Law Database

## Case Law Database

Search Cases

x



... or start browsing by



Country



Offences

**Acts against the confidentiality,  
integrity and availability of  
computer data, and systems**

Computer related acts for personal  
or financial gain

Computer related specific acts

Illegal access to a computer system

Illegal access of computer data

Interception of computer data

Acquisition of computer data

Illegal data/system interference

Production/distribution/ possession of computer misuse tools

Breach of privacy/data protection measures



# Case Law Database

▼ Country (4)

-  Italy (1)
-  Russian Federation (1)
-  Spain (1)
-  United States of America (2)

▶ Acts against the confidentiality integrity and availability of computer, data and systems (7)

▼ Computer related acts for personal or financial gain (5)





- Copyright/trademark violations (1)
- Forgery (1)
- Fraud (4)
- Identity offences (2)
- Sending/controlling sending of SPAM (1)


▶ Computer related specific act (9)

▼ Decision/Verdict Date (1)


- 2013 (1)

▼ Defendant's Nationality (4)


-  Latvian (1)
-  Romanian (1)
-  Russian (1)
-  Ukrainian (1)

Search Cases  


Additional criteria:

Acts against the confidentiality integrity and availability of computer, data and systems: **Illegal access to a computer system** 

Found 5 cases

[Clear all search criteria](#) 

**RUx001 Organized cybercrime case 2004**

 **Russian Federation**

An organized criminal group consisting of Russian and Kazakh nationals extorted money from foreign companies between 2003 and 2004. The suspects attacked servers of the corporate victims and demanded the payment of thousands of US dollars in order to stop attacking such servers.

[Show more](#)

**SPA0001R Operation Exposure**

 **Spain**

Operation "Exposure" was an international cybercrime investigation carried out in Europe and South America. In February 2012, law enforcement from various countries arrested 25 alleged members of the international hacking network Anonymous. Ten arrests were made in Argentina, six in Chile, five in Colombia and four Spain.

[Show more](#)

**ITAx004 Operation Stop Intrusion**

 **Italy**

The case involves the sending of fake email messages to employees of the Italian Ministry of Foreign Affairs and other civil servants in order to steal their credentials and access



# Case Law Database



## Cybercrime

Acts against the Confidentiality, Integrity and Availability of Computer, Data and Systems

- **Illegal data/system interference**
- **Breach of privacy/data protection measures**

## Operation Exposure



 **Spain**

UNODC No.: **SPA0001R**

Sentence Date:



## Cross Cutting

### Liability

... for

- **completed offence**

... based on

- **criminal intent**

... as involves


- **principal offender(s)**
- **participant, facilitator, accessory**

### Application of the Convention


#### Involved Countries

 **Argentina**

 **Chile**

 **Colombia**

 **Spain**

 **Bulgaria**

 **Czech Republic**

#### Investigation

#### Involved Agencies

- **INTERPOL**

• **Europol**



# Operation 'Exposure'

- International cybercrime investigation
- 2012 - 25 alleged members of the international hacking network '*Anonymous*' arrested in Argentina, Chile, Colombia Spain
- Charges: illegal interference, breach of privacy and disclosure of confidential information
- Direct & quick response from Europol Cyber Crime Centre
- Servers hosted in Bulgaria and Czech Republic
- Simultaneous arrests, house searches and disruption of the servers



# Lessons Learned



## REPOSITORY CYBERCRIME

The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.



### Case Law Database

Database of cybercrime case law.



### Database of Legislation

Database of legislative provisions on cybercrime and electronic evidence.



### Lessons Learned


Database of lessons learned, containing national practices and strategies in preventing and combating cybercrime.

[Acknowledgements](#)

[About us](#)

[Contact Us](#)

