

Project on Cybercrime

www.coe.int/cybercrime



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Second draft (8 June 2007)

Cybercrime legislation – country profile

Argentina

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
 Department of Technical Cooperation
 Directorate General of Human Rights and Legal Affairs
 Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
 Fax: +33-3-9021-5650
 Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	
Signature of Convention:	Yes: _____ (Date) No: <input checked="" type="checkbox"/> _____
Ratification/accession:	Yes: _____ (Date) No: <input checked="" type="checkbox"/> _____
	<p>If not yet signed/acceded to:</p> <p>What measure are being undertaken in your country to become a Party?</p> <p>The Government created a commission with the Ministry of Justice and with Ministry of Foreign Affairs in order to elaborate the adjustment of the criminal law and procedural law, and also to evaluate the possibility to sign the Convention and its implementation. Recently, the Ministry of Foreign affaire began to take measures in order to follow all the step for approving the Convention.</p> <p>There is a Draft of Bill that includes all the cyber crimes that is now under analysis by the Congress (see the explanation below). Also there is a commission created by the Executive Power which is working in the integral modification of the criminal procedural law.</p>
Provisions of the Convention	Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<i>Chapter I – Use of terms</i>	
Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”	“informatics system” “electronic communication”, “traffic data” are all terms added in several drafts of law.
<i>Chapter II – Measures to be taken at the national level</i>	There is a Draft of Law approved in one of the “Cámaras” of the Congress, that include the integral modification of crimes related to Cybercrime established in the Convention (see the attachment)

<p><i>Section 1 – Substantive criminal law</i></p>	<p>However, there are already specific laws related to some of the cybercrimes of the Convention. “Ley de Protección de Secretos Comerciales” (24.766) “Ley Penal Tributaria” (24.769) included the crimes related to informatics records of the Taxes Office. “Ley 25.036” included the copyright’s violation of intellectual property related to software. “Ley 25.286 de Protección de datos personales” included the crime related false information and illegal acces at personal data base.</p>
<p>Article 2 – Illegal access</p>	<p>art. 157 of the Criminal Code in the case of personal data bases. Article 5 of the Federal draft of bill.</p>
<p>Article 3 – Illegal interception</p>	<p>Art. 4 of the Federal draft of bill.</p>
<p>Article 4 – Data interference</p>	<p>Art. 6 of The Federal draft of bill “The National Criminal Code will include what follows as second and third paragraphs of Section 183:</p> <p style="padding-left: 40px;">Whoever, through any means, destroys completely or partially, erases, alters temporarily or permanently, or in any way prevents the use of data or programs, whatever the medium containing them, during the processing of an electronic communication shall be punished by imprisonment of a term not less than one month nor more than two years...”</p> <p>However, in some cases the Judges have used the all law included in the force Penal Code.</p>
<p>Article 5 – System interference</p>	
<p>Article 6 – Misuse of devices</p>	<p>Art. 6 of The national draft of bill</p> <p style="padding-left: 40px;">“...The same punishment shall apply to whoever sells, distributes or in any way disseminates through or introduces in a computer system, any program destined to cause damages as those described in the previous paragraph, or in a computer program or in data contained in any form of computer and telecommunications systems...”</p>
<p>Article 7 – Computer-related forgery</p>	<p>Included in the case of the base of personal data. Article 117 force Penal Code.</p>
<p>Article 8 – Computer-related fraud</p>	<p>Art. 11 of the federal draft of bill as follow: “Whoever, with the intent of obtaining his own or someone else’s patrimonial benefit, causes a prejudice in the patrimony of a third party through the inclusion of false data, the alteration, illicit collection or suppression of true data, the addition of programs or the modification of programs contained in information technology media, or the alteration of the operation of any process or performance, or through any form of computer manipulation alters the normal operation of a computer system, or the transmission of data after their processing”</p> <p>However, there are precedents that some judges have used the Basic crime of fraud: “Any person who defrauds another by use of false name, position or title, or by the pretense of false influence or by</p>

