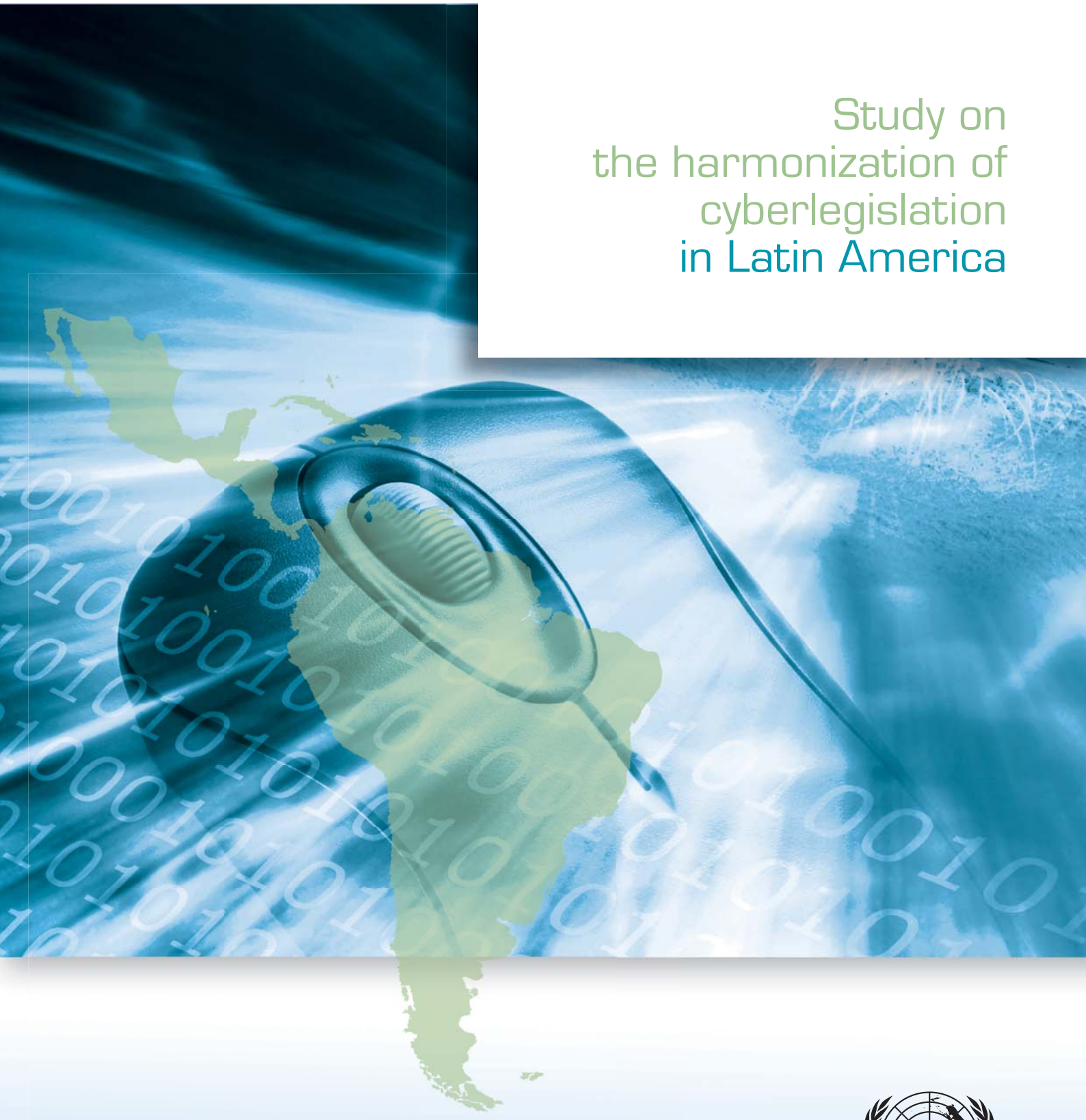
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Study on the harmonization of cyberlegislation in Latin America



UNITED NATIONS

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Study on the harmonization of cyberlegislation in Latin America

UNITED NATIONS

New York and Geneva, 2016

NOTE

Symbols of United Nations documents are composed of capital letters with figures. Mention of such a symbol indicates a reference to a United Nations document.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

This publication was submitted for external editing.

UNCTAD/DTL/STICT/2015/4
UNITED NATIONS PUBLICATION

ACKNOWLEDGEMENTS

This study was prepared as part of the work of the Science and Technology and Information and Communication Technology Branch and the TrainForTrade Programme of the Division of Technology and Logistics of the United Nations Conference on Trade and Development (UNCTAD).

It was prepared under the supervision of the UNCTAD team comprised of Gonzalo Ayala Borda, Cécile Barayre and María Luz Jaureguiberry. The chief consultant in charge of drafting the study was Mr. Jorge Navarro Isla. We are grateful for the contributions made by participants in the training course on the legal aspects of e-commerce for Latin America and the Caribbean, held in June 2014, and in particular participants in the regional workshop on harmonization of cyberlegislation for e-commerce in Latin America and the Caribbean, which was held in Guayaquil, Ecuador, in September 2014: Analía Aspis, Angelique Codd, Carlos Fernando Escobar Revollo, Nicolás Schubert, Paola Andrea Arango Henao, Salomé Vega Morera, Madelyn Rodríguez Lara, Hernán Gustavo González López, Salomón Eduardo Custodio González, Aracely Amaya Fabian, Elide Gina Tassy Cherubin, Karina Elizabeth Aquino Valle, Peter Bailey, Jonathan López Torres, Idelvia María Campos Urbina, Rafael Jesús Quintero Yau, María Luján Ojeda Chamorro, Katia Janeth Núñez Portal de Vásquez, María Elena Ferrer Lovera, Sara Patnella, Julissa Cruz and Julio Enrique Nieto Conde.

Important contributions were also made by Adrián Carballo, Alfredo Reyes Krafft, Erick Rincón, Karina Medinaceli, Moisés Fraguela, Natalia Enciso, Olga Cavalli, Patricia Stanley, Belisario Contreras, Rudy Orjales, Eduardo Pizarro, Gloria Cañas, Silvia Hernández, Fiorella Niro, Gabriela Slack, Rocío Martínez Houssay, Iván Rivadeneyra, Leonardo Otatti and Carlos Vera Quintana.

The cover was designed by Nadège Hadjémian. Ion Dinca was in charge of electronic formatting, and Caridad Ríos prepared the text for publication.

UNCTAD is grateful for the financial support provided by the Government of Finland.

FOREWORD

With the evolution of information and communications technologies (ICTs) and in particular developments in the use of mobile devices and the development of cloud computing and big data, security issues such as data security, cybercrime and consumer protection are essential to gaining the trust of users in e-commerce. The actors involved in designing and implementing public policies are faced with challenges relating to legislation, technical and administrative matters, implementation and harmonization peculiar to the dynamics of their own countries and of the region as a whole.

The purpose of this publication is to provide up-to-date information on the legal framework of the countries in the region as follow-up to the studies on prospects for harmonizing cyberlegislation in Latin America and in Central America and the Caribbean that were published in 2009 and 2010. This study reports on progress made by the countries in regard to electronic transactions/electronic signatures, online protection of consumers, protection of personal data, industrial and intellectual property, domain names, cybercrime and security of information, and pending legislation and challenges. The situation in 20 countries of the region is reviewed, and information is provided on the commitments and responsibilities assumed by the individual countries in regard to cyberlegislation, bearing in mind the regional context, so as to identify the collaborating agencies and the implications, limitations and challenges involved. Reference is made to the many agencies in the region that have generated a wide range of legal instruments and public policies and the need for coordination within the governments of the countries so as to promote progress in this regard. This study can be useful to government personnel involved in designing and implementing legislation that will foster development.

Since 2003, the United Nations Conference on Trade and Development (UNCTAD) has been active in cooperating and providing technical assistance to Governments of developing countries in Africa, Asia and Latin America, with the aim of contributing to the development of legislation to regulate the use of ICTs. UNCTAD delivers training on legal aspects of ICTs, along with support for the creation of a harmonized legal framework to promote the development of an environment that will be conducive to ICT use in the developing countries. Thus, since 2007, UNCTAD has carried out several joint activities with the General Secretariat of the Latin American Integration Association, with the Latin American Economic System and, since 2014, with the Association of Caribbean States in order to strengthen the capacities of the countries concerned, share their regulatory experiences and encourage the formation of multidisciplinary and specialized working groups on the legal aspects of e-commerce.

CONTENTS

I. INTRODUCTION

The reform of cyberlegislation is key to strengthening the economic development of individual countries and of the region as a whole. It also helps to promote national and cross-border trade, including for agencies at the different levels of government, as well as for corporations and individual entrepreneurs, consumers and citizens.

In Latin America, business-to-consumer (B2C) e-commerce has increased over the last decade, from US$ 1.6 billion to US$ 70 billion, yet from the global standpoint, the region still plays a minor role.[1]

As shown in table 1, the United Nations Conference on Trade and Development (UNCTAD) B2C e-Commerce Index,[2] which reflects the underlying capacity of countries to carry out B2C e-commerce, Chile, Uruguay and Brazil rank at the top of the region, with Chile in first place for Latin America and thirty-ninth worldwide.

Table 1. UNCTAD B2C e-Commerce Index 2015

Economy	Share of population having mail delivered at home (2012 or latest, per cent)	Share of individuals with credit cards (15+, 2011, per cent)	Share of individuals using Internet (2013 or latest, per cent)	Secure servers per 1million people (normalized, 2013)	UNCTAD e-Commerce Index value	Rank
Chile	94	22.8	61.4	73.9	63.0	39
Uruguay	93	27.1	58.0	72.1	62.5	40
Brazil	81	29.2	58.0	69.9	59.5	47
Argentina	93	21.9	54.1	67.6	59.1	48
Costa Rica	98	12.2	47.5	72.5	57.6	52
Dominican Republic	99	12.2	45.0	61.5	54.5	57
Mexico	91	13.0	43.5	63.7	52.8	60
Bolivarian Republic of Venezuela	93	10.4	44.1	56.6	51.0	63
Colombia	60	10.2	51.27	65.6	46.9	71
El Salvador	95	5.3	25.5	60.9	46.7	72
Ecuador	68	10.2	35.1	63.0	44.1	76
Guatemala	95	6.9	16.0	58.1	44.0	77
Peru	56	10.0	38.2	61.9	41.5	82
Panama	25	10.7	45.2	73.5	38.6	84
Honduras	75	5.3	18.1	55.1	38.4	85
Nicaragua	44	2.5	13.5	54.4	28.6	98
Plurinational State of Bolivia	19	4.1	34.2	54.9	28.1	99
Haiti	40	1.8	9.8	37.7	22.3	107

Source: UNCTAD, 2015.

Cyberlegislation fosters the conditions necessary to achieve a secure and reliable environment characterized by transparency, respect for privacy, protection of data, legal security, freedom of expression and freedom of consumption and of enterprise. While it is true that the different countries of the region have undertaken reforms in their cyberlegislation on e-commerce, it is also true that the region as a whole has not given priority to that effort; as a result, there are disparities in the legislative development of different countries.

This publication was undertaken to update the previous studies on prospects for harmonizing

[1] eMarketer, 2014.

[2] UNCTAD Information Economy Report 2015. The Index includes information on 130 countries; it has no information on Cuba.

cyberlegislation in Latin America (2009)[3] and in Central America and the Caribbean[4] in the following categories: (a) electronic transactions/electronic signatures,[5] (b) consumer protection, (c) protection of personal data, (d) industrial and intellectual property, (e) domain names, (f) cybercrime and information security,[6] and (g) pending legislation and challenges.

The studies were prepared to provide a regional overview of the status of cyberlegislation in the member countries of the Latin American Integration Association (ALADI) and of the Central American subregion, the Latin American Economic System (SELA) and the Association of Caribbean States (ACS), which participated actively in the different training programmes offered by UNCTAD from 2007 to 2014.

Both studies highlight the existence of many different international organizations (multilateral as well as regional and subregional) that have generated a broad range of legislative instruments and public policies. This has resulted in a complex set of regulations under which the same country may be required to comply with provisions issued by different agencies, creating (i) tensions arising from the incompatibility of some of the regulatory bodies, (ii) disparate development of regulations, laws and public policies, (iii) duplication of efforts, (iv) lack of leadership and coordination among international agencies, and (v) lack of coordination within the national governments.

Table 2. Status of cyberlegislation in the countries of Latin America, 2015[7]

Country	Electronic transactions/ electronic signatures	Consumer protection	Protection of personal data	Intellectual property	Domain names	Cybercrime and information security
Argentina						
Plurinational State of Bolivia						
Brazil						
Chile						
Colombia						
Costa Rica						
Cuba						
Ecuador						
El Salvador						
Guatemala						
Haiti						
Honduras						
Mexico						
Nicaragua						
Panama						
Paraguay						
Peru						
Dominican Republic						
Uruguay						
Bolivarian Republic of Venezuela						

Source: UNCTAD, 2015.

[3] See http://unctad.org/es/docs/webdtlktcd20091_sp.pdf.
[4] See http://unctad.org/es/docs/dtlstict20093_sp.pdf.
[5] In order to simplify the presentation of results, the category of "electronic transactions/electronic signatures" includes the following categories from previous studies: "electronic transactions", "electronic signatures" and "taxes and customs".
[6] Bearing in mind the importance of the issue, the category "information security" was added to the category on "cybercrime"; thus, the two concepts are now included in a single category, "cybercrime and security of information".

A. STATUS OF CYBERLEGISLATION IN THE LATIN AMERICAN COUNTRIES

Table 2 shows the progress made in the countries of the region through the regulatory framework de-

[7] Table 2 does not include pending legislation or draft bills and/or regulations.

Normative Values:

Value	Item	Description
	Facilitates e-commerce	The legislation is in line with international best practices adopted by international organizations, such as the United Nations Commission for International Trade Law, the World Intellectual Property Organization, the World Trade Organization, the International Telecommunications Union, the Ibero-American Data Protection Network, the Inter-American Committee against Terrorism of the Organization of American States, the Council of Europe and the Organization for Economic Cooperation and Development.
	Partially facilitates e-commerce	There is some legislation on the subject, but it is not consistent with international best practices. It needs to be brought in line with normative standards.
	There is no legislation	

scribed later on. The most notable progress has been made primarily in the areas of electronic transactions/electronic signatures and of protection of personal data. Progress has been slower in the areas of cybercrime and information security and, to a lesser extent, in regard to domain names and consumer protection.

ELECTRONIC TRANSACTIONS/ELECTRONIC SIGNATURES

Most countries in the region have adopted standards for electronic transactions/electronic signatures. Nineteen countries already have legislation on the matter, and 16 have incorporated provisions that are consistent with the Model Law on Electronic Commerce and the Model Law on Electronic Signatures adopted by the United Nations Commission for International Trade Law (UNCITRAL). Three countries do not apply the model laws, and one country has no legislation on the matter.

Under the ALADI Digital Certificate of Origin project, Argentina, Bolivia, Brazil, Chile, Cuba, Colombia, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay and Venezuela have made considerable progress in the management of digital certificates of origin for cross-border trade.

Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, Nicaragua and Panama have made significant progress at the subregional level with implementation of the Unified Central American Customs Code (CAUCA) and the regulations thereto, as well as through the signing of the Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR).

As regards the Southern Common Market (MERCOSUR), its resolution No. 37/06 recognizes the legal validity of electronic documents, electronic signatures and advanced electronic signatures within the MERCOSUR region. Resolution 34/06 provides guidelines for mutual recognition agreements on advanced electronic signatures within MERCOSUR. These resolutions have made it possible for electronic customs transactions to be carried out in Argentina, Brazil, Paraguay, Uruguay, Venezuela and Bolivia. Similarly, pursuant to decision 571, on the customs value of goods introduced into the customs territory of the Andean Community, Bolivia, Colombia, Ecuador and Peru have promoted the use of digital signatures in electronic customs declarations in the member countries.

CONSUMER PROTECTION

Eighteen countries have enacted legislation on consumer protection; 11 of those countries have implemented United Nations General Assembly resolution 39/248 on guidelines for consumer protection, while two of them have no laws on the subject nor has any such legislation been proposed.

MERCOSUR resolution 21/04, on consumers' right to information in commercial transactions made over the Internet, resolution 45/06, on consumer protection and deceptive advertising, decree No. 10/96, on the Santa María Protocol, and resolution 10/96, on international jurisdiction in matters of consumer relations, have facilitated the harmonization of legislation on these matters in Argentina, Brazil, Paraguay, Uruguay, Venezuela and Bolivia.

