



UNODC

United Nations Office on Drugs and Crime

Approaches in national cybercrime legislation and the UNODC Cybercrime Repository

Organized Crime Branch
UNODC



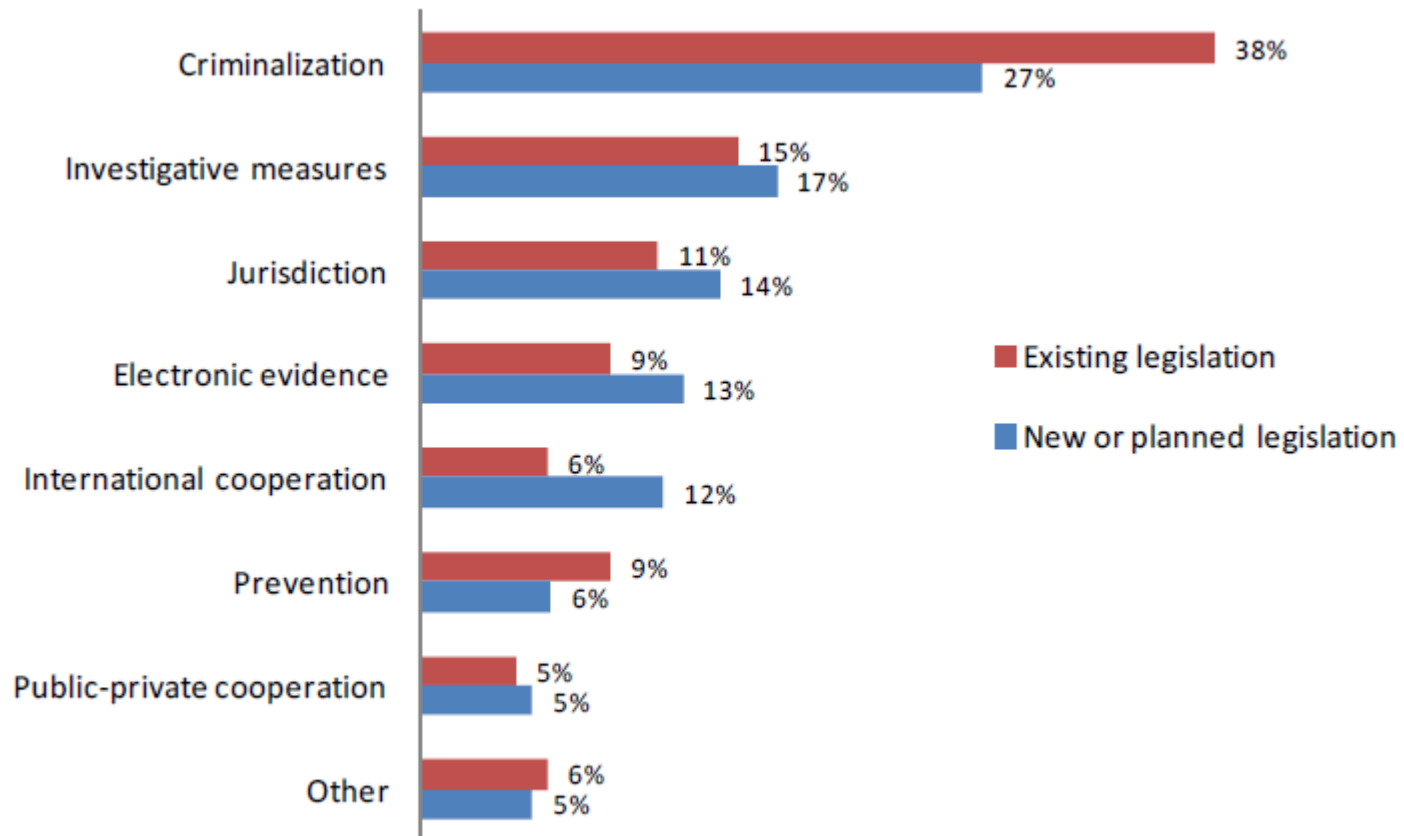
cybercrime@unodc.org

UNODC Global Programme on Cybercrime



Cybercrime Legislation

Figure 3.1: Cybercrime legislation areas



Source: Study cybercrime questionnaire. Q12 and Q14. (n=55,36; r=262,111)

