Web site: www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 March 2008 T-CY (2008) 02

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

COMPILATION OF NATIONAL LEGISLATION FROM A NUMBER OF STATES PARTIES TO THE CONVENTION CONCERNING ARTICLES 1.d, 2, 16 and 17 OF THE CONVENTION ON CYBERCRIME

Secretariat Memorandum
prepared by
the Directorate General of Human Rights and Legal Affairs (DG-HL)

Replies for each article are presented by States Parties

A) Article 1.d concerning the definition of traffic data

Bulgaria

Penal Procedure Code Additional provisions

§ 1. (2) For the purposes of this Code **"data concerning traffic"** shall mean all data related to a message going through a computer system which have been generated as an element of a communications chain indicating the origin, destination, route, hour, date, size and duration of the connection or of the main service.

Croatia

Criminal Code, article 89 paragraphs 31, 32, and 33 (OG 105/04.)

Cyprus

Article 2 of Cyprus Law No 22(III)04

"Traffic data" means any computer data created by a computer system and related to a communication achieved through computer systems, representing a part of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of service used for the communication.

Estonia

National law including Penal Code uses the definitions of the Convention. Penal Code does not define these terms separately.

France

Hungary

Article 2 of Hungarian Law no 108/2001 (E-Commerce and IT)

Romania

Article 35 (1) of Romania Law no 161/2003

Article 35 (1) d) „computer data" are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function;

Ukraine

The United States

B) Article 2 concerning illegal access to computer system and computer data

Bulgaria

Article 216 (3), (5), (6) and article 319a of the Penal Code

(3) (New, SG 92/02) Who, by unwarranted access to a computer of importance for an enterprise, corporate body or individual, destroys or damages another's property, shall be punished by imprisonment of one to six years and a fine of up to ten thousand levs.

Croatia

Criminal Code, article 223 paragraph 1. (OG 105/04.)

Article 223
(1) Whoever, without authorization despite the protective measures, accesses the computer data or programs of another shall be punished by a fine or by imprisonment not exceeding three years.

Cyprus

Article 4 of Cyprus Law No 22(III) 04

Article 4 - Any person who intentionally and without authority access a computer system by breaking the security measures commits a criminal offence and is liable to 5 years imprisonment or to 20.000 Cyprus Pounds fine or both.

Estonia

Penal Code Article 217

§ 217. Unlawful use of computer, computer system or computer network
(1) Unlawful use of a computer, computer system or computer network by way of removing a code, password or other protective measure is punishable by a pecuniary punishment.
(2) The same act, if it:
1) causes significant damage, or
2) is committed by using a state secret or a computer, computer system or computer network containing information prescribed for official use only,
is punishable by a pecuniary punishment or up to 3 years' imprisonment.

France

Code Pénal, article 323-1

Hungary

Criminal Code, article 300/C and 300/E of Hungarian Law no 4/1978

Criminal Conduct for Breaching Computer Systems and Computer Data
Section 300/C
(1) Any person who gains unauthorized entry to a computer system or network by compromising integrity of the computer protection system or device, or overrides or infringes his misdemeanor punishable by imprisonment not to exceed one year, work in community service.

(2) Any person who
a) without permission alters, damages or deletes data stored, processed or transmitted network or denies access to the legitimate users,
b) without permission adds, transmits, alters, damages, deletes any data, or uses any other computer system or network is guilty of misdemeanor punishable by imprisonment not community service or a fine.

(3) Any person who, for financial gain or advantage,
a) alters, damages or deletes data stored, processed or transmitted in a computer system to the legitimate users,
b) adds, transmits, alters, damages, deletes data or uses any other means to disrupt use network
is guilty of felony punishable by imprisonment not to exceed three years.

(4) The punishment for the criminal act defined in Subsection (3) shall be
a) imprisonment between one to five years if it causes considerable damage,
b) imprisonment between two to eight years if it causes substantial damage,
c) imprisonment between five to ten years if it causes particularly substantial damage.