In the area of self-regulation, a number of national associations and chambers of commerce have developed codes of conduct and seal-of-trust schemes for e-commerce (see box 1). The participation of the Central American countries in the CAFTA-DR Agreement and the United States-Panama Trade Promotion Agreement have made it possible to encourage the adoption of this type of mechanisms.

Box 1. The eConfianza and eResolución initiatives of the e-Commerce Latin American Institute

The eConfianza initiative of the e-Commerce Latin American Institute (eInstituto) has been added to the efforts of the Argentine Chamber of e-Commerce, the Chamber of Commerce of Santiago, the Venezuelan Chamber of e-Commerce, the Brazilian Chamber of e-Commerce, the Mexican Internet Association, the Paraguayan Chamber of e-Commerce, the Peruvian Chamber of e-Commerce, the Dominican Chamber of e-Commerce Inc., the Chamber of Commerce of Lima, the Colombian Chamber of e-Commerce, the Chamber of Commerce of Guayaquil and the Ecuadorian e-Commerce Corporation, all of which have a system providing for mutual recognition of seals of trust.

Both the eConfianza Seal of Trust and the Mexican Internet Association Seal of Trust participate in the World Trustmark Alliance, which is comprised of seal-of-trust schemes in 12 Asian countries, 6 European countries and TRUSTe in the United States.

Through its eResolución initiative, e-Instituto is developing a pilot programme on online dispute resolution in eConfianza (for disputes arising from e-commerce and e-business) under which eConfianza would serve as a neutral online third party. The idea is to encourage positive online experiences so as to allow for the growth and strengthening of the digital economy in the region.[8]

Source: eInstituto, 2014.

Some countries, such as Mexico and Chile, had already included in their domestic legislation the Organization for Economic Cooperation and Development (OECD) Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) and the OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders. They had also participated in the Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder project.

PROTECTION OF PERSONAL DATA

Most countries have adopted laws on protection of personal data. Nineteen countries have already enacted laws, and 10 countries follow the guidelines developed by the Ibero-American Data Protection Network. One country does not have any legislation or proposals on the matter.

INTELLECTUAL PROPERTY

As regards intellectual property, all the countries have signed most of the treaties administered by the World Intellectual Property Organization (WIPO), and only two have not signed the Internet treaties.

Chile has taken an important step with the adoption of Act No. 20,435, amending the Intellectual Property Act (Act No. 17,336), which for the first time in the region includes "safe harbour" provisions solely for copyright issues. The Act provides for a "notice and takedown" procedure and includes a section outlining the summary judicial proceedings to be followed in requesting that materials which violate copyright be taken down. Likewise, Costa Rica has included in Decree No. 36880-COMEX-JP, on regulations on the limitation of liability of service providers for infringement of copyright and related rights, a scheme of exclusions from liability for service providers. In Paraguay, the e-Commerce Act (Act No. 4,868/13) incorporates a regime for excluding providers of intermediation services, data storage, links and temporary copies from liability.

The Beijing Treaty on Audiovisual Performances (2012) administered by WIPO[9] represents one of the most significant developments on the international scene, owing to its widespread acceptance by the States of the region. It has been signed by Chile, Colombia, Costa Rica, El Salvador, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua and Peru. It will only enter into force, however, three months after 30 parties that are eligible under the terms of article 23 have deposited their instruments of ratification or accession.

DOMAIN NAMES

As far as domain names are concerned, the national registrars of 18 countries have adopted dispute-resolution rules; 12 of those countries have adopted the principles of the Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN); and 1 country does not have any legislation on the matter.

The dispute-settlement procedures applied by the Haitian Network Information Centre (NIC) do not follow

[8] See http://www.einstituto.org/site/iniciativas/eresolucion/.

[9] See http://www.wipo.int/treaties/en/text.jsp?file_id=295839.

the ICANN Uniform Domain-Name Dispute-Resolution Policy.

Coordination of the region's Internet registration authorities by the Latin American and Caribbean Addresses Registry, under the global oversight of ICANN, is one of the cornerstones of Internet development in Latin America, Central America and the Caribbean. The adoption of the ICANN Uniform Domain-Name Dispute-Resolution Policy is of paramount importance in ensuring that Internet registration authorities use uniform criteria throughout the region.

As regards domain names, NIC Argentina, NIC Chile, NIC Mexico, NIC Peru and NIC Venezuela have adopted the ICANN Uniform Domain-Name Dispute-Resolution Policy as part of their own policies, and they recognize the WIPO Arbitration and Mediation Centre's arbitration procedure. In Peru, the Cybertribunal serves as the official arbitration venue. NIC Paraguay deals with domain-name disputes through extrajudicial mechanisms under Act No. 1878/02, on arbitration and mediation.

In addition, the CAFTA-DR Agreement requires its member countries to create mechanisms for combating cyberpiracy by implementing procedures based on the principles of the ICANN Uniform Domain-Name Dispute-Resolution Policy. The dispute-resolution procedures used by the NICs of Costa Rica, El Salvador, Honduras and the Dominican Republic diverge from the ICANN Uniform Domain-Name Dispute-Resolution Policy. This could hinder the development of cross-border business in the region.

CYBERCRIME

On the matter of cybercrime, two countries have signed the Council of Europe's Convention on Cybercrime and have amended their substantive and procedural legislation to bring it in line with the Convention. Seventeen countries have passed laws defining certain cybercrimes, while one country has no such legislation. With regard to information security, 13 countries have set up computer security incident response teams and have adopted the recommendations of the Organization of American States (OAS) Inter-American Committee against Terrorism.[10]

At the subregional level, the Union of South American Nations (UNASUR)[11] has been working on annual plans of action of the South American Defense Council.[12] Thus, it has set up a working group to assess the feasibility of establishing regional policies and mechanisms for dealing with cyberthreats in the field of defence. In 2013, the working group carried out a regional seminar on cyberdefence with a view to generating capacities for addressing cyberthreats in the area of defence. The South American Infrastructure and Planning Council and the MERCOSUR Working Group on Telecommunications participated in the seminar.

In 2014, the Conference of Ministers of Justice of Ibero-American Countries[13] signed the Ibero-American Cooperation Agreement on Research, Underwriting and Obtaining Evidence on Cybercrime, the purpose of which is to strengthen mutual cooperation among the parties in connection with the adoption of measures for underwriting and obtaining evidence in the fight against cybercrime. The Conference also issued a recommendation on the definition and punishment of cybercrime. These instruments have been signed by Mexico, Guatemala, Nicaragua, Portugal, Peru and Uruguay, as well as by Argentina.

The aforementioned instruments represent the most important advances made by the region in addressing the issue of cybercrime. Considering that the criminal legislation of the Ibero-American countries has serious shortcomings in terms of the definition of cybercrimes and that this makes it possible for both individual and organized criminals to harm or seriously jeopardize essential juridical goods, and desiring to establish minimum common criteria for preventing and combatting cybercrime, without diminishing the importance of the advances made in the countries' legal frameworks and the international commitments of individual States, the Conference of Ministers of Justice of the Ibero-American Countries have recommended the harmonization, within the context of their national policies, of the substantive criminal laws defining the behaviours described below, with a view

10 http://www.oas.org/en/sms/cicte/documents.asp

11 UNASUR is an international organization made up of the 12 countries of the South American region, namely, Argentina, Bolivia, Brazil, Colombia, Chile, Ecuador, Guyana, Paraguay, Peru, Suriname, Uruguay and Venezuela. The objective of UNASUR is to develop opportunities for integration in the cultural, economic, social and political spheres while respecting the specific circumstances of each country.

12 See the Action Plan 2012 of the South American Defense Council: http://www.ceedcds.org.ar/English/09-Downloads/Eng-PA/ENG-Plan-de-Accion-2012.pdf; the Action Plan 2013 of the South American Defense Council: http://www.ceedcds.org.ar/English/09-Downloads/Eng-PA/ENG-Plan-de-Accion-2013.pdf and the Action Plan 2014 of the South American Defense Council: http://www.ceedcds.org.ar/English/09-Downloads/Eng-PA/ENG-Plan-de-Accion/Plan-de-Accion-2014.pdf

13 The Conference of Ministers of Justice of Ibero-American Countries is comprised of the ministries of justice and similar institutions of Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Portugal, Spain, Uruguay and Venezuela. See http://www.comjib.org/documentos

to achieving greater effectiveness in the prevention, prosecution and punishment of those behaviours so as to facilitate judicial cooperation among the different countries and try to prevent the existence of opportunities for impunity. The Agreement is compatible with other international instruments such as the Council of Europe's Convention on Cybercrime.

Special mention should be made of Special Declaration 15: On Internet Governance,[14] which was adopted at the Third Summit of the Community of Latin American and Caribbean States,[15] held in Belén, Costa Rica, in January 2015. In that text, the Heads of State and Government of the 33 States in the region resolved (i) to build regional networks of knowledge in Latin America and the Caribbean;[16] (ii) to strongly condemn the actions of espionage and indiscriminate massive and global monitoring among countries by State and non-State actors, demanding absolute obedience to the rules of international law, in relation to respect for State sovereignty and human rights, especially privacy;[17] and (iii) to promote actions and strategies to strengthen cybersecurity and prevent cybercrime, and in particular, create mechanisms for the eradication of cyberwar and promoting the Internet as a space of peace.[18]

B. A MULTIPLICITY OF INITIATIVES FOR PROMOTING INTERNATIONAL COMMERCIAL TRANSACTIONS IN THE REGION

The legal framework for e-commerce and the reform of cyberlegislation have been on the digital agendas of several countries in the region whose legislation is the subject of this study. Several countries of the region have regulations governing online commercial transactions based on the use of a public key infrastructure and digital certificates to foster the interoperability of platforms in a secure context, including through cloud technology, and provide economies of scale.

Both the study on prospects for harmonizing cyberlegislation in Latin America (2009) and the study on prospects for harmonizing cyberlegislation in Central America and the Caribbean (2010) stress the importance of the Regional Action Plan for the Information Society in Latin America and the Caribbean in 2008 and 2010 (eLAC 2010 and eLAC 2015), which represent some of the most significant advances made in the region. The Economic Commission for Latin America and the Caribbean (ECLAC) serves as the Technical Secretariat for these action plans. Most of the countries have established common regional goals which have played a part in the development of e-commerce and e-government through the adoption of digital signature and certification mechanisms, as well as implementation of the single window concept. These measures have proved to be compatible across the different divisions of individual states or of different states in the region.

Several states have proposed digital agendas featuring the use of ICTs as catalysts for development and social inclusion. These technologies should play a fundamental role in the relationship between government and the governed, and they have been explicitly integrated into the digital agendas and national e-commerce strategies of countries such as the Dominican Republic, Mexico, Paraguay and Peru.

In August 2015, at the Fifth Ministerial Conference on the Information Society in Latin America and the Caribbean, the countries of the region adopted the Digital Agenda for Latin America and the Caribbean. Under the Digital Agenda, States undertake to promote innovation and competitiveness by strengthening the digital economy. An objective of this new Digital Agenda is to strengthen the digital economy and e-commerce, adapting consumer protection regulations to the digital environment and coordinating aspects related to taxes, logistics and transportation, electronic payment mechanisms and personal data protection, and providing legal certainty to promote investment in the digital ecosystem.

Initiatives for international commercial transactions in the region include the ALADI project on a digital certificate of origin, which involves the participation of Argentina, Bolivia, Brazil, Chile, Colombia, Cuba, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay

[14] Available at: http://www.celac2015.go.cr/special-declaration-15-of-the-community-of-latin-american-and-caribbean-states-on-internet-gobernance-process/

[15] The Community of Latin American and Caribbean States (CELAC) is an intergovernmental mechanism for dialogue and political agreement whose permanent members are 33 countries of Latin America and the Caribbean, as follows: Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Surinam, Trinidad and Tobago, Uruguay and Venezuela. Source: http://www.celacinternational.org/.

[16] Operative paragraph 10 of Special Declaration 15: On Internet Governance.

[17] Operative paragraph 2 of Special Declaration 15: On Internet Governance.

[18] Operative paragraph 3 of Special Declaration 15: On Internet Governance.

and Venezuela. The project has helped facilitate cross-border trade through the use of electronic media, especially through the integration and harmonization of standards, formats and platforms, allowing for interoperability of the customs systems in the different countries.

The adoption by member States of the technical specifications and general procedures for the digital certificate of origin issued by the General Secretariat of ALADI in 2014 will be especially important for the economic integration of the region, which also relies heavily on bilateral agreements[19] (see box 2).

Box 2. Digital certificate of origin in ALADI[20]

In the context of ALADI, the digital certificate of origin (DCO) consists of a set of specifications, standards and technical procedures that provide the basis for an IT infrastructure consisting of applications and electronic documents that make it possible to recognize DCOs in the context of ALADI. A description of the aforementioned specifications, standards and technical procedures makes up the main content of this document.

The main applications that make up the DCO are (i) those pertaining to the receipt of requests for and issuance of DCOs of eligible entities; (ii) those used by customs to receive and validate DCOs in the importing country, and (iii) the computerized DCO System of ALADI.

i. The applications used to receive requests for and issue DCOs for eligible entities should allow for the DCO request to be signed electronically by the exporter or his or her legal representative. To that end, the exporter or his or her legal representative must previously obtain a digital identification certificate (digital ID) from the competent certification authority. This process will produce an XML (eXtensible Markup Language) file containing the information required for processing the request for the DCO, in accordance with the origin regime specified in the relevant agreement.

In that regard, the eligible entity must provide the necessary IT infrastructure for receiving and processing the DCO request, validating the digital signature of the exporter or his or her legal representative, digitally signing the new XML file which constitutes the DCO and issuing it in accordance with the terms of the relevant origin regime.

ii. Customs houses must adapt their IT systems to allow for the receipt and validation of DCOs. The validation process will entail sending automatic requests for the DCO information to the automated DCO system.

iii. The ALADI DCO system is a web application that is mainly designed to administer a secure directory of digital IDs of staff who are qualified to sign DCOs while at the same time making it possible to ascertain from customs authorities whether information on qualified staff and their digital IDs is current when validating DCOs at the time of the importation.

The main electronic documents of the DCO are: the DCO, the digital IDs of qualified staff and of users of the DCO system, which make up the electronic identification documents of users of the DCO system and of qualified staff; a description of the mechanisms used for the electronic exchange of information, i.e., the web services and the exchange files of the secure directory of the DCO system.

Source: ALADI.

[19] See the final report of the second meeting of national coordinators for the digital certificate of origin at http://www.aladi.org/nsfaladi/reuniones.nsf/documentos/$file/InformeFinalCOD2014.pdf (available only in Spanish). With regard to the importance of bilateral agreements, section 3, on overview and follow-up to horizontal technical cooperation projects between buyer and seller countries concerning implementation of the programme on cooperation for implementation of DCOs in member countries of ALADI, states that the presiding officers of the meeting have encouraged countries to continue making progress in horizontal cooperation in order to achieve implementation of the digital certificate of origin as soon as possible, and to that effect, it would provide opportunities for bilateral meetings. Likewise, in section 4, on bilateral coordination meetings to facilitate implementation of cooperation projects, the report states that 23 bilateral meetings were held among the countries present, and the results of those meetings are reflected in section 5, on presentation of the results of bilateral meetings for the purpose of updating document ALADI /SEC/dt 536, of 8 November 2013, entitled Instrumentación del Programa de Cooperación para la implementación del COD en los países miembros de la ALADI.

[20] See Certificación de Origen Digital de la ALADI – Especificaciones Técnicas y Procedimientos Generales at http://foros.aladi.org/gtah/ALADI_SEC_di2327rev2.pdf

Table 3. ALADI digital certificate of origin (DCO) implementation matrix*

Country	1		2		3		4		5		6	7
	Development of platform for issuing DCOs (eligible entities)		Development of platform for receiving DCOs		Official registration in the test DCO system		Internal approval (validation of the DCO signature in the DCO system)		External approval (validation of the DCO signature in the DCO system)		Official registration in production DCO system	Production (validation of the DCO signature in the DCO system)
	In process	Completed	In process	Completed	In process	Completed	In process	Completed	In process	Completed		
Argentina		X		X		X		X	X		X	
Plurinational State of Bolivia	X											
Brazil		X		X		X		X	X		X	
Chile		X	X		X	X						
Colombia		X	X			X	X		X		X	
Cuba	X		X									
Ecuador	X		X		X							
Mexico	X		X		X							
Panama	X		X									
Paraguay	X		X									
Peru (**)												
Uruguay		X		X	X		X	X				
Bolivarian Republic of Venezuela												

* Matrix showing the status of implementation of DCO (version 1.8.0) in member countries of ALADI, based on the provisions of resolution 386 of the Committee of Representatives.
** Peru does not currently have a proposal for adjustment of the DCO system.