Cybercrime Offences

Cybercrime

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

- Fraud
- Forgery
- Identity offences
- Copyright/trademark violations
- Sending/controlling sending of SPAM

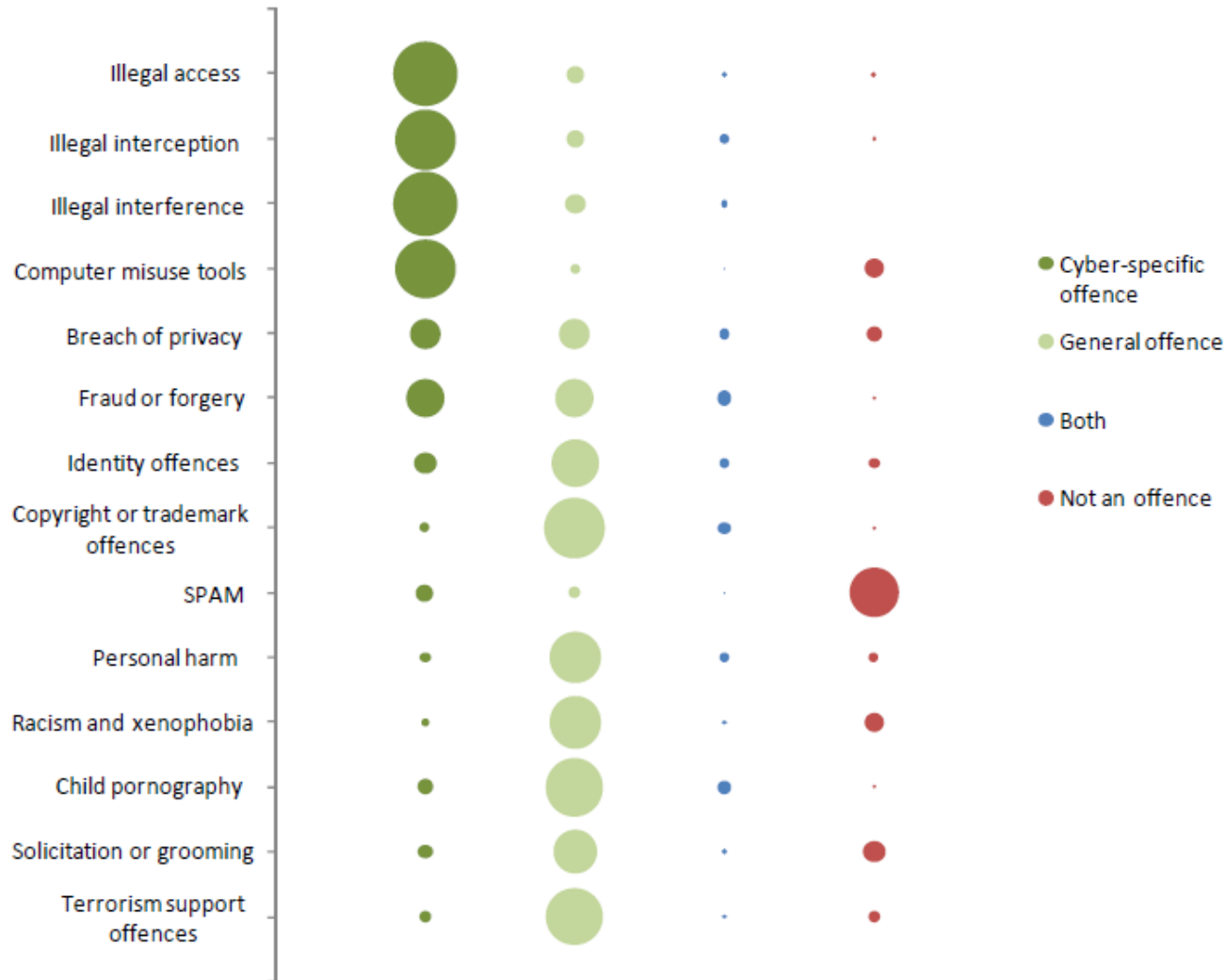
Computer-related specific acts

- Acts causing personal harm
- Acts involving Racism/xenophobia
- Production/distribution/ possession of child pornography
- Solicitation/'grooming' of children
- Financing/planning of terrorism
- Incitement to terrorism
- Incitement to genocide
- Incitement to discrimination/hostility/violence
- Propaganda to war



Cybercrime Criminalization

Figure 4.1: National approaches to criminalization of cybercrime acts



Source: Study cybercrime questionnaire. Q25-38. (n=61)