	abuse of confidence, or by pretending imaginary wealth, credit, commission, enterprise or negotiation or by any other kind of artifice or deceit, shall be punished with jailing from one month to six years”
Article 9 – Offences related to child pornography	<p>Art. 1 of the draft of bill.</p> <p>However, there is a criminal law allows to charge of this crime.</p> <p>Section 128 (text in accordance with Law 25,087)</p> <p>Any person who produces or publishes pornographic images portraying persons under eighteen years of age or organizes live performances with pornographic scenes involving such minors shall be punished with jailing from six months to four years.</p> <p>The same punishment shall be imposed upon anybody who distributes pornographic images with external characteristics that evidence the fact that the portrayed persons were under eighteen years of age when the image was created.</p> <p>Any person who facilitates the access of persons under fourteen years to pornographic shows or supplies such minors with pornographic material shall be punished with jailing from one month to three years.</p>
Title 4 – Offences related to infringements of copyright and related rights	<p>Federal Bill 25036 (Protection of software):</p> <p><i>The amended section 1 of Law 11,723 states that intellectual property, writings of whatever type and length (as in dictionaries, prayer books, almanacs and articles), computer software, compilation of data or other materials, dramatic works, musical compositions, or musical drama; cinematography, choreography and pantomime works (as long as these works have been materialized in a tangible form) television programs, works of art or science used in commerce or industry, printed matter, blueprints and maps, digital discs, photographs, engravings and phonograph records, etc., may be objects of a violation of copyrights.</i></p> <p>Article 71: Anyone who, in any way or through any means whatsoever defrauds the intellectual property rights acknowledged by this Act shall be subject to the punishment established by Section 172 of the Criminal Code¹.</p>
Article 10 – Offences related to infringements of copyright and related rights	
Article 11 – Attempt and aiding or abetting	
Article 12 – Corporate liability	Is not legislate up to the moment in Criminal Code.
Article 13 – Sanctions and measures	
Section 2 – Procedural law	<i>Argentina is a federation composed of Provinces and the city of Buenos Aires, which retain all powers not delegated to the Federal Government in accordance with the Federal Constitution. Among those</i>

	<i>delegated powers are those of enacting substantive law such as the Penal Code. Adjective Law (i.e. that related to procedures before courts) depends, in each case, on such provisions as legislative power of each Province (and the city of Buenos Aires) may provide.</i>
Article 14 – Scope of procedural provisions	
Article 15 – Conditions and safeguards	
Article 16 – Expedited preservation of stored computer data	Law number 25.873 Its implementation laws were against Constitutional Law. Then, Judges have declared that it has no effect for violating Constitutional law.
Article 17 – Expedited preservation and partial disclosure of traffic data	Idem
Article 18 – Production order	Similar Procedural Law related to postal and phone communications are used for these cases with some problems in the jurisprudence.
Article 19 – Search and seizure of stored computer data	Idem
Article 20 – Real-time collection of traffic data	Idem
Article 21 – Interception of content data	Idem
<i>Section 3 – Jurisdiction</i>	There are not specific rules for cybercrimes. General rule is art. 1 of National Criminal Code
Article 22 – Jurisdiction	There is no specific rules about cybercrimes. Criminal Code, art. 1 establish the principle of territory. (The Criminal Code will be applied where the crime is committed, with some exceptions given in the same Code related to the effects of the crimes and the principle of national when is affected some national interest)
<i>Chapter III – International co-operation</i>	<i>There is no specific rules for cybercrime but there is a general law, Nro. 24.767 y some bilateral agreements with other countries.</i>
Article 24 – Extradition	There is no specific rules for cybercrime (but there is a general law, Nro. 24.767)
Article 25 – General principles relating to mutual assistance	There is a general law related to international cooperation and procedures (Ley 24767) and there are many bilateral agreements signed with other countries, but not specifically about cybercrime.
Article 26 – Spontaneous information	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	
Article 28 – Confidentiality and limitation on use	
Article 29 – Expedited preservation of stored computer data	
Article 30 – Expedited disclosure of preserved traffic data	

Article 31 – Mutual assistance regarding accessing of stored computer data	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	
Article 33 – Mutual assistance in the real-time collection of traffic data	
Article 34 – Mutual assistance regarding the interception of content data	
Article 35 – 24/7 Network	
Article 42 – Reservations	<i>No need to fill in this information as it will be copied from the Council of Europe treaty data base</i>

Appendix: Solutions in national legislation.

National Criminal Code In Spanish

Código Penal

LIBRO PRIMERO DISPOSICIONES GENERALES Título. I –

Aplicación de la ley penal

Art. 1.- Este Código se aplicará:

1º Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción;

2º Por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo.