Compromising or Defrauding the Integrity of the Computer Protection System or Device
Section 300/E
(1) Any person who, for the commission of the criminal activities defined in Section 300/C,
a) creates,
b) obtains,
c) distributes or trades, or otherwise makes available computer software, passwords, entry codes, or other data with which to gain access to a computer system or network is guilty of misdemeanor punishable by imprisonment not to exceed two years, work in community service or a fine.
(2) Any person who, for the commission of the criminal activities defined in Section 300/C, conveys his economic, technical and/or organizational expertise to another person for the creation of computer software, passwords, entry codes, or other data with which to gain access to a computer system or network shall be punished according to Subsection (1).
(3) In the case of Paragraph a) of Subsection (1), any person who confesses to the authorities his involvement in the creation of any computer software, password, entry code, or other data with which to gain access to a computer system or entire computer network before the authorities learned of such activities through their own efforts, and if the person surrenders such produced things to the authorities and assists in the efforts to identify the other persons involved, shall be exonerated from punishment.

Romania

Article 42 of Romania Law no 161/2003

Article 42 – (1) The illegal access to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years.

Ukraine

Criminal Code, article 359 (with amendments of September 1, 2001)
Criminal Code, article 361 (with amendments of June 5, 2003)

Article 359. Illegal use of special technology for secret obtaining of information
1. Unlawful use of special technology for secret obtaining of information, -
shall be punishable by a fine of 100 to 200 tax-free minimum incomes, or restraint of liberty for a term up to four years, or imprisonment for the same term.
2. The same actions, if repeated, or committed by a group of persons upon their prior conspiracy, or by an organized group, or if they caused any substantial damage to legally protected rights, freedoms and interests of individual citizens, or state and public interests, or interests of individual legal entities, shall be punishable by imprisonment for a term of three to seven years.

Article 361. Unauthorized interference to work of electronic machines (computers), automated systems, computer networks or Networks of electrical communication
1. Unauthorized interference to functioning of electronic machines (computers), automated systems, computer networks or networks of electrical communication that resulted in a leak, loss, fouls, blocking of information, distortion of information processing or to violation of set order of its routing, -
Shall be punishable by a fine in the amount of 600 up to 1000 untaxed minimums of income of citizens or by restraint of liberty for the term of 2 up to 5 years, or by deprivation of liberty for the term of up to 3 years with disqualification to hold certain position or carry on certain activity for the period of up to 2 years or without such and with confiscation of program means (software) and technical means (hardware) by means of which unauthorized interference was committed and are owned by guilty person.

2. The same actions, accomplished repeatedly or with prior agreement of the group of persons, or if they caused serious harm, -
Shall be punishable by deprivation of liberty for the term of 3 up to 6 years or carry on certain activity for the period of up to 3 years and with confiscation of software and technical devices by means of which unauthorized interference was committed and are owned by guilty person.

Note: in the articles 361- 363-1 “serious harm” means the sustaining a material damage which in 100 and more times exceeds untaxed minimum of citizens’ income.

The United States

Title 18, Part I, Chapter 47, § 1030 of the US Code

CHAPTER 47 - FRAUD AND FALSE STATEMENTS
Sec. 1030. Fraud and related activity in connection with computers
(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) - (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; (!1)
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. (c) The punishment for an offense under subsection (a) or (b) of this section is -

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if - (i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section -

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer -
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means -
(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) (!2) of the Federal Reserve Act;
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic

damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

C) Article 16 concerning expedited preservation of stored computer data

Bulgaria

Article 159 in connection with article 125, article 172 (3), Penal Procedure Code
Article 55, article. 56, article 148, Ministry of Interior Act
Article 251 of the Electronic Communications Act

Article 159
Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Article 125
(1) Where material evidence cannot be separated from the place, where it was found, and also in other cases specified by this Code, the following shall be prepared: photographs, slides, films, video tapes, sound-recordings, recordings on carriers of computerized data, layouts, schemes, casts or prints thereof.
(2) The court and the authorities entrusted with pre-trial proceedings shall also collect and inspect the objective forms of evidence prepared with the use of special intelligence means in the hypotheses herein set forth.
(3) The materials under the paragraphs 1 and 2 shall be enclosed with the case file.
Persons who shall prepare objective forms of material evidence.