Cybercrime Procedural Aspects

Procedural aspects

**Investigative
Measures**

**Electronic
evidence**

Jurisdiction

**International
cooperation**

**Third parties
cooperation
obligations**



UNODC

United Nations Office on Drugs and Crime

Procedural Investigative Powers

Figure 5.3: National approaches to investigative measures for cybercrime



Source: Study cybercrime questionnaire. Q42-51. (n=55)

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

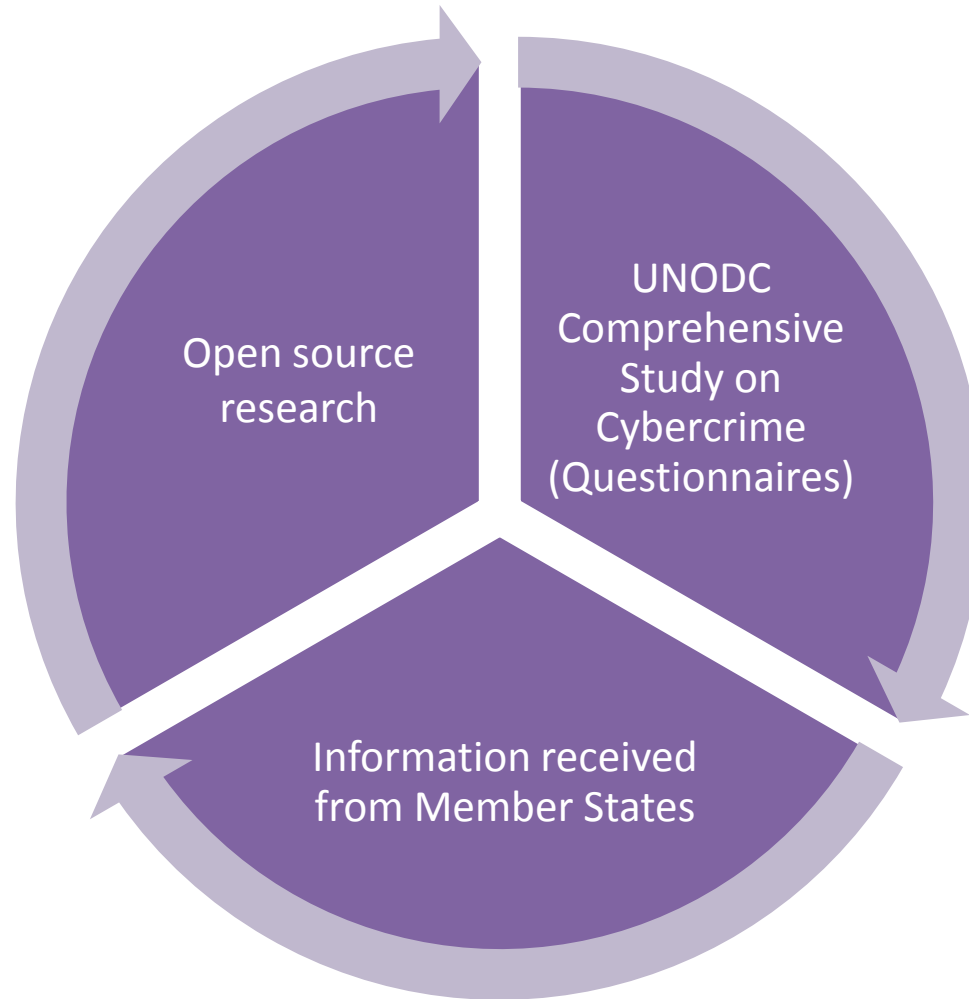
5. *Further requests* the United Nations Office on Drugs and Crime to serve as a **central data repository of cybercrime laws and lessons learned** with a view to facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance;