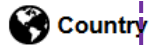
# Lessons Learned

 > LESSONS LEARNED

## Lessons Learned

Search Lessons Learned  

... or start browsing by











































Country




Topics



Filter Countries

- |          |   |   |  |
|----------|---|---|--|
| <b>A</b> |  <b>Afghanistan</b> (1)                        |  <b>Albania</b> (1)                    |  <b>Algeria</b> (5)             |
|          |  <b>Andorra</b> (0)                            |  <b>Angola</b> (0)                     |  <b>Antigua and Barbuda</b> (0) |
|          |  <b>Argentina</b> (5)                          |  <b>Armenia</b> (0)                    |  <b>Australia</b> (11)          |
|          |  <b>Austria</b> (2)                            |  <b>Azerbaijan</b> (1)                 |  |
| <b>B</b> |  <b>Bahamas</b> (0)                            |  <b>Bahrain</b> (0)                    |  <b>Bangladesh</b> (1)          |
|          |  <b>Barbados</b> (0)                           |  <b>Belarus</b> (1)                    |  <b>Belgium</b> (2)             |
|          |  <b>Belize</b> (0)                             |  <b>Benin</b> (1)                      |  <b>Bhutan</b> (0)              |
|          |  <b>Bolivia (Plurinational State of)</b> (0) |  <b>Bosnia and Herzegovina</b> (1)   |  <b>Botswana</b> (5)          |
|          |  <b>Bulgaria</b> (0)                         |  <b>Brazil</b> (5)                   |  <b>Brunei Darussalam</b> (0) |
|          |  <b>Cabo Verde</b> (0)                       |  <b>Burkina Faso</b> (0)             |  <b>Burundi</b> (0)           |
| <b>C</b> |  <b>Canada</b> (13)                          |  <b>Cambodia</b> (1)                 |  <b>Cameroon</b> (0)          |
|          |  <b>Chile</b> (3)                            |  <b>Central African Republic</b> (0) |  <b>Chad</b> (0)              |
|          |  <b>Comoros</b> (0)                          |  <b>China</b> (1)                    |  <b>Colombia</b> (4)          |
|          |   |  <b>Congo</b> (0)                    |  <b>Cook Islands*</b> (0)     |



# Lessons Learned

 > LESSONS LEARNED

## Lessons Learned

... or start browsing by

-  Country
-  Topics
  - Prevention
  - Investigation**
  - Evidence and Procedure
  - International Cooperation
  - Technical Assistance
  - Prosecution

Investigative powers  
Obtaining data from service providers  
Other investigative measures

# Lessons Learned

🏠 > LESSONS LEARNED > SEARCH

- ▶ Country (30)
- ▼ Investigation (1)
  - Obtaining data from service providers (31)


## Lessons Learned

Additional criteria:

Investigation: Obtaining data from service providers

Found 31 entries [Clear all search criteria x](#)

### Good practice for obtaining information relevant to a cybercrime investigation from a service provider

 Estonia

Service Providers collect and retain data for 1 year in accordance with the Electronic Communications Act. Thus, we have no problems in receiving the necessary data from the service providers. For basic data like IP addresses, an inquiry is sufficient and the provider shall answer within 30 days. For real-time data or e-mails, we use a specific method that requires a court order. A court order is also necessary for stored content. After the

### Approaches to expeditious preservation of computer data involving multiple service providers

 Finland

In practice, preservation orders may be ordered so that they are addressed to all operators which were involved with the communication, even if they can not yet, at the moment of the order, be identified. (Finnish Governments proposal for implementing the data preservation 153/2006 page 72). However, preservation orders must be issued CSP by CSP. The difficulty lies in receiving enough information from one identified CSP to enable the

[Show more](#)


### Good practice for obtaining information relevant to a cybercrime investigation from a service provider

 Finland

An order is sent to a service provider for the purpose of identifying the possible suspect. The needed information is normally obtained in digital format, and in most cases it is the traffic data that is relevant for the investigation. Information is collected during the

# Lessons Learned

## Good practice for obtaining information relevant to a cybercrime investigation from a service provider

 **Estonia**

### Investigation

#### Topic

- **Obtaining data from service providers**

#### Details:

Service Providers collect and retain data for 1 year in accordance with the Electronic Communications Act. Thus, we have no problems in receiving the necessary data from the service providers. For basic data like IP addresses, an inquiry is sufficient and the provider shall answer within 30 days. For real-time data or e-mails, we use a specific method that requires a court order. A court order is also necessary for stored content. After the issuance of the order, service providers release the requested data, establishing the delivery method on a case-by-case basis.

# The cybercrime repository can assist countries in the fight against cybercrime

- Legislative drafting
- Policy response to cybercrime
- Good practices & lessons learned in investigation, prosecution and prevention of cybercrime
- Cooperation with third parties
- Formal and informal international cooperation



Thank you!



<http://cybrepo.unodc.org>

E-mail: [cybercrime@unodc.org](mailto:cybercrime@unodc.org)