Article 172
(1) Pre-trial bodies may use the following special intelligence means: technical means - electronic and mechanical devices and substances that serve to document operations of the controlled persons and sites, as well as operational techniques - observation, interception, shadowing, penetration, marking and verification of correspondence and computerised information, controlled delivery, trusted transaction and investigation through an officer under cover.
(2) Special intelligence means shall be used where this is required for the investigation of serious criminal offences of intent under Chapter one , Chapter two , Sections I, II, IV, V, VIII, and IX, Chapter five , Sections I - VII, Chapter six , Section II - IV, Chapter eight , Chapter nine "a" , Chapter eleven , Sections I - IV, Chapter twelve , Chapter thirteen , and Chapter fourteen , as well as with regard to criminal offences under Article 219 , para 4, proposal 2, Article 220 , para 2, Article 253 , Article 308, paras 2, 3 , and 5, sentence two, Article 321 , Article 321a, Article 356k . and 393 of the Special Part of the Criminal Code, where the irrelevant circumstances cannot be established in any other way or this would be accompanied by exceptional difficulties.
(3) Computer information service providers shall be under the obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special technical devices only where this is required for the purposes of detecting crimes under paragraph 2
(4) The special intelligence means of controlled delivery and trusted transaction may be used to collect material evidence, whereas under cover officers shall be interrogated as witnesses.

(5) The materials under paragraphs 1-4 shall be enclosed with the case file.

Article 55
(1) Police bodies may issue orders to state bodies, organizations, legal entities and citizens, whenever required for fulfilment of the functions, assigned to them. The orders shall be given verbally or in writing.
(2) Should it be impossible to issue orders verbally or in writing, they may be conveyed through actions, the meaning of which is understandable for the persons they concern.
(3) In fulfilment of the functions of control of road traffic safety, the orders may be conveyed by actions or signs, as stipulated by act.
(4) The orders of a police body are obligatory unless they would force a person to commit an obvious crime or a violation.
(5) Orders issued in writing may be appealed against in accordance with the Administrative Procedure Code.

Article 56
(1) Police bodies issue a verbal or written warning to persons, in regard to whom sufficient data exist and they lead to suspicion that he/she would commit a crime or a violation of public order.
(2) Written warnings are included in a notice to the person informing him/her of the liability related to the respective crime or violation of the public order.
(3) The notice of warning is issued in the presence of the person and one witness, and signed by the police body, the person and the witness after being read by them. Should the person refuse to sign the notice, the fact is certified by signature of the witness. In cases of domestic violence a copy of the notice of warning would be made available to the victim upon request.

Article 148
(1) The bodies carrying out investigative work, issue compulsory instructions to state bodies, organizations, legal entities and citizens, within their competences.
(2) State bodies and organizations must provide to the bodies under paragraph (1) access to official premises, technical junctions and other property of theirs.

Article 251
(1) For the needs of national security, as well as for detection of criminal offences, the undertakings providing public electronic communications networks and/or services shall store specified categories of data for a period of twelve months. Any data disclosing the content of the communications may not be stored according to this procedure.

Croatia

Cyprus

Estonia

Criminal Procedure Code Art 215
The obligations of a communication undertaking are regulated in Electronic Communications Act: article 111 (only available in Estonian)

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices

(1) The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

France

Code de Procédure Pénale, article 56, paragraphe 7
Code de Procédure Pénale, article 60-2

Article 56
Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal.

Il a seul, avec les personnes désignées à l'article 57 et celles auxquelles il a éventuellement recours en application de l'article 60, le droit de prendre connaissance des papiers, documents ou données informatiques avant de procéder à leur saisie.

Toutefois, il a l'obligation de provoquer préalablement toutes mesures utiles pour que soit assuré le respect du secret professionnel et des droits de la défense.

Tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues à l'article 57.

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

Si une copie est réalisée, il peut être procédé, sur instruction du procureur de la République, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Avec l'accord du procureur de la République, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité.
Le procureur de la République peut également, lorsque la saisie porte sur des espèces, lingots, effets ou valeurs dont la conservation en nature n'est pas nécessaire à la manifestation de la vérité ou à la sauvegarde des droits des personnes intéressées, autoriser leur dépôt à la Caisse des dépôts et consignations ou à la Banque de France.

Lorsque la saisie porte sur des billets de banque ou pièces de monnaie libellés en euros contrefaits, l'officier de police judiciaire doit transmettre, pour analyse et identification, au moins un

exemplaire de chaque type de billets ou pièces suspectés faux au centre d'analyse national habilité à cette fin. Le centre d'analyse national peut procéder à l'ouverture des scellés. Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés entre les mains du greffier de la juridiction compétente. Ce dépôt est constaté par procès-verbal.