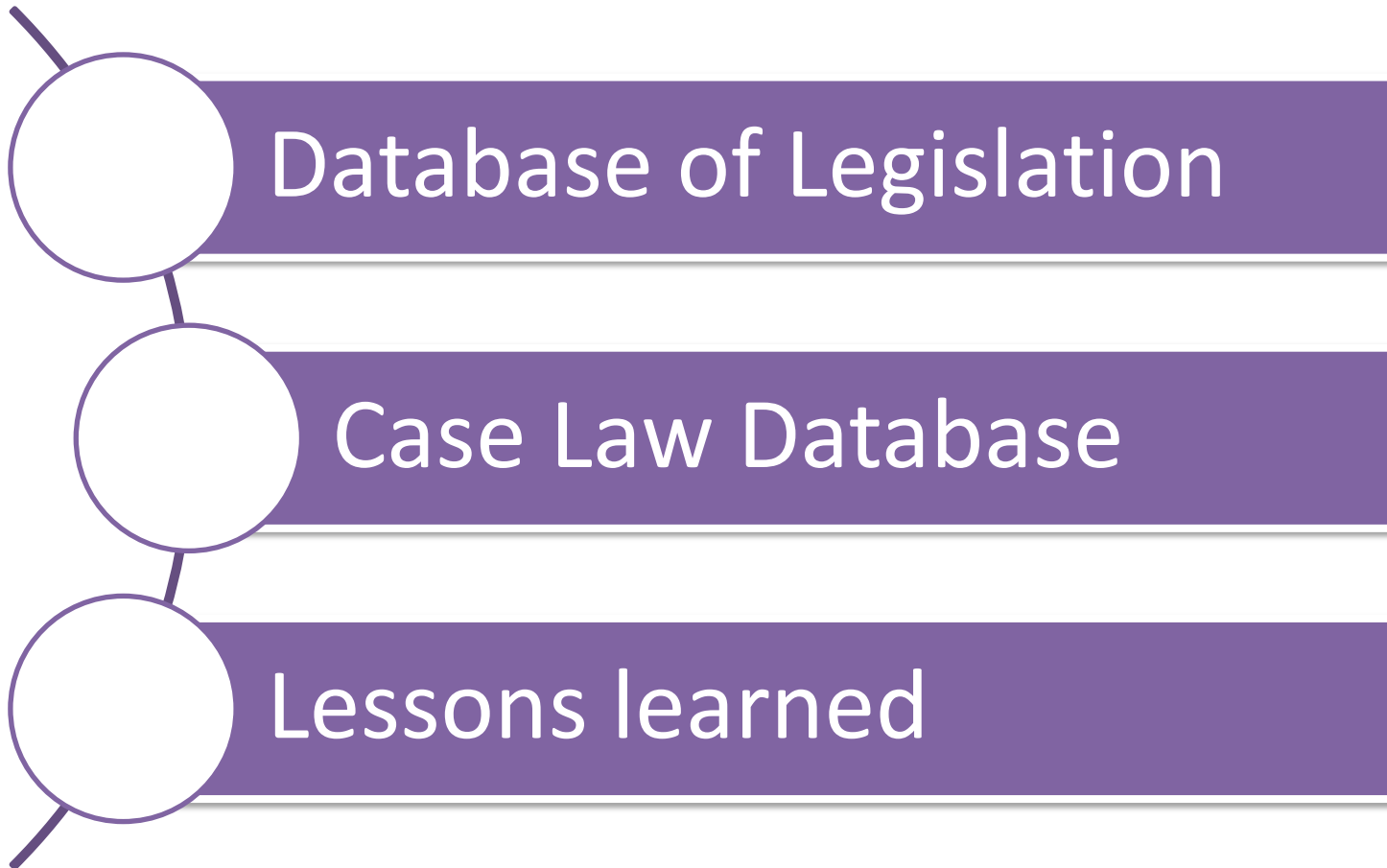
UNODC

United Nations Office on Drugs and Crime

Cybercrime Repository - Sources



Cybercrime Repository



SHERLOC Knowledge Management Portal



SHaring Electronic Resources and
Laws On Crime

The SHERLOC portal is an initiative to facilitate the dissemination of information regarding the implementation of the UN Convention against Transnational Organized Crime and its three Protocols.



Case Law Database

A comprehensive case law database that allows you to see how Member States are tackling organized crime cases in their courts.



Database of Legislation

An electronic repository of laws relevant to the requirements of the Organized Crime Convention and the Protocols thereto. Most of the legislation included in this database has been enacted specifically to counter the relevant crime type. For more information click [here](#).



CNA Directory

Directory of competent national authorities that have been designated to receive, respond and process requests pertaining to mutual legal assistance, extradition and transfer of sentenced prisoners, smuggling of migrants and trafficking in firearms.

(Account needed to access the Directory. For more information click [here](#).)



Bibliographic Database

An annotated bibliography providing a synopsis of key articles that are search-able by countries, research methods and keywords. The database is under development and currently includes research on migrant smuggling.

Newsletter

Want to get the latest updates in your inbox? Just drop us your email below and we keep you up to date.

Subscribe



UNODC

United Nations Office on Drugs and Crime

UNODC Global Programme on Cybercrime
cybercrime@unodc.org

<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.

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

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

Investigation Procedure

- Computer Specific Procedural Aspects**
- Jurisdiction
- International Cooperation
- Regulatory Provisions
- Witnesses & Victims


Investigative Measures


- Search for computer hardware or data
- Seizure of computer hardware or data
- Order for subscriber information
- Order for stored traffic data
- Order for stored content data
- Real-time collection of traffic data
- Real-time collection of content data
- Expedited preservation of computer data
- Use of remote forensic tools