Source: ALADI – 2015.

Table 3 describes the status of implementation of the latest version of the ALADI digital certificate of origin.

SELA, for its part, has also promoted the Single Window for Foreign Trade in the region. This system has benefited different economies in Latin America, Central America and the Caribbean (see table 4).

Around 52 per cent of the countries in the region have used this tool to some degree. The level of im-

Table 4. Development of the Single Window for Foreign Trade in Latin America and the Caribbean (2014)

Country	Exports	Imports	In development
Argentina	-	-	X
Brazil	X	X	
Chile	X	-	X – in development. Incorporation of services: to supplement exports and initiate imports
Colombia	X	X	Constant improvement: inclusion of other services, in addition to exports and imports
Costa Rica	X	-	X – Incorporation of services: imports
Ecuador	X	X	
El Salvador	X	-	X – Incorporation of services: imports
Guatemala	X	-	
Honduras	-	-	X
Mexico	X	X	Constant improvement: inclusion of other services
Nicaragua	-	-	X
Panama	X	-	X: in development. Incorporation of services: to supplement exports and initiate imports
Paraguay	X	-	-
Peru	X	X	Constant improvement: inclusion of other services in addition to exports and imports
Dominican Republic	-	-	X
Trinidad and Tobago	X	X	X – in development. Incorporation of other services: imports
Uruguay	X	X	X – supplementing exports and imports

Source: SELA 2015.

plementation and maturity of the system ranges from countries such as Colombia, which has had an operational Single Window for Foreign Trade in place since the mid-2000s, to Argentina, which recently started applying it, and Nicaragua, which has begun to develop it. The information provided in the table above was provided directly by countries of the region in which SELA maintains a permanent presence in regard to trade facilitation and in particular to development of the Single Window for Foreign Trade.

SELA has played an important role in fostering regional dialogue through the annual Latin American and Caribbean regional meetings on single windows for international trade.[21] These regional meetings have become especially important for disseminating information and best practices within the Latin American and Caribbean region and for learning from the progress made in other regions. This has undoubtedly helped to encourage implementation and development of Single Windows for Foreign Trade in the countries of the region.

In addition, the Permanent Secretariat of SELA has contributed to the considerable development of the intellectual production and systematization of the documentation on the Single Window for Foreign Trade and to paperless cross-border trade, through the Scenario for Digitalization of Foreign Trade Procedures in Latin America and the Caribbean (SELA, 2010)[22] and the Pilot Project for Interoperability and Harmonization of Single Windows for Foreign Trade[23] within the framework of the Latin American Pacific Rim, which was developed in 2012 under a cooperation agreement between the Andean Development Corporation, the Development Bank of Latin America and SELA. The project also includes specific documents on digital signatures and e-commerce.

Since 2014, also in the framework of a cooperation agreement with the Andean Development Corporation, progress was made in a programme for creation of the Latin American and Caribbean Network of Digital and Collaborative Ports which involves not only digitizing port procedures, operational aspects of services synchronization, elements of governance and quality standards, but also ensuring the interoperability of the Single Window for Foreign Trade and the Port Single Window. The Permanent Secretariat of SELA contributes by implementing, developing and consolidating the Single Window for Foreign Trade in Latin America and the Caribbean as a key component of trade facilitation, with a view to helping the countries of the region improve their competitiveness and sustainability so as to achieve greater and more efficient insertion in an increasingly globalized international trade system.

Likewise, MERCOSUR and the Central American Integration System have promoted e-commerce in their respective subregions and are working to achieve greater integration among the different agencies concerned, in order to further harmonize legislation on the subject.

To facilitate cross-border e-commerce, it is especially important that those countries that have not yet done so incorporate the UNCITRAL treaties on e-commerce into their legislation, in particular the United Nations Convention on the Use of Electronic Communications in International Contracts.

Self-regulation schemes and online alternative dispute-resolution mechanisms are viable and efficient options for protecting consumer interests, whether they are supported by robust legal frameworks or by less developed ones. There has been an increase, albeit modest, in the use of regional seals of trust, which can help encourage the development of e-commerce. The regional eConfianza programme of eInstituto and the Argentine Chamber of e-Commerce combines the regional efforts of 12 e-commerce chambers and associations and includes a standard of best practices that facilitate the adoption, use and mutual recognition of seals of trust and codes of best practices in Latin America.[24]

The adoption of data protection laws that comply with the parameters set in the guidelines of the Ibero-American Data Protection Network will go a long way towards increasing trust among online consumers. In addition, States should ratify the Council of Europe's Convention on Cybercrime and the Ibero-American Cooperation Agreement on Research, Underwriting and Obtaining Evidence on Cybercrime and adopt the recommendation of the Conference of Ministers of Justice of Ibero-American Countries on the definition and punishment of cybercrime. The creation of a computer security incident response team according to the terms of the Inter-American Strategy to Combat Threats to Cybersecurity of the OAS Inter-American Committee against Terrorism will go a long way towards consolidating confidence in electronic means.

[21] See the final reports of the meetings at http://www.sela.org.

[22] See http://www.sela.org/media/266219/t023600003963-0-di_3_panorama_digital_tramites_comercio_exterior.pdf .

[23] See https://www.unece.org/fileadmin/DAM/cefact/cf_forums/Geneva_2013/PPTs/11_SWIMethodologyforNationalSingleWindowAlignment.pdf .

[24] See http://www.einstituto.org/site/iniciativas/econfianza/.

II. REPORT ON LEGISLATION IN THE LATIN AMERICAN COUNTRIES

This section discusses the development of legislation in each of the participating countries. A brief analysis is made of legislation in the areas of (a) electronic transactions/electronic signatures, (b) consumer protection, (c) protection of personal data, (d) industrial and intellectual property, (e) domain names, (f) cybercrime and information security, and (g) pending legislation and challenges.

ARGENTINA

Argentina has not adopted specific legislation on contracts made electronically. It does have regulations covering different areas of e-commerce, however, such as the Digital Signature Act (Act No. 25,506), of 11 December 2001, and the Consumer Protection Act (Act No. 24,240), of 13 October 1993 (updated by Act No. 26,994, which entered into force on 1 August 2015), the Civil Code and the Commercial Code and the new Civil and Commercial Code, of 8 October 2014, which will enter into effect on 1 January 2016.

a) Electronic transactions/electronic signatures

The Civil Code governs various issues associated with the formation of contracts and related formalities. It sets forth the principal rules governing offerings to the public, their acceptance, the formation of contracts between parties both of whom are physically present, as well as between parties that are not, and the time at which a contract takes effect.

Under the Commercial Code, indeterminate offers to the public are not binding. To protect consumers, Act No. 24,240 makes offers that are directed to non-specific potential consumers binding on those issuing them over the period of time during which the offer is in force, and parties making offers must provide information regarding the modalities, conditions and limitations surrounding the offers. It also establishes that the specifics offered through advertising shall be binding on the party offering them and that these specifics must be included in the contract made with the consumer.

Act No. 25,506 recognizes the legal validity of electronic documents and signatures and of digital signatures, making handwritten signatures and digital signatures legally equivalent. It also requires that digital documents comply with the requirements applicable to written documents. The law is based on the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, and it is used in both the public and private sectors.

Several of the provinces have made this law applicable to public administration in their jurisdictions. In addition, Argentina has signed and incorporated into its domestic legislation the MERCOSUR regulations on standards for the use of digital signatures (Resolutions GMC 34/06 and 37/06 on electronic and digital signatures).

The Federal Public Revenue Administration has issued general resolutions imposing additional fees for those who carry out e-commerce transactions. General Resolution 3579 requires anyone purchasing merchandise from foreign suppliers that is brought into the country to complete form No. 4550 (Purchases from foreign suppliers) before they retrieve or receive the goods.

General Resolution 3582, which supplements the provisions of General Resolution 3579, provides that individuals purchasing goods from foreign suppliers that enter the country through the official post – including door-to-door service – may use the procedure envisaged in General Resolution 3579 only twice each calendar year, taking into account the annual exemption of US$ 25 envisaged in article 80 (1) (c) of Decree No. 1001/82 and the amendments thereto. Any shipment additional to the aforementioned limit must be processed under the General Import Regulations.

General Resolution 3377 requires taxpayers who sell goods or provide services to end users to exhibit form No. 960/NM – Tax Data, at their retail or service locations, waiting rooms, offices or reception areas, and to display the form 960/NM-Tax Data logo in a visible place on their website along with the hyperlink provided by the Federal Public Revenue Administration.

In the area of public procurement through electronic means, Decree No. 1023/2001 governs the procurement system of the national government, and the related regulations are set forth in Decree No. 1818/2006, which authorizes use of the Government Electronic Procurement System. Administrative Decision No. 6/2007 of the Office of the Chief of the

Cabinet of Ministers sets technical operational standards for the country's digital signature infrastructure.

In connection with cross-border transactions, Argentina is considering signing the United Nations Convention on the Use of Electronic Communications in International Contracts developed by UNCITRAL. It and has already signed the United Nations Convention on Contracts for the International Sale of Goods of 11 April 1980 and the treaties on international civil law (Montevideo Treaties of 1889 and 1949) which establish the law applicable to international contracts.

The new Civil and Commercial Code governs certain aspects of e-commerce. In Book Three, on personal rights, obligations and contracts, Title III, on consumer contracts, includes a section on special types of contracts that covers remote contracts, including those entered into via electronic means. It also stipulates that whenever the Code or a special law requires that a contract be made available in written form, this requirement shall be understood to be met if the contract with the consumer or user is supported by software or a similar technology.

Several articles in the Code allow for the use of "electronic means or mechanisms" for different actions or legal acts, thus recognizing the use of ICTs. With regard to digital signatures, the Code provides that in the case of documents generated electronically, the requirement that they be signed by an individual may be considered met if a digital signature is used which establishes without a doubt the identity of the author and the integrity of the document.

b) Consumer protection

Act No. 24,240 sets forth special requirements for contracts with consumers, who, within five days of the date on which the product is delivered or on which the contract is signed, have the right to opt out without incurring any liability, if procurement of the goods is effected through electronic means. In addition, some sectors have adopted self-regulation measures to protect consumers' rights. These include the Code of Conduct of the Chamber of Commercial Information Firms and the Code of Ethics of the Direct and Interactive Marketing Association.

At the regional level, Argentina has incorporated into its domestic law MERCOSUR Common Market Group (GMC) Resolution No. 21/2004, on consumers' right to information in connection with transactions conducted via the Internet.

At the provincial level, Act No. 2,224 of the Autonomous City of Buenos Aires requires individuals who market or provide online services to consumers or users within the boundaries of the Autonomous City of Buenos Aires must include a link to the Directorate-General for Consumer Protection.

Act No. 2,817 of the Autonomous City of Buenos Aires lays down a number of requirements for suppliers selling goods or services to consumers. With regard to service contracts by electronic or other remote means, the Act provides that the consumer shall be entitled to have clear, comprehensible and unequivocal access to the general terms of the contract and be able to store or print such terms and conditions, and that it must be clearly stated that the contract can be terminated at the discretion of the consumer or user by the same means used to conclude it.

Act No. 863 of the Autonomous City of Buenos Aires provides that commercial establishments that provide Internet access must install and activate filters for pornographic content. In addition, Act No. 26,104, on advertising for tourism, provides that all advertising contained in electronic means which shows show pictures of tourist attractions must meet certain requirements regarding information.

The new Civil and Commercial Code governs consumer contracts and, among other rights, includes the right of consumers to opt out without incurring liability, provided that they do so within 10 days after accepting the offer.

c) Protection of personal data

For the protection of personal data, Act No. 25,326 provides a regime that is aligned with European regulations (Directive 95/46/EC). This Act establishes the National Office for the Protection of Personal Data, an ad hoc entity responsible for monitoring compliance with the Act in various contexts. In 2003, the European Union recognized the country's regulatory framework as being consistent with the standards of the Council of Europe. Decree No. 1,558/2001 lays down regulations for the Act on Protection of Personal Data.

d) Industrial and intellectual property

In the area of intellectual property rights, Argentina has signed the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works

- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Brussels Convention relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

With regard to domain names, at the request of the Ministry for Foreign Affairs, the Public Bar Association of the Federal Capital drew up a set of arbitration regulations relating to domain names. It was proposed that the Bar Association should be in charge of resolving disputes regarding domain names in Argentina, including disputes concerning cases of cybersquatting. In addition, under Resolution No. 20/2014, the NIC.ar platform stopped being administered by the Ministry for Foreign Affairs and came under the aegis of the Legal and Technical Secretariat of the Office of the President.

In February 2014, the practice of registering domain names free of charge was discontinued, and a fee of 160 Argentine pesos was set for the registration procedure.

f) Cybercrime and information security

In terms of criminal law, Act No. 26,388, of 24 June 2008, amending the Criminal Code, defines certain cybercrimes such as intercepting communications, gaining illicit access to computer systems, causing harm to IT systems, fraud, falsifying electronic or IT-based documents, interrupting communications and deleting or altering digital evidence. Other instruments, such as Act No. 25,036, provide sanctions for violating intellectual property rights associated with software, and Act No. 25,506 punishes the offence of forging digital signatures. The National Intelligence Act defines the offence of violating secrecy and improperly intercepting communications.

Regarding security of information, the Office of the Chief of the Cabinet of Ministers issued Decision No. 580/2011, of 28 July 2011, creating the National Programme of Critical Information and Cybersecurity Infrastructures, to operate within the National Office of Information Technologies. By Decision No. 3/2013 of the National Office of Information Technologies, the Security Policy for Model Information was adopted for the national public sector; this decision also provides for the operation of a national computer emergency response team.

At the national level, the Cyberdefence Commando was created by Ministry of Defence Decision No. 343, of 14 May 2014. At the regional level, UNASUR initiatives on the establishment of joint cyberdefence policy were created in 2014.

At the international level, Argentina has adopted the Declaration on Strengthening Cyber-Security in the Americas and the Panama Declaration on Protection of Critical Infrastructure from Emerging Threats, both initiatives of the Inter-American Committee against Terrorism. It should be noted that Argentina is a member of the Conference of Ministers of Justice of Ibero-American Countries.

g) Pending legislation and challenges

Bills that are currently under discussion in the legislature include the preliminary draft law on digital format of legal acts – e-commerce, which was submitted to Congress in August 2000. The Congress is also considering the bill on online commerce, abrogating Decisions Nos. 3579/2014 and 3582/2014 of the Federal Public Revenue Administration.

Among the main challenges it faces, Argentina needs to ensure that the provinces accept Act No. 25,506 and, in the international context, the country needs to adhere to the Council of Europe's Convention on Cybercrime and sign the United Nations Convention on the Use of Electronic Communications in International Contracts developed by UNCITRAL.

BOLIVIA (PLURINATIONAL STATE OF)

The Political Constitution of the Plurinational State of Bolivia of 9 February 2009 recognizes as fundamental rights the right to communication, the right to information and the right to freedom of expression, all of which can be implemented and publicized by means of the new ICTs.

a) Electronic transactions/electronic signatures

In Bolivia, e-commerce is governed by Chapter Four, on e-commerce, of Title IV, on content development and ICT applications, of the General Act on Telecommunications, Information and Communications Technologies (Act No. 164, of 8 August 2011). Chapter Four of Title IV includes articles on the electronic

supply of goods and services, the validity of electronic contracts, valuation and disputes.

Act No. 164 attributes probative legal validity to legal acts or business carried out by individuals or legal entities in digital form and approved by the parties through digital signatures, to electronic data messages and to digital signatures. The Act covers personal and work-related e-mail and electronic advertising communications. Digital documents lacking digital signatures may be admitted as evidence.

Supreme Decree No. 1793, on the regulations to Act No. 164 on telecommunications, information and communications technologies, of 13 November 2013, goes into greater detail on the technical, administrative and legal requirements for electronic signatures, digital signatures, digital certificates, the root certification authority, the certification agency and the registration authority.

Act No. 393, on financial services, of 21 August 2013, also empowers financial institutions to provide services through electronic means, provided security standards are met to guarantee integrity, confidentiality, authentication and non-repudiation. Such transactions and any information contained in and transmitted in the form of electronic data messages shall have the same legal effect and the same probative validity as written documents with handwritten signatures.