Constitution of Argentina

Section 18

No inhabitant of the Nation may be punished without previous trial based on a law enacted before the act that gives rise to the process, nor tried by special committees, nor removed from the judges appointed by law before the act for which he is tried. Nobody may be compelled to testify against himself, nor be arrested except by virtue of a written warrant issued by a competent authority. The defense by trial of persons and rights may not be violated. The domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed. Death penalty for political causes, any kind of tortures and whipping, are forever abolished. The prisons of the Nation shall be healthy and clean, for the security and not for the punishment of the prisoners confined therein; and any measure taken with the pretext of precaution which may lead to mortify them beyond the demands of security, shall render liable the judge who authorizes it.

NATIONAL CHAMBER OF DEPUTIES

**ORDINARY SESSIONS
2006
Order of the Day No. 1227**

**Communications and Information Technology Committee
and Criminal Legislation Committee**

Printed October 26, 2006

Summary: National Criminal Code, information technology crimes, modification. Nemirovski, Romero, Bisutti, Irrazábal, Lovaglio Saravia, Osorio, Ritondo, Zottos, Canevarolo, Morini, Pérez (A.), Conti, Pinedo, Uñac y Solanas. (5.864-D.-2006)

Committee Resolution

Honorable Chamber:

The Communications and Information Technology Committee and the Criminal Legislation Committee have considered the Bill signed by Deputies Nemirovski, Romero, Bisutti, Irrazábal, Lovaglio Saravia, Osorio, Ritondo, Zottos, Canevarolo, Morini, Pérez (A.), Conti, Pinedo, Uñac y Solanas, on information technology crimes; and for the reasons stated in the accompanying report and those that will be given by reporting member, advice the sanction of the following

BILL

The Senate and the Chamber of Deputies...

Crimes against Sexual Integrity

Section 1 – Section 128 of the National Criminal Code will be substituted by the following:

Section 128: Whoever produces, facilitates, disseminates, finances, offers, trades, distributes or publishes through any means, any representation of a person under eighteen years of age engaged in explicit, real or simulated, sexual activities as well as any representation of such a person's genital organs for mainly sexual purposes shall be punished by imprisonment for a term not less than one nor more than five years.

The punishment will be for not less than six months nor more than two years imprisonment for whoever possesses depictions as those described above for dissemination or commercialization purposes.

Whoever facilitates the access to pornographic shows or to pornographic material to a child under fourteen years of age will be punished by imprisonment for a term of not less than one month nor more than one year.

Crimes against Privacy

Section 2 – The epigraph of Chapter III, Title V, Book II of the National Criminal Code will be substituted by the following: "Violation of Secrets and Privacy".

Section 3 – Electronic communications enjoy the same legal protections of epistolary communications and telecommunications.

Section 4 – Section 153A of the National Criminal Code will be substituted by the following:

Section 153A - Whoever unduly opens or accesses to an electronic communication, a letter, a closed envelope, a telegraphic or telephonic or other manner of dispatch that is not addressed to him, or unduly takes hold of an electronic communication, a letter, an envelope, a dispatch or any other form of private paper, even if it is not closed; or suppresses or deviates from its destination a piece of mail or an electronic communication that is not

addressed to him shall be punished by imprisonment for a term of not less than fifteen days nor more than six months.

Whoever communicates to someone else or published the contents of a letter, written paper, electronic dispatch or communication, shall be punished by imprisonment for a term of not less one month nor more than one year.

Section 5 - The National Criminal Code will include what follows as Section 153B:

Section 153B: Whoever illegitimately and knowingly accesses through any means and without due authorization or exceeding his own authorization, an information system or data set whose access is restricted, and if this does not result in an offense more severely punished, shall be punished by imprisonment for a term of not less than fifteen days nor more than six months.

Punishment shall be imprisonment of not less than one month nor more than one year when this access affects the information system of a government agency or a public service provider.

Section 6 - The National Criminal Code will include what follows as Section 153C:

Section 153C: Whoever illegitimately and in order to violate someone else's privacy, using devices that may capture, intercept, transmit, record or reproduce voices, sounds or images, obtains, disseminates, reveals or releases to a third party the data or facts thus uncovered or the captured images, shall be punished by imprisonment for a term not less than one month nor more than two years.

Section 7 - The National Criminal Code will include what follows as Section 153D:

Section 153D: Whoever unduly intercepts, captures or deviates postal communications, telecommunications or any other mailing system or private data package of a restricted character or unduly reveals its existence shall be punished by imprisonment for a term of not less than one month nor more than two years.