- Trans-border access to a computer system or data
- Informal approaches to obtain data from third parties

Procedural Aspects

- Electronic Evidence**
 - Admissibility of Electronic Evidence

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

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](#)


- ▶ 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



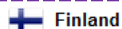
Database of Legislation



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

Database of Legislation

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.



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



Cross Cutting

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

REPOSITORY  CYBERCRIME

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

[Home](#) > [CASE-LAW DATABASE](#) > [SEARCH](#)



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**



UNODC

United Nations Office on Drugs and Crime

UNODC Global Programme on Cybercrime

cybercrime@unodc.org

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](#)

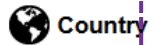
Lessons Learned

 > LESSONS LEARNED

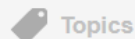
Lessons Learned

Search Lessons Learned 

... or start browsing by











































Country



Topics

Filter Countries

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

Lessons Learned

[Home](#) > LESSONS LEARNED

Lessons Learned

x



... 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



UNODC

United Nations Office on Drugs and Crime

UNODC Global Programme on Cybercrime


cybercrime@unodc.org

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 ✕

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

Strengthening of the capacities of El Salvador National Police to effectively identify and investigate cybercrime cases.

Objective: to strengthen El Salvador's national capacities to prevent and fight against cybercrime through tailor-made technical assistance services focused on crime prevention and criminal justice and based on UNODC's assessment, protocols and tools.

Outcome 1: Effective investigation, prosecution and adjudication of cyber crime cases in El Salvador.

1.1.

- Assistance delivered for the development of normative and operational documents for the Cybercrime Unit of the National Civil Police of El Salvador.

1.2.