The Financial System Supervisory Authority and the Central Bank of Bolivia, each within its own sphere of authority, are empowered to promulgate laws establishing security procedures and standards for transactions, as well as minimum requirements that must be met by entities wishing to carry out online banking and banking by telephone and mobile devices. These standards are obligatory for financial entities that provide such services.

In regard to tax laws, the Tax Code (Act No. 2492), of 2 August 2003, provides that IT devices and printouts of the information contained in them shall constitute legal evidence, in accordance with the regulations issued on the matter. Any electronic medium may be used for invoicing, submission of sworn statements and other tax-related information, withholding, collection and payment of taxes, bookkeeping, records and accounting annotations, as well as documentation on tax obligations and the preservation of such documentation, subject to authorization by the Tax Administration to taxpayers and responsible third parties. This also applies to communications and notifications from the Tax Administration to taxpayers and third-party payers.

Tax regulation No. 10-0049-13, on the virtual invoicing system, of 19 December 2013, establishes the virtual invoicing system within the framework of the Tax System Administration Model. The virtual invoicing system makes considerable use of the Internet in order to modernize, optimize and integrate tax procedures and applications, with a view to providing the National Tax Service with timely and efficient control mechanisms that will enable it to satisfactorily fulfil its purpose and facilitate compliance with tax obligations of taxpayers or third-party payers. Electronic transactions conducted and recorded in the computerized system of the Tax Administration by an authorized user have legal validity.

Tax regulation No. 10-0044-13, of 20 December 2013, issued by the National Tax Service, governs taxes relating to the sale of goods through e-commerce within the national territory. It covers transactions pertaining to the sale of goods through e-commerce that are conducted by individuals or legal entities.

b) Consumer protection

Articles 75 and 76 of the Constitution provide general protection for consumers. In addition, although products and services provided by electronic means are not specifically mentioned in the General Act on the Rights of Users and Consumers (Act No. 453), of 4 December 2013, they may be considered to fall within the scope of application of the Act. The Act governs the right to information and deals with deceptive or abusive advertising. It also requires providers to comply with the terms offered, regulates the content of contracts establishing acceptance and prohibits abusive clauses. It includes provisions on the right to lodge complaints, the granting of service guarantees, the duties of users and consumers and the duties of providers, and it lays down rules on the processing of administrative complaints and on forms of redress, among other provisions.

c) Protection of personal data

With regard to the protection of personal data, the Political Constitution of the Plurinational State of Bolivia establishes the right to bring an action for protection of privacy, whereby the data subject, the legal person or body corporate is entitled to demand compliance with the right to know, challenge, cancel or remove his or her personal data. It also recognizes the fundamental right to personal or family privacy, or to a person's image, honour or reputation. Chapter Four, on action for the protection of privacy, of the Code of Constitutional Procedure of 5 July 2012 outlines the procedure for bringing an action for protection of privacy, without

a prior administrative complaint being necessary owing to the imminence of violation of the protected right; the action is intended as a precautionary measure.

The supreme decree laying down the regulations to Act No. 164, on telecommunications, information and communications technologies, establishes guidelines for the handling of personal data. One of the requirements is that the data subject give his or her express consent. In addition, persons who are asked to provide personal data must be informed in advance that their data will be subject to processing, the purpose for which the data are being collected and recorded, who will be the potential recipients of the information, the identity and domicile of the person responsible for processing the data or of his or her representative, and how to exercise the right to access, correct, update, cancel, challenge or revoke the information or take such other action as may be pertinent.

Likewise, the Tax Code (Act No. 2492), of 2 August 2003, provides that tax returns and individual data obtained by the Tax Administration shall be confidential. Such data may only be used for tax-related purposes or relevant procedures and may not be reported, assigned or communicated to third parties, unless there is a duly justified court order or a request for information under article 70 of the Constitution. Aggregated or general statistical information is public.

In addition, the Financial Services Act (Act No. 393) provides that any individual or body corporate that considers that they have been improperly or illegally prevented from knowing, challenging or obtaining the removal or correction of data recorded by financial entities, using any physical, electronic, magnetic or automated means, in public or private records or databanks, or which affect his or her fundamental right to personal or family privacy, or to his or her image, honour and reputation, may bring an action for protection of privacy, as envisaged in the Constitution.

d) Industrial and intellectual property

In regard to intellectual property, Bolivia has included the protection of computer programs (software) in its Copyright Act (Act No. 1322), of 13 April 1992, and has issued Supreme Decree No. 24582, on regulating computer applications and software, of 25 April 1997. Supreme Decree No. 0667, on the organized text of the Criminal Code, of 8 October 2010, defines offences against intellectual property related to the reproduction, plagiary, distribution, publication, transformation and mass marketing of copyright-protected works without the authorization of the holder of the copyright.

In the international sphere, Bolivia has signed the following instruments on intellectual property:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

With regard to domain names, the country's NIC (.bo) has adopted policies on delegation of domain names under its country code top-level domain name .bo, a policy on resolution of disputes concerning domain names registered under the country code top-level domain name .bo and regulations to the domain-name dispute-resolution policy. Recognized providers of arbitration services are the WIPO Mediation and Arbitration Centre and the Conciliation and Commercial Arbitration Centre of the Bolivian National Chamber of Commerce.

f) Cybercrime and information security

In regard to cybercrime, the Criminal Code adopted by Act No. 1768, of 10 March 1997, defines offences involving manipulation and alteration of ICT systems, improper access and use of cyberdata. The Financial Services Act (Act No. 393) defines a number of offences involving fraud employing electronic means, including misappropriation of funds.

g) Pending legislation and challenges

One of the main challenges faced by Bolivia is the need to adopt general legislation on the issue of personal data in order to meet its commitments in the Ibero-American Data Protection Network. The country's substantive and procedural criminal legislation also needs to be reviewed and brought up to date, bearing in mind the Council of Europe's Convention on Cybercrime and the Ibero-American Cooperation Agreement on Research, Underwriting and Obtaining Evidence on Cybercrime, along with the recommendation of the Conference of Ministers of Justice of Ibero-American Countries on the definition and punishment of cybercrime.

Bolivia must also address the challenge of the digital gap and develop appropriate public policies to promote connectivity and digital capacities.

BRAZIL

Brazil has in place a number of provisions governing different aspects of e-commerce. Several of them are quite recent, such as the e-Commerce Act contained in Decree No. 7,962 and the Civil Framework for the Internet contained in Act No. 12,965, of 23 April 2014, the content of which is described below.

a) Electronic transactions/electronic signatures

The e-Commerce Act enacted by Decree No. 7,962, of 15 March 2013, establishes obligations for anyone involved in online marketing of products and services. The Act focuses on consumer protection, as noted below.

Provisional Measure 2200-2, of 24 August 2001, issued by the President of the Republic, established the Public Key Infrastructure (ICP-Brasil) in order to guarantee the authenticity, integrity and legal validity of electronic documents, applications and support for applications through digital certificates and secure electronic transactions. ICP-Brasil is thus authorized to formulate policies for managing both the certification authorities and the registration authorities. The National Institute for Information Technology, a unit of the Ministry of Science, Technology and Innovation, is also empowered to act as the root certification authority for public keys in Brazil and to carry out supervisory activities, as well as to punish anyone infringing the regulations.

The Provisional Measure recognizes the full legal validity of public or private electronic documents produced under the certification process of ICP-Brasil. It also allows for the use of electronic documents for tax purposes, provided that the requirements of the national Tax Code are met. ICP-Brasil has authority to negotiate and approve bilateral certification agreements, cross-certification agreements, interoperability and other forms of international cooperation.

Act No. 12,682, of 9 July 2012, recognizes the legal validity of digitization, electronic storage and reproduction of public and private electronic, optic or equivalent documents, as well as of the means used to explore conversion of the representation of a digitally coded document. The exploration process must be carried out in order to maintain the integrity, authenticity and, if necessary, the confidentiality of digital documents, and the digital certificate issued in the context of ICP-Brasil must be used. Similarly, the means for communicating digital storage documents must be protected from unauthorized access, use, modification, reproduction or destruction.

In the area of government, the Civil Framework for the Internet provides that Internet applications used by government agencies must seek to ensure (i) that e-government services are compatible with different terminals, operating systems and access applications, and that there is interoperability among the different federal levels and the different sectors of society, and (ii) that e-government services are user-friendly. The adoption of open and free technologies, standards and formats is encouraged, as well as open and structured advertising and dissemination of data and public information.

In addition, Brazil has signed the two MERCOSUR resolutions on standards for the use of digital signatures, i.e., Resolution No. 34/06 and Resolution No. 37/06 on electronic and digital signatures.

b) Consumer protection

The Consumer Protection Code (Act No. 8,078), of 11 September 1990, is the most important legislation in this area. It stipulates that providers may not make performance of contracts with consumers contingent upon their accepting storage or dissemination of their information; any such provision is considered null and void and may be sanctioned by the competent economic authorities. In addition to the civil liability that providers may incur for non-compliance with the Code, they may also be liable to criminal prosecution if they are found to have committed any of the offences envisaged in the Code, i.e., (i) hindering or obstructing access by consumers to any personal information contained in files, databases, formats or records, which is punishable by imprisonment of six months to one year or by a fine, and (ii) failure to immediately correct consumer information that is included in files, databases, formats or records, when the provider is aware or should be aware of such inaccuracy, which is punishable by imprisonment of one to six months or by a fine.

The e-Commerce Act (Decree No. 7,962), of 15 March 2013, sets forth the obligations of providers, such as the duty to provide product information, including a complete description of the characteristics of the product, the terms of the contract and the benefits and advantages of the product, technical data, warnings or instructions for use, available options, guarantees and conditions for returning or exchanging the product. It also requires providers to supply their contact information, such as telephone number, e-mail or a link to a form showing contact information,

the physical address of the company and the procedure for returning the product without liability for the buyer.

The Act also makes it obligatory to provide product information, including price, availability, methods of payment and delivery options. Before the contract is concluded and payment is applied and recorded, the buyer must be given access to the contract he or she is required to accept, as well as to a mechanism for correcting mistakes. The sale contract must include the terms of acceptance, as well as the conditions for exercising the right to opt out without paying a penalty.

The Civil Framework for the Internet is designed to protect consumers in transactions conducted on the Internet and stipulates that any clause that encroaches on such protection shall be null and void, as well as any provision that entails infringement of the inviolability and secrecy of private communications on the Internet or which, in a contract, does not offer the contracting party access to Brazilian jurisdiction for the resolution of disputes arising from services provided in Brazil. It also promotes the use of parental controls for the protection of minors, as well as the implementation of security measures and procedures for maintaining the confidentiality of information, about which the provider of the service must give clear information. It also envisages individual and collective protection measures. It protects the principle of net neutrality, thus prohibiting any attempt to block, monitor, filter or analyse the content of data packages in connection with the provision, transmission, switching or routing of Internet connections (either paid or free). It provides that legal entities domiciled abroad that offer services to the public in Brazil, or in which at least one member of the same economic group has an establishment in Brazil, shall be liable for the non-compliance of its branches, offices or establishments located in Brazil.

c) Protection of personal data

Brazil is a member of MERCOSUR and of the Ibero-American Data Protection Network. The Federal Constitution enshrines the right to privacy, to private life, to honour and to one's personal image, and it ensures the right to compensation for material damage or moral prejudice arising from any violation of that right. It recognizes the inviolability of the secrecy of correspondence, telegraphic communications, telephone information and communications, unless, in the latter case, there is a court order in connection with a criminal investigation. It enshrines the action of habeas data, which entitles a person to receive information on his or her personal data that is in records or databanks of government agencies, as well as the right to correct such information.

Brazil does not have a general law on protection of personal data; however, different laws protect the right of individuals to a private life, including the Civil Code (Act No. 10,406/2002), of 10 January 2002, which recognizes the inviolability of personal privacy, and the Consumer Protection Code, which includes several rules on access to databases or files of consumers and on the storage and maintenance of such files. The Consumer Protection Code stipulates that consumer data shall be made available only pursuant to an individual request concerning a specific consumer, as the Code prohibits the supply of mass information on many persons. The request must also be relevant to a specific commercial relationship pertaining to a possible agreement between the consumer and the provider making the request.

The Civil Framework for the Internet protects the following rights of users: (i) inviolability of privacy and private life, ensuring the right to protection of that right and compensation for material damage or moral prejudice resulting from its violation; (ii) inviolability of the flow and secrecy of Internet communications, except by court order, as well as the inviolability and secrecy of stored private communications, except by court order; (iii) non-suspension of an Internet connection, except when a debt has been contracted directly for its use; (iv) clear and complete information in service contracts, describing in detail the regime for protecting data in connection records and records of access to Internet applications; (v) impossibility of supplying third parties with personal data about users, including records on connection and access to Internet applications, except when free, express and informed consent has been given or under circumstances established by law; (vi) clear and complete information on the collection, use, storage, handling and protection of users' personal data, which may only be used for purposes justifying such collection, whether by law or as specified in service contracts; (vii) express consent for the collection, use, storage and treatment of personal data must be stated separately from the other clauses of the contract, and (viii) definitive deletion of personal data, except as provided by law.

The Framework also provides that any operation involving the collection, storage, protection or handling of records, personal data or communications by providers of Internet connection and applications, in which at least one of those actions occurs on the national territory, must comply with Brazilian legislation, as well as with the rights to privacy and protection of personal

data and secrecy of private communications and of records.

d) Industrial and intellectual property

The Software Act (Act No. 9,609), of 19 February 1998, lays down rules to protect computer programs as works covered by copyright law and establishes, among other things, conditions for their marketing in Brazil. It also establishes the guarantees that a copyright holder must give to users of the software, as well as the applicable penalties for violating the Act.

In the international sphere, Brazil has signed the following instruments on intellectual property:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

With respect to the domain name .br for Brazil, NIC.br, the executive arm of the Internet Management Committee (CGI.br), is responsible for registering and maintaining .br domain names, as well as for assigning autonomous system numbers and IPv4 or IPv6 addresses in the country, which are coordinated by the Latin American and Caribbean Addresses Registry.

NIC.br has an administrative domain-name dispute-resolution process, under which rules are set for resolving disputes between the owner of a domain name and any third party who impugns the legitimacy of the domain registration. Arbitration services are provided by the Brazilian Intellectual Property Association, the Canada-Brazil Chamber of Commerce and WIPO.

f) Cybercrime and information security

To deal with cybercrime, Act No. 12,735 and Act No. 12,737, both dated 30 November 2012, amending the Criminal Code, define offences against computer and related systems that are perpetrated with electronic, digital or similar devices.

Act No. 12,737 includes the offence of "invasion of an IT device", and provides sanctions for anyone who invades an IT device, whether or not it is connected to the Internet, by wrongfully disabling a security mechanism, in order to obtain, manipulate or destroy data or information, without the express or tacit authorization of the owner of the device, or by installing vulnerabilities in order to obtain an illicit advantage.

The Act also provides penalties for anyone who produces, offers, distributes, sells or disseminates computer devices or programs in order to enable the aforementioned behaviours. Penalties are increased if the invasion results in economic loss. It also punishes anyone who receives commercial or industrial secrets or private content as a result of disabling the computer equipment's security mechanism. The aforementioned offences are aggravated if they are committed against public officials, including the president, governors and other officials at the federal, state or municipal level.

With regard to information security, the Civil Framework for the Internet is designed to guarantee net neutrality and preserve stability, security and functionality. In providing Internet connectivity services, system administrators must keep connection records for one year in a controlled, secure and confidential environment. The law enforcement or administrative authorities or the Public Prosecution Service are empowered to require, as a precautionary measure, that records be kept for a longer time. Providers of Internet applications must also maintain the relevant records of access to Internet applications for six months in a controlled, secure and confidential environment. Law enforcement or administrative authorities or the Public Prosecution Service may require, as a precautionary measure, that records of access to Internet applications be kept for a longer period of time.

Providers of Internet connections shall not be civilly liable for damage caused by content generated by third parties. Providers of Internet applications may be held liable for damage caused by content generated by third parties only if, pursuant to a specific court order, they fail to take steps, within the technical limits of their service and within the time frame assigned, to make available the content which has been identified as in violation.

g) Pending legislation and challenges

The most important bills currently under discussion in the legislature are the proposed general act on data protection, of 2011, and several amendments to criminal procedural law designed to bring it in line with the

Council of Europe's Convention on Cybercrime. The need to close the digital gap, especially in terms of the lack of ICT capacities, is one of the main challenges facing Brazil.