Les dispositions du précédent alinéa ne sont pas applicables lorsqu'il n'existe qu'un seul exemplaire d'un type de billets ou de pièces suspectés faux, tant que celui-ci est nécessaire à la manifestation de la vérité.

Si elles sont susceptibles de fournir des renseignements sur les objets, documents et données informatiques saisis, les personnes présentes lors de la perquisition peuvent être retenues sur place par l'officier de police judiciaire le temps strictement nécessaire à l'accomplissement de ces opérations.

Article 60-2

Sur demande de l'officier de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa du 3º du II de l'article 8 et au 2º de l'article 67 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 Euros. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du code pénal.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises.

Hungary

Article 151 of Hungarian Law no 100/2003 (Communication of Information Law)

Romania

Article 54 of Romania Law no 161/2003

Article 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer

systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) is bound to immediately make available for the criminal investigation body the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Ukraine

The United States

Title 18, Part I, Chapter 121, § 2704 of the US Code

CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS
Sec. 2704. Backup preservation

(a) Backup Preservation. –
(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.
(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).
(3) The service provider shall not destroy such backup copy until the later of –
(A) the delivery of the information; or (B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.
(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider –
(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and
(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.
(b) Customer Challenges. - (1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement (A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and (B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect. (2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure. (3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response. (4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed. (5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

D) Article 17 concerning expedited preservation and partial disclosure of traffic data

Bulgaria

Article 159 Penal Procedure Code
Article 55, article 56, article 148 of the Law on Ministry of Interior

Article 159
Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Article 55

(1) Police bodies may issue orders to state bodies, organizations, legal entities and citizens, whenever required for fulfilment of the functions, assigned to them. The orders shall be given verbally or in writing.
(2) Should it be impossible to issue orders verbally or in writing, they may be conveyed through actions, the meaning of which is understandable for the persons they concern.
(3) In fulfilment of the functions of control of road traffic safety, the orders may be conveyed by actions or signs, as stipulated by act.
(4) The orders of a police body are obligatory unless they would force a person to commit an obvious crime or a violation.
(5) Orders issued in writing may be appealed against in accordance with the Administrative Procedure Code.

Article 56
(1) Police bodies issue a verbal or written warning to persons, in regard to whom sufficient data exist and they lead to suspicion that he/she would commit a crime or a violation of public order.
(2) Written warnings are included in a notice to the person informing him/her of the liability related to the respective crime or violation of the public order.
(3) The notice of warning is issued in the presence of the person and one witness, and signed by the police body, the person and the witness after being read by them. Should the person refuse to sign the notice, the fact is certified by signature of the witness. In cases of domestic violence a copy of the notice of warning would be made available to the victim upon request.

Article 148
(1) The bodies carrying out investigative work, issue compulsory instructions to state bodies, organizations, legal entities and citizens, within their competences.
(2) State bodies and organizations must provide to the bodies under paragraph (1) access to official premises, technical junctions and other property of theirs.

Croatia

Cyprus

Estonia

Criminal Procedure Code Article 215
The obligations of a communication undertaking are regulated in Electronic Communications Act: article 111 (only available in Estonian)

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices
(1) The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection

(1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

France

Code de Procédure Pénale, article 60-2, paragraphe 2

Article 60-2

Sur demande de l'officier de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa du 3º du II de l'article 8 et au 2º de l'article 67 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 Euros. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du code pénal.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises.

Hungary

Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)

Romania

Article 54 of Romania Law no 161/2003

Article 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) is bound to immediately make available for the criminal investigation body the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Ukraine

The United States

Title 18, Part I, Chapter 121, § 2702 of the US Code

CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS
Sec. 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions. - Except as provided in subsection (b) –
(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.
(b) Exceptions for disclosure of communications. - A provider described in subsection (a) may divulge the contents of a communication -
(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
(7) to a law enforcement agency –
(A) if the contents – (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or [(B) Repealed. Pub. L. 108-21, title V, Sec. 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]
(8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.
(c) Exceptions for Disclosure of Customer Records. - A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) –
(1) as otherwise authorized in section 2703;
(2) with the lawful consent of the customer or subscriber;
(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;
(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
(6) to any person other than a governmental entity.

*****