Punishment shall be for a term not less than one nor more than four years if the author of the offense is a public official or a member of the armed or security forces.

Section 8 - Section 155 of the National Criminal Code will be substituted by the following:

Section 155: Whoever, being in possession of a piece of mail, an electronic communication, a closed envelope, a telegraphic or telephonic or other manner of dispatch, not intended for publication, has them unduly published, even if they were addressed to him, if the publication may damage or cause prejudice to a third party, shall be punished by a fine of not less than ten thousand pesos (\$10,000) nor more than one hundred thousand pesos (\$100,000).

Section 9 - Section 157 of the National Criminal Code will be substituted by the following:

Section 157: The public official who reveals facts, conducts, documents or data that by law should remain secret, whatever the nature of their medium, will be punished by imprisonment of not less than one month nor more than two years and a special ban of not less than one nor more than four years.

Section 10 - Subsection 2 of Section 157 of the National Criminal Code will be substituted by the following:

Subsection 2: Whoever unduly inserts or makes someone else insert data into a personal data file or provides a third party with information contained in a personal data file or reveals to someone else information kept in a personal data bank whose secrecy he is bound to keep by law.

Fraud

Section 11 - The National Criminal Code will include what follows as Subsection 16 of Section 173:

Subsection 16: Whoever, with the intent of obtaining his own or someone else's patrimonial benefit, causes a prejudice in the patrimony of a third party through the inclusion of false data, the alteration, illicit collection or suppression of true data, the addition of programs or the modification of programs contained in information technology media, or the alteration of the operation of any process or performance, or through any form of computer manipulation alters the normal operation of a computer system, or the transmission of data after their processing.

Damage

Section 12 - The National Criminal Code will include what follows as second and third paragraphs of Section 183:

Whoever, through any means, destroys completely or partially, erases, alters temporarily or permanently, or in any way prevents the use of data or programs, whatever the medium containing them, during the processing of an electronic communication shall be punished by imprisonment of a term not less than one month nor more than two years.

The same punishment shall apply to whoever sells, distributes or in any way disseminates through or introduces in a computer system, any program destined to cause damages as those described in the previous paragraph, or in a computer program or in data contained in any form of computer and telecommunications systems.

Section 13 - Subsection 5 of Section 184 of the National Criminal Code will be substituted by the following:

Subsection 5: To perpetrate it in files, registries, museums or in bridges, roads, pathways or other venues used by the general public; or on tombs, commemorative signs, monuments, statues, paintings or other works of art placed in public buildings or places; or in public computer systems or databases.

Section 14 - The National Criminal Code will include what follows as Subsection 6 of Section 184:

Subsection 6: To perpetrate it in computer systems related to the provision of health services, communications, energy provision or transport, means of public transportation or other public services.

Interruption of communications

Section 15 - Section 197 of the National Criminal Code will be substituted by the following:

Section 197: Whoever interrupts or obstructs any communication established through any means, or violently resists the reestablishment of the interrupted communication shall be punished by imprisonment for a term of no less than six months nor more than two years.

Alteration of evidence

Section 16 - Section 255 of the National Criminal Code will be substituted by the following:

Section 255: Whoever subtracts, alters, hides, destroys, or renders useless, in its entirety or partially, objects destined to serve as evidence before competent authorities, registries, documents, whatever their medium, trusted to the custody of a public official or any other

person in the interest of public service, shall be punished by imprisonment for a term of no less than one month nor more than four years. If the guilty person is the object's depositary, he shall be punished besides with a special ban for a double period. If the act is committed through the depositary's imprudence or negligence, he shall be punished by a fine of no less than seven hundred and fifty pesos (\$750) nor more than twelve thousand pesos and five hundred (\$12,500).

Falsification of electronic or information technology documents

Section 17 - The National Criminal Code will include what follows as the last paragraph of Section 77:

The term document encompasses any representation of acts or facts, independently of the medium used to support it, store it, or file it.

Section 18 - Let it be communicated to the Executive Branch.
Committee's Hall, October 10, 2006.