CHILE

Chile has different types of laws on e-commerce, in particular the Act on Electronic Documents, Electronic Signatures and Electronic Signature Certification Services (Act No. 19,799), of 25 March 2002, and Act No. 20,217, amending the aforementioned Act and the Code of Civil Procedure, of 12 November 2007. Other important legislation is the Consumer Protection Act (Act No. 19,496), of 7 March 1997, and the Act on Bases for Administrative Contracts for Provision of Services (Act No. 19,886), of 30 July 2003. The content of these laws is summarized below.

a) Electronic transactions/electronic signatures

Act No. 19,799, on electronic documents, electronic signatures and electronic signature certification services in Chile (2002), is based on a number of provisions in the UNCITRAL Model Law on Electronic Signatures and on the Digital Signature Act of the state of Utah.[25] Under Act No. 19,799, acts and contracts awarded or made by individuals or legal entities in the private or public sector that are signed with electronic signatures are valid on the same basis as, and legally equivalent to, written contracts. Such acts and contracts are considered equivalent to those made in writing, in cases where the law requires that they be in written form.

Act No. 19,799 authorizes State entities to execute or carry out acts, enter into contracts and issue documents, within their sphere of competence, and sign them with electronic signatures. It also sets forth the obligations of certification service providers, as well as the requirements for electronic signature certification and the rights and obligations of users of electronic signatures.

Decree 181, regulating Act No. 19,799, of 17 August 2002, lays down more detailed rules for providers of certification services and the certification process, protection for the rights of users and the use of electronic signatures by State agencies. It also establishes technical standards for digital certificates, time stamps and mobile signature services.

Act No. 20,217, amending the Code of Civil Procedure, provides for the inclusion of additional proof of authenticity for electronic documents that are not signed with an advanced electronic signature, while Act No. 19,799 introduced the concept of electronic dates.

In addition, the Act on Bases for Administrative Procurement Contracts (Act No. 19,886), requires government entities to obtain estimates, issue tenders, hire personnel, award contracts, request clearance and carry out all procurement transactions and contracts for goods, through electronic systems authorized by the Office of Public Procurement and Contracting, on either open or closed networks, using e-commerce platforms or digital transaction markets. It also creates an official electronic registry in which all qualified individuals and legal entities, whether Chilean or foreign, contracting with State entities, are required to register. Public entities generally may not award contracts for which bidding has not taken place through electronic or digital systems.

In order to recognize the validity, for tax purposes, of commercial operations executed through electronically generated documents, various legal provisions have been put in place or modified to permit electronic invoicing in Chile. The most important of these include (i) Decree-Law No. 825, on the value-added tax, of 31 December 1974; (ii) Exemption Resolution No. 09 of the Internal Tax Service, which establishes a number of standards under the Tax Code, regulating the use of electronic signatures and certificates in tax-related matters; (iii) Act No. 19,983, of 15 December 2004, which regulates transfers and stipulates that copies of invoices shall have the same validity as the original invoices; (iv) Exempt Resolution No. 86 of the Internal Tax Service, of 1 September 2005, which establishes the standards and procedures for authorized taxpayers to issue electronic invoices, and (v) Decree-Law 830, on the Tax Code, of 31 December 1974 and updated to 28 May 2014, which authorizes the filing of documents in forms other than hard copy.

The automation of various procedures by the National Customs Service is also worth mentioning. These arrangements streamline customs clearances by transmitting information via remote means and providing for its corresponding validation in various databases. The participation of Chile in APEC, WTO and the World Customs Organization has been a major force in efforts to modernize the country's customs service. The most important regulatory provisions in this area include Act No. 19,479, amending the Customs Ordinance and the Organic Act of the National Customs Service, of 21 November 1996, which sets management and personnel standards, and Decree with the Force of Law No. 30, of 4 June 2005, whereby the National Customs Service implements a

[25] A state in the United States of America.

system of electronic payment for duties, taxes, fees and other payments received by the Service.

b) Consumer protection

In the area of e-commerce, the Consumer Protection Act (Act No. 19,496) requires providers to give their postal or e-mail address and explain what technical means it provides for consumers to identify and correct errors in shipments or in personal data. It also stipulates that promotional and advertising communications sent by e-mail must include the subject matter of the communication, the identity of the sender and a valid address at which the recipient can request that shipments be suspended, after which time they shall be prohibited.

c) Protection of personal data

The Political Constitution of Chile recognizes the right to privacy and to personal and family honour. It also enshrines the right to inviolability of all forms of private communication and prohibits the interception, opening or recording of communications, except in cases expressly envisaged by law. In addition to the protection provided by the Constitution, a number of laws safeguard personal privacy, including the Privacy Protection Act (Act No. 19,628), of 28 August 1999, as amended by Act No. 19,812, of 13 June 2002, which regulates the handling by public and private entities of personal data contained in records and databases.

The Act protects individuals whose personal data are to be used in any operation or set of operations or technical procedures, whether automated or not, that entail collecting, storing, recording, organizing, processing, selecting, extracting, comparing, interconnecting, dissociating, communicating, assigning, transferring, transmitting or cancelling data of a personal nature or using such data in any other form. It recognizes the right of individuals to provide, modify, cancel or block their personal data, as well as the judicial means for exercising their right in summary proceedings.

It also protects personal information or data, this being understood as data referring to any information concerning identified or identifiable individuals. It lays down further measures for protecting sensitive personal data defined as data that refer to the physical or moral characteristics of persons or to facts or circumstances of their private lives, such as their personal habits, racial origin, ideology and political opinions, religious beliefs or convictions, state of their physical or mental health and their sexuality. The Act stipulates that sensitive data may not be subject to handling, unless that is authorized by law, the data subject has consented or the information is needed in order to determine or grant health benefits to the data subject.

The Act enshrines the right of persons to be provide, modify, cancel or block their personal information, within the limits of national security or the national interest.

The Act provides that individuals or private-sector legal entities or public agencies that are responsible for personal databanks shall make compensation for material damage and moral prejudice caused by the improper treatment of personal information, without prejudice to their proceeding to eliminate, modify or block the data as requested by the data subject or, as the case may be, as ordered by the court that is competent to establish the amount of compensation. The Act does not designate any administrative authority in charge of enforcing the law, although it does confer powers on the judiciary to, in summary proceedings, order compliance with the Act and punish non-compliance with its decisions.

d) Industrial and intellectual property

The Intellectual Property Act (Act No. 17,336), of 2 October 1970, protects computer programs and compilations of data throughout the life of the author and up to 70 years thereafter, reckoned from the date of his or her death.

Act No. 20,435, amending the Intellectual Property Act (Act No. 17,336), of 23 April 2010, introduces, for the first time in the region, a “safe harbour” system, solely for copyright issues, whereby a “notice and takedown” procedure is followed. The Act includes a section outlining the summary judicial proceedings to be followed in requesting that materials which violate copyright be taken down. The procedure may consist of precautionary measures or special judicial proceedings in the context of measures for limiting the liability of providers of telecommunications and Internet services.

Under the “safe harbour” model, providers of telecommunications and Internet services who (i) do not initiate transmission of materials that violate the law; (ii) do not exercise editorial control over such materials; (iii) have no knowledge of the illicit nature of the materials that violate the law, or (iv) quickly remove, block or prevent access to materials that violate the law (notify and takedown procedure) shall not be responsible for materials they transmit, route, store, link or reference, and shall be exempt from the obligation to supervise or monitor such materials, as well as from the obli-

gation to actively search for facts or circumstances that might suggest or indicate the existence of illicit activities.

The "safe harbour" regimen in Chilean law meets the standards set forth in the joint declaration on freedom of expression and the Internet, of 1 June 2011, issued by the United Nations Special Rapporteur on freedom of opinion and expression, the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, the OAS Special Rapporteur on freedom of expression and the African Commission on Human and Peoples' Rights Special Rapporteur on freedom of expression and access to information.

The regulations to the Intellectual Property Act (Act No. 17,336), of 30 April 2013, include provisions on the appointment of a representative of Internet service providers to receive judicial notifications.

Chile has ratified the following international instruments on the right to intellectual and industrial property:

- Beijing Treaty on Audiovisual Performances (2012)
- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- WIPO Patent Cooperation Treaty
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

The Computer Science Department of the University of Chile has been delegated by the International Assigned Numbers Authority (IANA) to administer the .CL Domain Names Registry (NIC Chile), in accordance with the principles contained in Request for Comments 1591: Domain Name System Structure and Delegation. The delegation was formally recognized on 24 June 2006, in a framework agreement between ICANN and NIC Chile, which outlines the responsibilities of the two entities in regard to the preservation of stability, security and interoperability of the Internet.

Disputes arising as a result of the revocation of a .cl domain name must be resolved in accordance with the .CL Domain-Name Dispute-Resolution Policy. All disputes are submitted, resolved and processed in accordance with the arbitration procedure laid down in that policy, which empower the .CL Dispute-Resolution Centre to act as the unit of NIC Chile in charge of administering the .CL domain-name dispute-resolution system. NIC Chile does not participate at the arbitration stage, except to appoint the arbitrator in accordance with established procedure and to implement the arbitration award.

f) Cybercrime and information security

In terms of criminal law, the Cybercrime Act (Act No. 19,223), of 7 June 1993, defines the offences of (i) cybersabotage, which involves destroying or rendering useless an information-processing system or its parts or components, or impeding, obstructing or altering their functions – an offence whose seriousness increases when data are affected; (ii) cyberespionage, which consists of intercepting, interfering with or accessing an information-processing system to control, utilize or improperly gain knowledge of information contained therein; (iii) alteration of data, which includes destroying or causing damage to them; and (iv) revealing or disseminating, without authorization, data contained in an information-processing system.

The General Telecommunications Act (Act No. 18,168), of 2 October 1982, requires concessionaires and providers of Internet access to make every effort to preserve the privacy of users, provide protection against viruses and ensure the security of the network. It also defines as offences which the prosecutor can act on ex officio: (i) maliciously interfering with, intercepting or interrupting a telecommunication service, which is punishable with a short prison sentence of any length and confiscation of equipment and facilities; and (ii) maliciously or seriously intercepting or capturing, without proper authorization, any type of signal emitted through a public telecommunication service, which is punishable with a short prison sentence of medium length and a fine of 50 to 5,000 monthly tax units.

g) Pending legislation and challenges

Among the pending legislation is the bill on amendments to the Privacy Protection Act (Act No. 19,628), of 11 January 2012, which inter alia proposes the elimination of legal entities as subjects of protection and the redrafting of a number of definitions and innovations in the complaint procedure so as to expedite processing. One of the main challenges that needs to be addressed in Chilean legislation is the matter of

designating an administrative authority to guarantee the protection of data.

COLOMBIA

Several provisions in regulatory framework of Colombia recognize the use of data messages and electronic means, in particular electronicIn the area of electronic transactions and electronic signatures, Act No. 527, of 18 August 1999, known as the e-Commerce Act, incorporates a number of provisions from the UNCITRAL Model Law on Electronic Commerce and Electronic Signatures. The Act authorizes the use of data messages in electronically executed commercial operations and covers, among other things, the authenticity, integrity, originality and preservation of electronic documents.

a) Electronic transactions/electronic signatures

In the area of electronic transactions and electronic signatures, Act No. 527, of 18 August 1999, known as the e-Commerce Act, incorporates a number of provisions from the UNCITRAL Model Law on Electronic Commerce and Electronic Signatures. The Act authorizes the use of data messages in electronically executed commercial operations and covers, among other things, the authenticity, integrity, originality and preservation of electronic documents.

The Act also recognizes the use and evidential value of digital signatures backed by digital certificates issued by certification service providers. Regulations relating to this legislation have been issued recently, e.g., in Decree 2364, of 22 November 2012, covering electronic signatures as a mechanism equivalent to written signatures that is more flexible than digital signatures, and Decree 333, of 19 February 2014, governing conditions for setting up and operating digital certification entities and modernizing their accreditation methodology. This decree replaces Decree 1747 of 2000.

Act 527 provides that no administrative or judicial action shall deny the effectiveness, validity or binding nature and evidential value of information provided in the form of data messages based solely on the form of such messages or on the fact that they are not presented in their original form. The evidential value of data messages is determined in accordance with the relevant provisions of the Code of Civil Procedure. Colombia has signed the United Nations Convention on the Use of Electronic Communications in International Contracts (2005), although it has not yet ratified it.

Pursuant to Decree Law 019, of 10 January 2012, the Office of the Superintendent of Industry and Commerce is no longer in charge of authorizing certification entities, which are now accredited by the National Accreditation Agency of Colombia. Accreditation of certification entities is also governed by Decree 333 of 2014; the specific accreditation criteria to be issued by the National Accreditation Agency are pending as of this writing. The Office of the Superintendent of Industry and Commerce is still responsible for oversight of digital certification procedures.

Act No. 962, of 8 July 2005, bears on administrative matters, containing provisions to rationalize administrative procedures and formalities in State entities and in private entities that carry out public functions or provide public services. It includes a number of measures to facilitate the relationship between private persons and government, as well as various guiding principles for policy in the areas of rationalization, standardization and automation of procedures to prevent the imposition of unjustified requirements on users. Such measures include enhancing technology to coordinate the actions of public administration and reduce the time and cost of formalities to users. They also provide incentives for the use of integrated technological tools; to this end, the Administrative Department of Public Service is authorized to oversee, in coordination with the Ministry of Information and Communication Technology, the technical support needed by government agencies. Electronic invoicing is one of the services that is based on this Act.

As regards e-government, Act 1437, of 18 January 2011, on the Code of Administrative Procedure, includes a separate chapter (III) on electronic administrative procedure. This legislation provides for electronic notification procedures to completely eliminate the need for the concerned party to be physically present; the use of a website to streamline formalities and requests for services, and the use of electronic files and virtual meetings. Regulations governing electronic files have already been issued by the Government in Decree 2609, of 14 December 2012.

In addition, Act 588, of 5 July 2000, governing notarial activities, authorizes notarial services and consulates that have applied to the Office of the Superintendent of Industry and Commerce, to act as certification entities under Act 527 of 1999. They are allowed to transmit to other notarial services or consulates – in the form of data messages through electronic, optical or similar means – copies, certificates and records of documents taken from their files. Under the Act, the resulting documents are considered authentic.

Decree 624, of 30 March 1989, issuing the Tax Statute, regulates the use of electronic invoices and documents equivalent to sales invoices. Decree 1929, of 29 May 2007, regulating article 616-1 of the Tax Statute, defines the concept of electronic invoicing and sets rules on various aspects of the issuance of electronic sales invoices, as well as on their validity, authorizing persons required to perform this duty to do so through electronic means.

In the area of customs operations, Decree 4149, of 10 December 2004, creates the Single Window for Foreign Trade, which is administered by the Ministry of Commerce, Industry and Tourism, using electronic means, through which the administrative entities concerned with foreign trade operations share information for the purpose of granting authorizations and permits related to the importation and exportation of goods. The Single Window for Foreign Trade provides for digital signatures and electronic payments based on XML documents, which are used to digitize documents and administrative procedures connected with advance import and export authorizations.

b) Consumer protection

The Political Constitution of Colombia protects consumers from being sold goods and services that pose a threat to their health or safety. It also recognizes consumers' right to efficient public services. In terms of protection for online customers, Act 1480, of 12 October 2011, a new statute designed to protect consumers, includes a complete chapter on e-commerce, laying down a full set of regulations on business-consumer relations and stressing the duty to provide information and act with loyalty and prudence in offering goods through electronic means. The Office of the Superintendent of Industry and Commerce is the oversight agency for such services.

c) Protection of personal data

Personal data are protected by two laws: the Special Act on Protection of Personal Data (Act No. 1581), of 17 October 2012, and the Act on Habeas Data relating to Financial Matters (Act No. 1266), of 31 December 2008. These acts regulate the handling of personal data contained in databases – particularly financial, credit, commercial and services-related information – as well as information from other countries. The purpose of these acts is to guarantee the right of all persons to have access to, update and correct information concerning them in databanks, along with the other constitutional guarantees, rights and freedoms relating to the collection, processing and circulation of personal data. This legislation applies to all personal data contained in databases, whether administered by public or private entities, without prejudice to the special regulations that apply to them. Intelligence databases produced by the State Intelligence Service to safeguard the foreign and domestic national security interests of Colombia, as well as data maintained for personal or domestic use and data that are only circulated internally, i.e., that are not provided to other legal entities or individuals.