- Other Units of the National Police and Prosecution Offices supported by the Cybercrime Unit in Cybercrime-related cases.

1.3.

- Cybercrime Unit equipped.

1.4.

- Law enforcement officers and prosecutors trained in different areas, for example: cybercrime investigation techniques, crimes against children, financial crimes, etc.

Outcome 1: Effective investigation, prosecution and adjudication of cyber crime cases in El Salvador.

1.5.

- National Police officers in El Salvador trained to effectively identify and report cybercrime cases.

1.6.

- Judge in El Salvador trained to work with cybercrime cases, including the interpretation of electronic evidence.

1.7.

- Training courses on cybercrime approved and replicated by the National Academy of Public Security.

1.8.

- Training courses on cybercrime approved and replicated by the Prosecutors' Academy.

Outcome 2: Citizens in El Salvador are aware of the threats posed by cybercrime and take steps to prevent and fight against it.

2.1.

- Increased understanding among children of the threats that may be found on the internet and the best way to address them.

2.2.

- Cybercrime reporting mechanisms established.

Outcome 3: Government institutions works jointly with the private sector and other countries in the region to effectively address cybercrime.

3.1.

- National Police and prosecutors supported by internet services providers in the prevention and fight against cybercrime.

3.2.

- Law enforcement officials have a better understanding of the corporate procedures, jurisdiction, legal process requirements and cooperation channels with International Private Companies.

3.3.

- Cooperation networks with other countries in the region established.



On September, 2015 the Cybercrime Unit was created by the Subdirection of Investigations with intermediation of UNODC.



In order to deliver effective tools for preventing and countering cybercrime, UNODC has provided 6 external hard drives, 2 multifunctional printers, 1 mobile printer, 2 UFED Ruggedized Kits (to National Civil Police's Cybercrime Unit and Attorney General's Office Criminal Analysis Unit), 1 laptop for on site forensic examination, 16 desks and 16 chairs.



In order to strengthen El Salvador's national capacities to prevent and fight against cybercrime a training workshop on «*Investigation and Digital Forensic Techniques. Child Pornography Cases*» (May 18-22), a workshop on «*Cybercrime General Perspective and Comprehensive Care for Children and Adolescents*» (September, 16) and a «*Basic Course on Cybercrime Investigation*»(September, 7-October, 5) have been delivered.



Up to now, 485 children and adolescents, as well as 79 parents and teachers, have been sensitized through workshops focused on threats that may be found by children on the internet



On May 10-13, 2015, a study visit to Mexico took place. The objective was that the Salvadoran delegation -six investigators and two prosecutors- obtained first-hand knowledge about the organization of Mexico Federal Police Cyber Coordination and Mexico City Cybercrime Police organization, working procedures and the challenges they face when investigating cybercrime.

Guatemala Cybercrime Project

This programme is intended to support the law enforcement and criminal justice community to combat the abuse of Internet technology services against children. This will be accomplished by improving local law enforcement capacity and making the investigation and prosecution of cybercrime against children a local responsibility that is confidently undertaken.

Direct Effect 1: Strengthening of the Anti-Organized Crime Department at National Civil Police, Specialized Division on Criminal Investigation, through the implementation of the Criminal Investigation Management Model in the Cybercrime Section.

1.1.

- Analysis and revision of legal and operation framework of the Cybercrime Section and development of protocols and operational guides.

1.2.

- Design and implementation of the Criminal Investigation Management Model in the Cybercrime Section

Direct Effect 2: Strengthening the strategic criminal prosecution of human trafficking crimes in the Specialized Office of the General Attorney's Office.

2.1.

- Design and create the monitoring ICAC unit in the Specialized Attorney Office against human trafficking.

Direct Effect 3: Increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime acts against children, leading to greater deterrence and just outcomes for suspected persons, in line with international human rights standards

3.1.

- Provide skills and knowledge to investigators and prosecutors to combat the abuse of Internet technology services against children.

3.2.

- Provide instruction on considerations for judges in handling child victims in ICAC cases.

Thank you!



cybercrime@unodc.org