Oswaldo M. Nemirovski. - Rosario M. Romero. - Daniel R. Kroneberger. - Luis B. Lusquiños. - Mirta Pérez. - Adrián Menem. - María A. Carmona. - Arturo M. Heredia. - Miguel J. Baladrón. - Alberto J. Beccani. - Elisa M. Carrió. - Nora A. Chiacchio. - Diana B. Conti. - Jorge E. Coscia. - Francisco J. Ferro. - Amanda S. Genem. - Miguel A. Iturrieta. - José E. Lauritto. - Gustavo A. Marconato. - Oscar E. Massei. - María C. Moisés. - Ana M. del C. Monayar. - Pedro J. Morini. - Cristián R. Oliva. - Cristián A. Ritondo. - Paola R. Spatola. - Marta S. Valverde.

In partial dissidence:

Paula M. Bertol.

REPORT

Honorable Chamber:

The Communications and Information Technology Committee and Criminal Legislation Committee have considered the bill proposed by the deputies Nemirovski, Romero, Bisutti, Irrazábal, Lovaglio Saravia, Osorio, Ritondo, Zottos, Canevarolo, Morini, Pérez (A.), Conti, Pinedo, Uñac y Solanas on computer crimes.

It is obvious that computer technology has made an enormous impact on the everyday life of individuals and organizations, and that its evolution and progress has great importance for any country's development. However, alongside the progress of information technology, a new series of illicit behaviors known generally as computer crimes and taking very diverse forms, have appeared. They may be committed anywhere and at any time. These crimes against computer systems threaten the construction of a safer society and of spaces of liberty, security and justice.

The present legal void in our legal system and the juridical insecurity that results from it, drove us to analyze the need to propose legislation that may provide juridical protection to the integrity and availability of information. We believe, moreover, that it is necessary to provide members of the judiciary and of law enforcement agencies who are in charge of investigating these crimes with knowledge (training) as well as advanced modern tools (technology).

Therefore, a subcommittee made up of advisors from both committees was created. Both public and private experts were invited and they made important contributions to improve future legislation. The list of experts specially invited includes police chief Rodolfo Koleff and inspector Miguel Justo, members of the Technology Crimes and Criminal Analysis Division of Argentina's Federal Police; Daniel Sentinelli, an expert in computer safety, from "Dominio Digital" (a television show on information, technology and the Internet); Juan P. Cardinal, Microsoft's representative;

Javier Díaz, Dean of the Computer Technology School of the Universidad Nacional de La Plata; representatives from Telecom; Dr. Juan Pablo Maglier and Dr. Sonia Agnen; Diego Velardem Eduardo Gabelloni and Mariana Cruglia from Telefónica; and Dr. Pablo Marzilli from cell phone company Movistar; Ricardo Presta, vice-president of Proveedores de Internet (ISPS); Carlos Achiary, Computer Director at the Cabinet Chief's Office; Patricio Seoane and Mónica Abalo, representatives of the Database Chamber (CABASE). At the same time, another expert, Dr. Ricardo Oscar Sáenz, Chief Prosecutor at the Criminal and Correctional Appeals Court of the City of Buenos Aires and chief prosecutor in charge of the committee that analyzes all issues related to the investigation and prosecution of computer and high technology crimes within the orbit of the Public Prosecutor's Office, contributed his expertise and assisted the subcommittee.

In the course of three months, all initiatives related to this issue were analyzed, namely 5.084-D.-06, Lovaglio Saravia, Irrazábal and Perié; 3.873-D.-06, Ritondo; 3.326-D.06, Nemirovsci and others; 3.194-D.-06, Solanas and others; 3.109-D.-06; Pérez (A.) and others; 3.001-D.-06, Canevarolo; 2.991-D.06, Conti and Rossi; 2.981-D.06, Gioja and Uñac; 2.032-D.-06, Bisutti and others; 1.798-D.-05, Martínez (S.V.) (m.c.); 1.225-D.-05, Osorio; 985-D.-05, Zottos.

Furthermore, foreign legislation was also analyzed. In this sense, we consider it is necessary to mention most European countries have reformed their legislation (as recommended by the Council of Europe), in order to include the protection of criminal law over computer systems and data. This trend can also be noticed in the penal legislation of both North and South American countries.

It should be remarked that this initiative is the result of a long process that implied the watchful reflection over the issues related to this type of crimes, the permanent search for agreement and the participation of both public and private sectors with an interest in the subject, all of which is reflected in the broad support received by this bill.

After a profound analysis, we have thought it convenient to give our favorable opinion in support of this bill.

Oswaldo M. Nemirovsci

(Sigue, bajo el encabezado "Antecedente", el texto del proyecto de ley ya incluido y traducido arriba como parte del dictamen de las comisiones)