The principal rights recognized by this legislation include the "right of expungement", understood as the right of persons on whom there is data relating to payment delinquencies, collections, portfolio status, as well as data relating generally to failure to meet obligations, to have such data expunged four years from the date on which the overdue amounts are paid or from the date on which the overdue obligation is met. Once this term has elapsed, the information must be removed from the databases of the entities maintaining such information, thus ensuring that users will not have access to such information maintained by credit agencies. The legislation contains a special title regulating complaints and requests to access data.

Decree 1377, of 27 June 2013, partially regulates Act No. 1581 and establishes a number of provisions stipulating that the person referred to in the information must authorize the use of his or her personal data, as well as policies on the handling of data by the persons in charge of such matters and on how the data subjects can exercise their rights.

d) Industrial and intellectual property

In the area of intellectual property rights, the Andean Community's supranational regulatory framework is deserving of note, in particular, Decision 351 of 1991, on the Common Copyright and Related Rights Regime, which protects the right of authors and other rights holders to literary, artistic and scientific works of the imagination, including computer programs, regardless of their type or form of expression, or their literary or artistic merit or purpose. It also protects copyright-related rights of performers, producers of phonograms and broadcasting organizations in member States. In the domestic realm, Act 23, of 28 January 1982, addresses copyright; Decree 162, of 22 January 1996, provides for regulation under Andean Decision 351, and Act 44, of 5 February 1993, relates to collective management bodies overseeing copyright and related rights.

In addition, Colombia has signed the following instruments:

- Beijing Treaty on Audiovisual Performances (2012)

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Brussels Convention relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

Under Act 1065 of 2006, the country's .co domain name is administered by the University of the Andes by delegation of IANA. It is governed on a "first come, first served" basis, as established the regulations for the use of .co domain names. Pursuant to its authority under Act 1065, the Ministry of Information and Communications Technology adopted the ICANN Uniform Domain-Name Dispute-Resolution Policy.

f) Cybercrime and information security

As regards criminal law, Act 1273, of 5 January 2009, amending the Criminal Code of Colombia, defines as protected legal assets the information and data preserved entirely in systems that utilize ICTs.

The Act adds a section on the protection of information and data, and defines various crimes, such as illegal access to computer systems, illegally impeding the functioning of such a system or of a telecommunications network, intercepting computer data, damaging computer systems, using malicious software, violating personal data and accessing websites to obtain personal data. Such behaviours are considered to violate confidentiality and interfere with the integrity and availability of data and information. The Act also provides sanctions for theft using information technology media and for unauthorized transfer of assets through such media.

g) Pending legislation and challenges

At present, two proposals for regulations are worthy of mention, namely, a draft decree mandating the mass use of electronic invoicing and draft regulations on transferable electronic documents, which would govern electronic securities.

Colombia has implemented a number of public policies aimed at promoting connectivity for its citizens; however, the fact that entrepreneurs still have not appropriated technology in their production chains remains a challenge. There is also a need for improved internal harmonization of ICT-related standards, given the proliferation of provisions applicable to businesses that have not yet been understood or applied.

COSTA RICA

Costa Rican legislation on e-commerce includes the Certificates, Digital Signatures and Electronic Documents Act (Act No. 8454), of 13 October 2005, the Civil Code (Act No. 63), the Commercial Code (Act No. 3284), of 30 April 1964 and the Act on Promotion of Competition and Effective Consumer Protection (Act No. 7472), of 20 December 1994. The following paragraphs contain a review of these and other important laws.

a) Electronic transactions/electronic signatures

In the area of electronic transactions, the Commercial Code (Act No. 3284), which governs commercial transactions, and the Civil Code (Act No. 63), which deals with the formation of contracts between present parties and absent parties, the time and place at which a contract is executed and the formalities required, are supplemented by the Digital Certificates, Digital Signatures and Electronic Documents Act (Act No. 8454), which recognizes the use and validity of electronic means for executing contracts.

Act No. 8454 incorporates certain principles from the UNCITRAL Model Law on Electronic Signatures and establishes a general legal framework for the transparent, reliable and secure use of electronic documents and electronic signatures by public and private entities, i.e., (i) it applies to all types of transactions and legal acts, whether public or private, in the absence of legal provisions to the contrary, provided that the specific nature or requirements of the act or business involved are not incompatible with such application; (ii) it explicitly authorizes the State and all public entities to use digital certificates, digital signatures and electronic documents in their areas of authority; (iii) it recognizes the issuance of certificates, affidavits and other documents; (iv) the submission, processing and registration of documents in the National Register, and (v) the processing, preservation and use of notarial protocols.

Executive Decree No. 33018-MICIT, of 20 March 2006, regulates the Digital Certificates, Digital Signatures and Electronic Documents Act, which, among

other things, defines the duties and hierarchy of different certifying authorities, beginning with the root certification authority, and the characteristics and functions of the public key infrastructure. It also lays down the technical and administrative qualifications that must be met by registered certifying authorities.

As regards public contracting, the Administrative Procurement Act (Act 7494), of 8 June 1995, incorporates the use of electronic communications in public contracting procedures, provided the delivery and content of messages can be guaranteed. The regulations for use of the CompraRED Government Procurement System, set forth in Executive Decree No. 32717, of 24 October 2005, and the regulations for the use of the Mer-Link Online Market Electronic System for Government Procurement, in Executive Decree No. 36242-MP-PLAN, of 21 October 2010, make it possible to electronically publish requests for goods, works and services; to electronically provide information on providers and the procurement process from beginning to end, including decisions on, and results of, purchases, thus allowing potential providers, citizens and the Government itself to obtain relevant information online.

The Integrated Public Procurement System was created by Executive Decree No. 38830-MICITT, of 15 January 2015 as the technological platform that must be used by the central administration in all administrative contracting procedures. CompraRED and Mer-Link may be used by decentralized institutions on a voluntary basis.

In the area of public administration, Directive No. 067-MICITT-H-MEIC, on massification of the implementation and use of digital signatures in the Costa Rican public sector, of 25 April 2014, instructs public agencies to implement technical and financial measures to enable citizens to use electronic means to obtain information, make queries, submit requests, express their consent and commitment, make payments, carry out transactions and oppose administrative decisions and acts.

b) Consumer protection

Addressing consumer protection, the Promotion of Competition and Effective Consumer Protection Act (Act No. 7472) incorporates the basic principles of consumer relations set forth in United Nations General Assembly resolution 39/248, on guidelines for consumer protection. Among other things, the Act regulates merchants' obligations to consumers in regard to information, advertising or public offering of goods or services. In addition, it provides administrative and judicial protection against misleading advertising and abusive practices and clauses, as well as against unfair commercial methods or methods that limit freedom of choice.

The regulations to the Promotion of Competition and Effective Consumer Protection Act, issued by Executive Decree No. 37899-MEIC, of 23 September 2013, expand on the concept of "means of dissemination" to include the use of e-mail and other means of electronic or online communication and telecommunications for advertising purposes. The regulations also cover the right of consumers to opt out, which may be exercised via e-mail within eight days after the date of purchase.

c) Protection of personal data

With regard to privacy and protection of data, Costa Rica has adopted the Universal Declaration of Human Rights and the Inter-American Convention on Human Rights (the San José Pact), which recognize as fundamental rights the right to confidentiality and to a private life; these rights are also reflected in the Constitution.

In terms of domestic legislation, the Act on Protection of Persons and Processing of their Personal Data (Act No. 8968), of 5 September 2011, establishes the legal framework for the processing of personal data by individuals and public and private institutions. The Act complies with the Directives for Harmonization of Data Protection in the Ibero-American Community issued by the Ibero-American Data Protection Network. The Act protects the right of data subjects to decide what information on their life or private activities may be the subject of automated or manual data processing.

The Act also stipulates that all databases, public or private, that are administered for the purpose of distribution, dissemination or sale, must be registered in the registry to be set up for that purpose by the Personal Data Protection Agency, subject to payment of a yearly fee of US$ 200 for database regulation and management. It also provides that in the case of overall contracts for low, medium and high numbers of queries to the registered database, or for online service contracts by number of applications, the regulations shall determine the applicable fee which may not be higher than 10 per cent of the contract price.

Executive Decree No. 37554-JP, issuing regulations to the Act on Protection of Individuals in connection with the Processing of their Personal Data, of 5 March 2013, describes in detail: (i) the security measures that the parties responsible must implement to protect personal data; (ii) registration of databases with the Personal Data Protection Agency; (iii) the amounts

of fees to be paid based on the level of queries to the database, and (iv) issues relating to evidence.

d) Industrial and intellectual property

On the matter of intellectual property, the Copyright and Related Rights Act (Act No. 6683), of 14 October 1982, as amended by Act No. 8834, of 3 May 2010, protects artistic and literary works, as well as computer programs and databases and compilations. Decree No. 36880-COMEX-JP, issuing regulations on limitations on liability of service providers for infringement of copyright and related rights, pursuant to CAFTA-DR article 15.11.27, of 16 June 2011, establishes those cases in which the liability of providers of caching, hosting, connection and linking services shall be limited in respect of the materials cached or transmitted through their systems or networks.

As regards industrial property, it should be noted that the Patents, Drawings and Industrial Models Act (Act No. 6867), of 25 April 1983, as most recently amended by Act No. 8632, of 25 March 2008 does not cover mathematical methods or computer programs in isolation as inventions eligible for patent protection. The Undisclosed Information Act (Act No. 7975), of 4 January 2000, is also relevant.

On the international intellectual property rights front, Costa Rica has ratified the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances (2012)
- Protocol to the Central American Agreement for the Protection of Industrial Property
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Lisbon Agreement for the Protection of Appellations of Origin and their International Registration
- Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite

It has also signed the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO.

e) Domain names

The National Academy of Science, through its subsidiary NIC-Internet Costa Rica (http://nic.cr) is responsible for administering and coordinating the operation of the top-level domain .cr. Its domain removal policy establishes that in the case of a dispute over a .cr domain name, NIC-Internet Costa Rica will remove the domain name when ordered to do so by a domestic or foreign court. The procedure does not apply the ICANN Uniform Domain-Name Dispute-Resolution Policy.

f) Cybercrime and information security

The Cybercrime Act (Act No. 9048) and other amendments to the Criminal Code, of 6 November 2012, a number of computer-related offences were added to punish (i) anyone who takes control of, gains access to, modifies, alters, deletes, intercepts, interferes with, uses, disseminates or deflects from their intended recipient messages, data or images in electronic, computer-based, magnetic or telematic form for the purpose of discovering the secrets or violating the privacy of another without the latter's consent; (ii) anyone who influences data processing or results in a computer system through programming, use of false or incomplete data, improper use of data or any other action that affects the system's data processing with the intention of obtaining material benefit for him/herself or for a third party; and (iii) anyone who by any unauthorized means accesses, erases, deletes, modifies or renders unusable data recorded in a computer.

The General Customs Act (Act No. 7557), of 20 October 1995, defines certain IT-related offences committed to the detriment of the systems used by the National Customs Service.

g) Pending legislation and challenges

Among the bills deserving special attention are those referring to criminal procedure to facilitate the collection and processing of evidence in electronic media. On the international scene, Costa Rica has not yet ratified the United Nations Convention on the Use of Electronic Communications in International Contracts or the Council of Europe's Convention on Cybercrime.

CUBA

The development of e-commerce in Cuba – through the deployment of technological infrastructure and a

regulatory system to support it – represents an important opportunity for exploiting the economic benefits of ICT.

a) Electronic transactions/electronic signatures

In terms of regulation, e-commerce and electronic signatures are governed by the administrative regulations issued by different entities of the executive branch, in particular, the Guidelines for the Development of e-Commerce in Cuba, of 26 December 2005, issued by the Council of Ministers, and Decision 61/2002 of the Central Bank of Cuba, of 14 November 2002, which lays down rules for executing collections and payments for e-commerce transactions.

b) Consumer protection

Cuba does not have legislation on consumer protection, although related issues are dealt with in the context of the Consumer Protection System, which has been in force since 2001 and applies to entities that engage in retail commerce. The system does not expressly cover e-commerce. The Criminal Code (Act No. 62), of 29 December 1987, provides for punishment of certain behaviours that are harmful to the interests of consumers, as described below.

c) Protection of personal data

Cuban legislation does not expressly recognize the right to protection of personal data; consequently, there are no mechanisms or means for protecting such data. An administrative regulation issued by the Ministry of Information Technology and Communications includes certain protections for personal data. In particular, Decision 57/1996 of the Ministry of Information Technology and Communications created the National Registry of Electronic Information for Data Networks, and Decision 188/2001 of the same Ministry, of 15 December 2001, established the Methodology for Access by Cuban Entities to the Internet and to Other Foreign Data Networks.

d) Industrial and intellectual property

In the area of intellectual property rights, Joint Decision 1-99, on software copyright protection, was issued by the Ministry of Culture and the Ministry for the Steel and Heavy Machinery Industry on 21 June 1999. This decision establishes regulations to protect computer programs and databases and enshrines the principle of cumulative protection of copyright and industrial property, so that the two systems are considered independent and compatible.

In the international context, Cuba has signed the following instruments:

- Paris Convention for the Protection of Industrial Property
- Berne Convention for the Protection of Literary and Artistic Works
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

The following decisions of the Ministry of Commerce are especially relevant to the matter of domain names: Decision 93/2003, on domain name .cu on Cuban servers, of 15 October 2003, provides that Cuban websites using the domain name .cu must be located on servers in Cuba, independently of whether they are also hosted on foreign servers. Decision 150/2008, on responsibility of Cuba-NIC and generic domains, provides that the Cuba-NIC Network Information Centre is responsible for the proper administration and management of the .cu domain, for the operation of primary and secondary domain-name servers in the second-level Registry of Domain Names under .cu and for the Registry of Domains in generic categories under the .cu domain.

By its Decision 72/2013, the Ministry of Information Technology and Communications issued domain name regulations and set rules for assigning and registering domain names of entities. It authorized the Ministry's Control and Supervision Agency to take steps to ensure that the Cuban domain- names system is a distributed, hierarchical and scalable service with decentralized control. It also establishes measures to be taken in cases of non-compliance with regulations on the part of bodies and agencies, including temporary or definitive invalidation of operating licenses or suspension of services.

f) Cybercrime and information security

The Criminal Code (Act No. 62) does not refer to cybercrime, but it does define as offences a number of behaviours that violate consumer protection rules, including (i) selling to the public items that are incomplete or underweight or deteriorated or in poor condition; (ii) charging for merchandise or services amounts that are higher than the price or rate approved by the competent authority or agency, or the price agreed on by the parties; (iii) selling industrial or agricultural products under false claims as to their brand or quality, and (iv) illegal use of a trademark, industrial model or patent, on a given product.

As regards security of information, Decision No. 127/2007 of the Ministry of Information Technology and Communications, of 9 July 2007, issued the regulations for IT security. Decision No. 6058 of

the Executive Committee of the Council of Ministers, issued on 9 July 2007, established guidelines for improving IT security.

g) Pending legislation and challenges

The regulatory proposals currently under review include a decree law on general standards for the practice of e-commerce which incorporates provisions regulating the transmission and reception of data messages, legal business carried out electronically, protection of personal data and activities of certification and registration authorities and of entities that perform certification and registration functions.

Consideration is being given to a bill on the public key infrastructure. A bill on amendments to the Criminal Code is also under review which would cover various cybercrimes, as well as a proposals on amendments to the Copyright Act (Act No. 14).

The main challenges facing Cuba include the digital gap and the lack of connectivity, as well as the need to enhance the ICT capacities of the general public and the government agencies. Another factor that has held back the development of connectivity in Cuba has been the 50-year-long trade embargo imposed on the country by the United States.

DOMINICAN REPUBLIC

The Dominican Republic has established a legal basis for promoting e-commerce as a tool for national development. Under the National Development Strategy Act (Act No. 1-12), of 25 January 2012, the Dominican Republic promotes the use of ICTs as a means for increasing business productivity and improving public administration through more efficient and accessible services. In addition, the e-Commerce, Documents and Digital Signatures Act (Act No. 126-02), of 4 September 2002, includes a number of precepts taken from the UNCITRAL Model Law on Electronic Commerce.

a) Electronic transactions/electronic signatures

The e-Commerce, Documents and Digital Signatures Act (Act No. 126-02) is the main legislation on electronic transactions and electronic signatures. It defines e-commerce as all relations of a commercial nature, whether contractual or not, that are based on the use of one or more digital documents or data messages, or other similar media. The Act promotes facilitating commerce and recognizing the validity of transactions conducted through electronic means, as well as the functional equivalence of digital documents and data messages with respect to printed documents, and of digital signatures with respect to handwritten signatures. It also recognizes their probative value.

The Act also regulates certification entities responsible for issuing digital signature certificates and offering or facilitating registry services and time stamps in connection with the transmission and receipt of data messages. With respect to the formation of contracts, the Act provides that the offer and its acceptance may be expressed by means of digital documents or data messages. It also recognizes digital certificates issued by foreign certification entities.

In the area of finance, the Act empowers the Monetary Board to regulate all matters pertaining to financial transactions and services associated with electronic means of payment carried out by the Monetary and Financial System of the Dominican Republic. The Monetary Board issued the payment systems regulations which establish a legal regime applying to the country's payments and settlements system.

The Monetary and Financial Act (Act No. 183-02), of 21 November 2002, authorizes the Monetary Board to establish requirements for the admission of evidence in electronic form regarding banking matters and debit and credit card transactions, as well as any other tangible or electronic payment instrument.

In the sphere of government, Act No. 126-02 stipulates that when a signature is legally required, or certain legal consequences flow from the absence of one, the requirement may be satisfied by a digital document or data message if said document or message has been digitally signed and the digital signature meets the requirements for validity established in this law. It stipulates that in any interaction with a public entity that requires a signed document, this requirement may be satisfied by one or more digital documents or data messages digitally signed pursuant to the provisions of this law.

Decree No. 335-03, approving the regulations for implementation of Act No. 126-02, of 8 April 2003, describes in greater detail the powers of the Dominican Telecommunications Institute and establishes the requirements for certification entities. By Decision No. 10-04, of 30 January 2014 (supplementary rule) on Act No. 126-02, the Dominican Telecommunications Institute adopted supplementary rules, including the rule on authorization and accreditation procedures, which sets forth general aspects, the requirements and the procedure to be followed in requesting the Institute's authorization to operate as a registry unit.

Regarding taxes, the Tax Rectification Act (Act No. 495-06), of 28 December 2006, incorporates the ability to store tax-related information in data storage media used in computer systems. It allows taxpayers to keep their accounting records, including receipts or payment vouchers, in electronic media for 10 years. It also authorizes taxpayers to register with tax authorities identification and access codes (PINs) for sworn statements, queries, tax settlements and payments, as well as other procedures through electronic means, and grants these documents the same probative value as actions signed by hand.

In the area of foreign trade, the Customs Regime Act (Act No. 3489) makes no reference to electronic media for operations associated with customs clearance. However, Decree No. 248-09, of 9 July 1998, created the Integrated Single Window for Foreign Trade System, a scheme using automated electronic procedures for managing all formalities and services needed for export activities.

On the international scene, it is worth noting Decision No. 6-12, of 2 February 2012, approving accession to the United Nations Convention on the Use of Electronic Communications in International Contracts.

b) Consumer protection

The General Consumer Protection Act (Act No. 358-05), of 6 September 2005, sets forth basic consumer rights in conformity with United Nations General Assembly resolution 39/248, on guidelines for consumer protection, of 9 April 1985. In regard to e-commerce, the Act requires providers to (i) inform the consumer, in advance, of prices, including taxes, form and date of delivery, shipping costs and insurance, where relevant; (ii) issue notification of shipping, with the name and address of the provider and the precise good or service being provided to the consumer; (iii) provide documentation of the delivery of the product or service to the consumer or user, or have such documentation provided to a duly authorized representative, in the form of proof of receipt; (iv) permit the consumer to make claims, and return or exchange products through the same medium as was used for the sale; (v) cover shipping costs in case of exchanges or repairs covered by guarantee; (vi) allow a minimum period of three days for the consumer to reconsider, prior to delivery; (vii) provide for and allow the consumer a minimum trial period of seven business days for returning the good or suspending the service contract; and (viii) issue and deliver to the consumer or user a written or digital invoice.

c) Protection of personal data

The right to protection of personal data is enshrined in the Constitution of the Dominican Republic of 26 January 2010. Under the Constitution, and pursuant to the commitments undertaken with the Ibero-American Data Protection Network, the Organic Act on Protection of Personal Data (Act No. 172-13), of 13 December 2013, provides for full protection of personal data contained in archives, public records, databanks or other data-processing media used to issue reports, whether public or private, as well as to guarantee that there will be no harm to the right to honour and privacy of individuals. The Act also incorporates a number of measures governing credit bureaus, credit reporting agencies and market information companies, guaranteeing respect for privacy and the rights of data subjects.

The Act recognizes the principles of information, consent, quality, lawfulness, loyalty, confidentiality, security and purpose that must govern the processing of data. It establishes the duty to guarantee the right of habeas data or of information for data subjects, a right that must be upheld by the courts. It also makes it obligatory to ensure that information is kept under secure conditions. It protects the right of persons to have access to, update, challenge the processing of their information and correct or destroy data that unlawfully affect them.

Act No. 310-14, of 11 June 2014, which governs the sending of unwanted commercial e-mail (spam), regulates the sending of unrequested commercial, advertising or promotional communications by electronic means, without prejudice to existing provisions on advertising and consumer protection. The Act requires that all commercial electronic communications must be labelled as “advertising” in the subject field of each message. It also stipulates that if the communication includes sexual content that should only be read by adults, it shall be labelled “advertising for adults”.

The Act specifies that electronic commercial communications sent from an e-mail address must allow the recipient to express his or her wish to not receive commercial communications. It also states that communications must include the name or business, complete domicile and e-mail address of the sender of the communication. The sender must include a valid and active telephone number or a valid and active e-mail address for replies, so that the recipient can send a message to notify his or her desire to not receive any further commercial communications.

The Act prohibits the sending, directly or indirectly, of commercial communications that have not been re-

quested or consented to by the recipient concerned. Nevertheless, it provides that sending unsolicited commercial communications shall not give rise to the actions and sanctions envisaged in the law, when the recipient has or has had a prior commercial relationship with the sender or when the recipient has expressed his or her agreement to receive the communication. It also prohibits communications that are sent, directly or indirectly, without having been requested or expressly agreed to by the recipient concerned, or when the content of the information is false or misleading in regard to the subject, or does not coincide with the content of the message.

On the international front, the Economic Partnership Agreement between the Member Countries of the Caribbean Forum and of the Group of African States, the Caribbean and the Pacific (CARIFORUM) and the European Community requires member countries to guarantee the right to privacy in the handling of personal information.

d) Industrial and intellectual property

The Constitution recognizes that individuals are entitled to exclusive ownership of inventions and discoveries, as well as of scientific, artistic and literary productions, for the period and in the manner stipulated by law.

The Industrial Property Act (Act No. 20-00) states that mathematical methods and computer programs shall not be considered patentable inventions. With regard to the use of trademarks, Act No. 20-00 makes no mention of their use on the Internet or in domain names.

The Copyright Act (Act No. 65-00), of 26 July 2000, considers computer programs and databases to be protected works. With regard to the related rights of artists, performers and broadcasting organizations, it defines the concepts of phonogram and videogram and recognizes the right of publication in any medium.

On the international intellectual property rights front, the Dominican Republic has ratified the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Protocol to the Central American Agreement for the Protection of Industrial Property
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

With regard to domain names, the country's NIC (http://www.nic.do), which is housed at Pontificia Universidad Católica Madre y Maestra, administers the country's top-level domain name .do. Its policies make no reference to the ICANN Uniform Domain-Name Dispute-Resolution Policy, although they do require parties applying for registration of domain names to ascertain that, in doing so, they are not violating any trademark. In cases of disputes between applicants over particular names, NIC incurs no liability by registering a name, but merely provides information to both parties. However, it does reserve the right to revoke the assignment of a domain to an organization or individual if the organization that owns the domain's trademark requests the domain.

f) Cybercrime

Act No. 53-07, on high-technology crimes and misdemeanours, of 23 April 2007, includes a number of provisions envisaged in the Council of Europe's Convention on Cybercrime. Substantive provisions from the Convention include definitions of crimes involving IT systems. Procedural provisions cover mechanisms for combating this type of crime by facilitating cooperation between the State and the private sector at the national level to detect, investigate and punish such crimes, as well as provisions for rapid and reliable international cooperation.

The Act defines high-technology crimes as conduct that jeopardizes legal rights protected by the Constitution and by laws, decrees, regulations and resolutions relating to information systems. It includes several definitions, including definitions of illicit access, cloning, malicious codes, user data, diversion of contracted facilities, electronic interception and transfer of funds.

The Act defines a number of crimes against confidentiality, integrity and availability of data and information systems, as well as crimes of content, crimes against intellectual property, crimes against telecommunications and crimes against the nation and acts of terrorism.

It also establishes which entities have the authority to investigate and prosecute cybercrimes, with emphasis on the interaction between the Public Prosecution Service and the Department of Telecommunications, Intellectual Property and e-Commerce of the Office of the Attorney General. It creates the Inter-Agency Commission against High-Technology Crimes and Misdemeanours and the Department for Investigation of High-Technology Crimes and Misdemeanours. This latter department is the country's official contact point for the International 24/7 Network of Assistance on Crimes Involving High Technology of the Subgroup on High-Technology Crimes of the G8 Group of Experts on Transnational Organized Crime.

The Department for Investigation of High-Technology Crimes and Misdemeanours also regulates certain precautionary and procedural measures, including the rules applicable to obtaining and preserving data contained in an information system or its components, traffic data, connection data, access data and any other information useful in the investigation of crimes covered by the Act.

It also requires service providers to preserve data on traffic, connection, access and any other information useful in the investigation for a minimum period of 90 days.

Act No. 310-14, of 8 August 2014, which governs the sending of unsolicited commercial e-mails (spam), defines the following behaviours as cybercrimes: (i) gaining access to a computer system without authorization and intentionally initiating transmission of commercial communications from or through that system; (ii) gaining access to a computer system to forward or resend commercial communications with the intention of deceiving the recipients about the origin of those messages; (iii) using a false subject line on a data message containing commercial communication and intentionally initiating transmission of same; (iv) registering and collecting, fraudulently or maliciously, with false information, the identity of the e-mail account holder or e-mail address of public-access sites, such as chat sites, public directories, news groups, online profile services, social networks and any other mass medium that uses groups of electronic addresses, or of a domain name, and intentionally initiating transmission of multiple commercial communications from any combination of such accounts or domains without authorization of the e-mail account holder or the operator of the access site, and (v) offering for sale databases containing e-mail addresses without the express consent of the owners of the databases, for the purpose of generating unsolicited commercial communications.

g) Pending legislation and challenges

The Dominican Republic needs to have a strategy or national policy on large-scale cybersecurity, as well as a national computer emergency response team to deal with computer security incidents.

ECUADOR

The e-Commerce, Electronic Signatures and Data Messages Act (Act No. 2002-67), of 17 April 2002, is the main regulatory tool covering contracts and electronic signatures, as well as issues relating to online consumer protection.

a) Electronic transactions/electronic signatures

The e-Commerce, Electronic Signatures and Data Messages Act is based on the UNCITRAL Model Law on Electronic Commerce, as well as on the European Council directive on e-commerce and the directive on electronic signatures. The Act assigns to data messages the same legal status as that of written documents and to electronic signatures the same status as handwritten signatures. It also establishes requirements that must be met by the information contained in a data message in order for it to be considered original.

The Act authorizes the dematerialization of documents, provided that the digitized documents contain duly certified electronic signatures. It also establishes the requirements that must be met by electronic signatures and electronic signature certifications, as well as the obligations and responsibilities of accredited information certification entities. It recognizes the evidential value of data messages, electronic signatures, electronic documents and domestic or foreign electronic certificates, subject to the conditions laid down in the Act. In addition, it establishes administrative and criminal sanctions for failure to comply with such provisions.

The regulations to the e-Commerce, Electronic Signatures and Data Messages Act, issued by Decree No. 3496-2002, of 31 December 2002, set the requirements that must be met for a data message to be considered accessible for consultation and assign to this form of data the same value as that of a written document. It also refers to the elements and principles governing the electronic signature infrastructure and the work of information certification entities, as well as of time stamping services.

The aforementioned regulations set rules for accreditation, registration and regulation of entities authorized to provide information certification and related services, as well as for related third parties. It establishes

standards and procedures to be followed in providing information certification services, issuing electronic signature certificates and registering data and time stamps. It also provides more detailed rules on the operation of the public key infrastructure and authorizes entities, State institutions and public corporations to obtain electronic signature certificates from accredited information certification and related services, under public or private law.

In the area of electronic transactions by government entities, the Organic Act on the National Public Contracting System, of 4 August 2008, governs electronic contracting procedures for government agencies and establishes the legal bases for implementing the National Public Contracting System for State procurement of goods and contracting of services. It also sets requirements to be met by providers engaging in electronic bidding for State business and in electronic reverse auctions.

Executive Decree 149, on e-government and simplification of formalities, of 20 November 2013, defines "e-government" as the use by government agencies of ICTs to transform relations with citizens and between government agencies and private businesses, in order to improve the quality of government services to citizens, promote interaction with private businesses, strengthen citizen participation through access to information and efficient and effective government services and contribute to transparency, participation and citizen collaboration. The Decree promotes plans for simplifying formalities in the central and institutional public administration in keeping with the principles of simplicity, economy, legality, celerity, presumption of truthfulness, reliability of information, privacy and confidentiality of personal information, transparency, preference for retrospective [rather than preventive] controls, minimizing formalities, acting for the benefit of the citizen, providing services free of charge and interconnection.

The interoperability of government services has been implemented in three areas: (i) automation of formalities and optimization of procedures, (ii) registration of public data, and (iii) financial data. The National Secretariat of the Public Administration has implemented the QUIPUX online system for handling documentation of public and private sector entities.

On the financial front, the Organic Code for Financial and Monetary Transactions, of 12 September 2014, governs the handling of electronic currency and empowers the Central Bank of Ecuador to implement, monitor and evaluate measures in this area. Decision No. 005-2014-M, on electronic currency, issued by the Monetary and Financial Policy and Regulation Board on 6 November 2014, lays down standards for the use of this means of payment, which is recognized by economic agents and managed exclusively by the Central Bank. It is used in electronic, mobile, electromechanical and fixed devices, smart cards, computers and other means produced as a result of technological advances.

In the area of taxes, both the Tax Code of 14 June 2005, as amended on 9 March 2009, and the e-Commerce, Electronic Signatures and Data Messages Act establish the validity of electronic notifications. The Act defines the concept of electronic invoice. The tax services are working to eliminate paper documents and automate procedures; agencies such as the National Customs Service of Ecuador and the Internal Revenue Service are good examples of this policy. The National Customs Service has implemented the Ecuapass computerized service and the Ecuadorian Single Window to develop smart risk-management systems, giving priority to protecting the security of taxpayers through electronic signature certificates. The Internal Revenue Service makes it possible to submit tax forms and make payments online and to implement electronic invoicing.

b) Consumer protection

The Constitution of Ecuador states that people have the right to have goods and services of optimum quality and to select them freely, as well as the right to receive accurate and non-deceptive information on the content and characteristics of such goods or services. It also regulates legal quality- control mechanisms and consumer-protection procedures, as well as sanctions for violating consumer rights.

The Organic Act on Consumer Protection (Act No. 2000-21), of 10 July 2000, establishes consumers' right to the protection of their life, health and safety as consumers of goods and services, as well as their right to protection from misleading or abusive advertising. It also includes the right to receive appropriate, truthful, clear, timely and complete information on goods and services.

Under the e-Commerce, Electronic Signatures and Data Messages Act, before a consumer or user indicates his or her acceptance of electronic records or data messages, he or she must be informed clearly, precisely and satisfactorily regarding the equipment and programs needed for access to the records or messages. In addition, the law establishes requirements for providing consumers with information on e-commerce transactions, including advertising and promotions, and regulates mechanisms for excluding

consumers from lists, message chains and databases in connection with sending data messages with information of any type.

c) Protection of personal data

In the area of privacy and personal data, the Constitution protects the right of persons, in all circumstances, not to have information concerning them demanded or used without their authorization, including information on their religious beliefs or associations or their political thought, as well as data on their health and sexual life, except as necessary for medical care.

It also recognizes the right of data subjects to know of the use, purpose, source and destination of their information. Persons responsible for databases containing personal information may disseminate the archived information with the authorization of the data subject or if required by law to do so.

Under the Constitution, the data subject may request that the party responsible for handling his or her information provide him or her access to the relevant files without charge, and that he or she be permitted to update, correct, remove or annul the data. When sensitive information is involved, the information may not be archived without authorization of the data subject, and security measures are mandatory. The Constitution also recognizes the inviolability and confidentiality of physical and virtual correspondence.Under the e-Commerce, Electronic Signatures and Data Messages Act, the confidentiality and non-disclosure of data messages must be protected. The Act makes punishable any violation – through electronic intrusion, illegal transfer of data messages or violation of professional confidentiality – of these principles. It also stipulates that preparing, transferring or using databases compiled directly or indirectly from the use or transmission of data messages requires the express consent of the data subject, unless the data are derived from publicly available sources. The data subject has the right to decide what information will be shared with third parties.

Under the Organic Act on the National Public Contracting System, of 4 August 2008, data provided to the portal at www.compraspublicas.gov.ec are considered confidential and may only be used for the purposes for which they have been provided.

The Organic Act on the National Registry of Public Data, of 31 March 2010, lays down the obligations of public and private sector institutions that currently manage or may in future manage databases or registries of public data on individuals or legal entities, their assets or property, and of users of public registries. Personal data must be kept confidential and access to them must be authorized by the data subject. Any private sector agency or person that holds personal data must establish security measures for protecting the privacy of personal data. Anyone requesting access to information regarding material assets must justify and explain the request, state what use will be made of the information and provide basic identification information.

d) Industrial and intellectual property

In the area of intellectual property rights, the Constitution of Ecuador guarantees the right of individuals to develop their creative capacities, to engage, in an ongoing and appropriate fashion, in cultural and artistic activities, and to enjoy protection of the moral and patrimonial rights associated with their scientific, literary or artistic productions.

In the international sphere, Ecuador has signed the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Universal Copyright Convention
- Common Provisions on Copyright and Related Rights, established by Decision 351 of the Commission of the Andean Community (Commission of Cartagena), which is in force for all countries of the Andean Community

Ecuador has also ratified the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO.

In the context of domestic legislation, the Intellectual Property Act, of 8 May 1998, protects copyright and related rights, as well as industrial property. In the area of copyright, there are provisions for the protection of computer programs and databases.

e) Domain names

In regard to domain names, NIC.ec is the entity responsible for administering the .ec domain, by delegation from IANA. In terms of domain-name dispute resolution, NIC.ec has adopted the arbitration procedure envisaged in the ICANN Uniform Domain-Name Dispute-Resolution Policy.

f) Cybercrime and information security

Cybercrimes are included in the Organic Comprehensive Criminal Code, of 10 February 2014, which punishes (i) violations of privacy committed by anyone who without proper authorization keeps, records, reproduces, disseminates or publishes personal data, data messages, voice, audio and video, postal objects, information contained in software, private or confidential communications of another person; (ii) fraudulent appropriation by electronic means; (iii) reprogramming or modification of information on mobile terminals; (iv) exchange, sale or purchase of information on mobile terminals; (v) suppression, alteration or assumption of identity and marital status; (vi) illegal disclosure of databases; (vii) illegal interception of data; (viii) electronic transfer of material assets; (ix) attacks against the integrity of IT systems; (x) offences against legally reserved public information; and (xi) access without consent to a computer, telematic or telecommunications systems.

In terms of procedure, the Organic Comprehensive Criminal Code lays down rules for intercepting communications or computer data pursuant to a court order, and defines the term "digital content".

As regards security of information, Decision JB-2012-2148 of the Banking Authority, of 26 April 2012, requires financial institutions to implement security measures for their electronic channels, including those used to provide mobile banking services, in order to ensure that transactions carried out through those channels have the necessary controls and security measures and elements to prevent fraudulent events and guarantee the security and quality of user information, as well as clients' assets that are in the custody of regulated institutions.

Ministerial Decision No. 166, on the government scheme for information security, of 20 September 2013, requires all departments of the central government and all government institutions to implement a government scheme for information security, which must include the following: (i) a policy on information security; (ii) organization of information security; (iii) file management; (iv) security of human resources; (v) physical and environmental security; (vi) management of communications and operations; (vii) access control; (viii) procurement, development and maintenance of information systems; (ix) management of information security incidents; (x) management of business continuity; and (xi) compliance.

g) Pending legislation and challenges

Several bills relating to data protection have been discussed by the National Assembly with a view to proposing a regulatory system that will be in line with the Directives for Harmonization of Data Protection in the Ibero-American Community issued by the Ibero-American Data Protection Network. In the area of information security, a national cybersecurity incident response team has not yet been set up.

EL SALVADOR

El Salvador has a number of laws for dealing with different e-commerce issues. In terms of substantive law, provisions from the following are applied: the Civil Code of 14 April 1860, which has been amended several times,[26] most recently on 11 October 1993; the Commercial Code, of 31 July 1970, most recently amended on 8 May 2014; the Consumer Protection Act, of 16 May 2006, most recently amended on 19 February 2013; the Tax Code, of 22 December 2000, most recently amended on 21 December 2009, and the Customs Simplification Act, of 13 January 1999, most recently amended on 4 July 2012.

In terms of procedural law, the Code of Civil and Mercantile Procedure, of 27 November 2008, as amended on 31 May 2010, recognizes the probative validity of data and data or information storage resources, including magnetic media and software, and admits them as evidence in court proceedings.

a) Electronic transactions/electronic signatures

With regard to electronic transactions and electronic signatures, neither the Civil Code nor the Commercial Code explicitly regulates electronic contracting. Nevertheless, the rules applying to the formation and conclusion of contracts, as well as those establishing the formalities to which contracts must conform, are applicable to electronic transactions.

For mercantile and financial matters, a number of provisions explicitly recognize the functional equivalence of printed documents with handwritten signatures and of digital documents with digital signatures. Both the Banking Act, of 30 September 1999, most recently amended on 20 April 2012, and the Electronic Book-Entry Securities Act, of 22 March 2002, most recently amended on 20 April 2012, recognize the legal validity of electronic transactions and electronic signature.

The Banking Act governs financial intermediation and other banking operations, under the oversight of the Central Reserve Bank of El Salvador and the Office of the Superintendent of the Financial System. It provides that interbank credit and debit transactions may be conducted by electronic exchange of data.

[26] The Civil Code has been amended 19 times.

It also recognizes the probative validity of records or logs kept in computer systems, as well as printed material reflecting transactions made by such records containing digital signatures or personal identification numbers (PINs) of authorized users of the systems. The law also requires the banks to accept electronic instructions for debit or credit operations.

As regards the securities market, the Electronic Book-Entry Securities Act also recognizes the use of electronic media for electronic transactions. It provides that electronic book-entry securities represent negotiable transferable securities in an electronic record and not in a hardcopy document. It also establishes that digitized or registered securities, like physical securities, are a valid type of security, and it recognizes that electronic book entries are obligatory for securities traded on the securities exchange. Issuers of stocks represented by book-entry securities are allowed to maintain an electronic registry of shareholders in place of the traditional shareholder registry book.

The Tax Code authorizes tax returns filed via electronic communications networks such as the Internet. It also authorizes the Tax Administration to use media of its own to access the billing systems of financial or similar institutions, as well as credit card management systems.

The Customs Simplification Act is an important advance for electronic transactions, since it incorporates measures consistent with the Regulations to the Unified Central American Customs Code and the CAFTA-DR Agreement and contains some provisions aligned with the UNCITRAL Model Law on Electronic Signatures. It authorizes the electronic transmission of declarations of merchandise, certificates or certifications of origin, shipping manifests, bills of lading and other documents needed to carry out foreign trade transactions. It also authorizes payment of customs duty obligations by electronic funds transfers from the bank accounts of those declaring items, customs agents or third parties, to the checking account of the Office of the Treasury.

The Act also provides that the use of computerized and electronic media for information exchange is to be fully valid for the formulation, transmission, recording and archiving of merchandise declarations and related information, including required attachments, and as a way of certifying payment of amounts due, and that their use is to have the same legal effect as would the delivery of the same information using physical media.

In order to ensure the authenticity, confidentiality and integrity of the information exchanged in systems that interact with customs systems, and to prevent its being subsequently contested, the Act establishes systems to certify the information transmitted, which are to be operated by certifying entities. The Act establishes that for the exchange of general information, each authorized user will have a pair of interconnected passwords or unique keys constituting the digital or electronic signature, which is the digital equivalent of the written signature.

b) Consumer protection

In terms of consumer protection, the Constitution of El Salvador recognizes the protection of consumers' interests as a fundamental right. Based on the Constitution, the Congress passed the Consumer Protection Act, which incorporates several precepts laid down in United Nations General Assembly resolution 39/248, on guidelines for consumer protection, including the right of consumers to information, as well as the right to have access to safe products.

Among other things, the Act recognizes the following rights of consumers: (i) to receive information that is complete, accurate, truthful, clear and timely regarding the characteristics of products and services; (ii) to receive information on the risks or side effects of products, as well as on the terms of contracts; (iii) to be protected from misleading or false advertising; (iv) to be educated and informed on consumer issues; (v) to have free choice and equal treatment; (vi) to be protected against the risk of receiving products or services that endanger life, health or personal integrity; (vii) to demand and receive compensation for hidden defects; (viii) to be protected from abusive practices and clauses in contracts; and (ix) to have access to a complete reading and explanation of all obligations and conditions stipulated in contracts and attachments thereto. In January 2013, the Act was amended to include the right of consumers to opt out without incurring liability within eight days after signing the contract, in the case of contracts made remotely, including through electronic media.

c) Protection of personal data

As regards the protection of personal data and the right to privacy, El Salvador has signed the American Convention on Human Rights and has incorporated the right to privacy as a fundamental right in several provisions of its Constitution. It prohibits interference with and intervention of telecommunications, although as an exception, it authorizes temporary intervention subject to a written and well-founded court order.

The Natural Persons Names Act, of 4 May 1990, contains a number of measures protecting the holder of a name against its improper use and punishes anyone

who usurps the name. The Consumer Protection Act includes measures for protecting consumers, prohibiting providers from sharing personal and credit-related information about a consumer, either to providers or through entities specializing in providing information services, without the authorization of the consumer. It lays down obligations for providers of information services, requiring them to give consumers access to information on their own data and to request that such data be updated, modified or removed free of charge. Such entities have the obligation to correct false, outdated or inaccurate information within no more than ten days from the date on which they receive a request from the party concerned.

As concerns financial matters, the Banking Act provides that information on deposits and savings received by banks shall be confidential, and that information on such transactions may be disclosed only to the account holders concerned, their legal representatives or the Directorate of Internal Revenue when so required for oversight purposes. The Act provides that banking confidentiality shall not be used to obstruct criminal investigations, oversight activities, determination of taxes or collection of tax obligations, or to prevent garnishment of assets. The Banking Act stipulates that the Office of the Superintendent of the Financial System shall maintain a credit information service to maintain information on users of institutions in the financial system, in order to facilitate assessment by the institutions of the risks involved in their operations.

The Regulation of Credit Reporting Services Act, of 27 July 2011, most recently amended on 20 April 2012, governs the handling of data on consumers' and clients' credit records. The purpose of the Act is to guarantee the right to honour, personal and family privacy and personal image by ensuring that information on consumers or clients that is included or likely to be included in a data service administered by a duly accredited legal entity is reliable, truthful and up-to-date and that it is properly handled. The Act also regulates the activities of legal entities in the public or private sector that are authorized to operate as data services and economic agents that maintain or handle data on the credit records of consumers or clients.

The Electronic Book-Entry Securities Act provides that deposits of securities received by depositories must be treated as confidential and that information on such transactions must only be given to account holders or their legitimate representatives. It provides that confidentiality shall not be used to obstruct criminal investigations or to prevent garnishment of assets or the oversight functions of the Office of the Superintendent of the Financial System.

In regard to customs , the Customs Simplification Act establishes the obligation to maintain the secrecy and confidentiality of the personal and normative information of those executing digital signatures that have been digitally certified. Such information may in no case be cross-referenced, profiled or used for purposes other than those provided for in the Act, except if the data subject agrees expressly in writing to its use for a different purpose.

d) Industrial and intellectual property

As regards intellectual property, the Constitution authorizes the granting of privileges for a limited time to discoverers, inventors and improvers of productive processes. The Intellectual Property Act, of 16 August 1993, most recently amended on 20 April 2012, grants copyright protection to artistic and literary works, including computer programs and compilations, a category that includes computer databases. The Act deems any permanent or temporary electronic storage of a work to be a reproduction. As concerns the related rights of artists, performers, producers of phonograms and broadcasters, it defines the concepts of phonogram and videogram and recognizes the right of public communication by any medium.

The Trademarks and Other Distinguishing Marks Act, of 8 July 2002, most recently amended on 19 April 2013, recognizes that acts of unfair competition, i.e., those carried out as part of mercantile activity or for purposes connected therewith, that are contrary to honest commercial usage and practice, are to be considered as such even if carried out through electronic communication or e-commerce media. The Act permits the use of electronic media to register distinguishing marks. This provision is consistent with the Act on Uniform Procedures for the Presentation, Processing and Registration or Deposit of Instruments in the Registries of Real Estate and Mortgages, Commercially Owned Real Estate, Commerce and Intellectual Property, which provides for the use of fax and e-mail addresses in requests for the recording of instruments in registries for purposes of notification to requesters by registry personnel.

As regards international commitments, El Salvador has ratified the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances
- Universal Copyright Convention

- Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- Central American Agreement for the Protection of Industrial Property
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

The Trademarks and Other Distinguishing Marks Act establishes the requirements and terms for the protection of trademarks, trade names, denominations of origin and other distinguishing marks. This Act, which is consistent with the CAFTA-DR Agreement, provides that in cases of cyberpiracy of trademarks, the national entity responsible for administering the country code top-level domain (Asociación SVNet) must have in place dispute-resolution procedures based on the principles of the Uniform Domain-Name Dispute-Resolution Policy and must provide public online access to a reliable and accurate database with contact information for those registering domain names, while observing the legal provisions relating to the protection of their privacy.

In this regard, the Asociación SVNet (NIC-El Salvador), which is responsible for issuing and updating policies for the functioning of the top-level domain .sv, has adopted its own Uniform Dispute-Resolution Policy and related regulations, under which it establishes rules on arbitration to resolve domain-name disputes. The policy recognizes the Centre for Mediation and Arbitration of the American Chambers of Commerce. The instruments adopted by the Asociación SVNet make no reference to the ICANN Uniform Domain-Name Dispute-Resolution Policy.

f) Cybercrime and information security

In regard to crime, the Special Act against Acts of Terrorism, of 17 October 2006, most recently amended on 20 November 2014, includes some cybercrimes. It provides penalties for facilitating the commission of any of the designated crimes using equipment, media, programs, computer networks or any other computer application to intercept, interfere with, deflect, alter, damage, render unusable or destroy data, information, electronic documents, data media, programs or information and communication or telematics systems associated with public, social, administrative, emergency or national security systems, as well as those of national, international or foreign entities. It provides the same sanctions for creating, distributing, marketing or possessing programs capable of producing the abovementioned effects.

The Special Act to Sanction Customs Violations, of 29 October 2001, most recently amended on 20 April 2012, in article 24 defines the following cybercrimes, which carry prison sentences of 3 to 5 years: (i) accessing by any unauthorized means the computer systems used by the Customs Service; (ii) taking control of, copying, destroying, rendering unusable, altering, facilitating the transfer of or possessing any computer program designed by or for the Customs Service or its databases, that the Customs Service uses exclusively in its control functions and services, without authorization from Customs authorities; (iii) damaging the material or physical components of the devices, machines or accessories supporting the functioning of the computer or information systems designed for the operations of the Customs Service in order to obstruct their functioning or obtain benefits for him or herself or for third parties; (iv) facilitating the use of a username and password assigned to enter the computer systems (with provision for sentences of 1 to 3 years if the activity is facilitated because of negligence); and (v) manipulating the computer or communications systems in order to obstruct any control function provided for in the system.

In addition to the cybercrimes envisaged in the Special Act against Acts of Terrorism and the Special Act to Sanction Customs Violations, it should be noted that neither the Criminal Code, of 10 June 1997, most recently amended on 16 October 2014, nor the Code of Criminal Procedures, of 30 January 2009, most recently amended on 28 January 2015, refer to cybercrimes or to data messages. However, the provisions of these laws can be applied to cybercrime. It is up to ministerial and judicial authorities to assess the IT elements involved in such crimes.

g) Pending legislation and challenges

El Salvador does not have a national strategy on e-commerce; however, it participates in the Mesoamerican Information Highway. Among the main bills currently under review in the Legislative Assembly is a draft bill on regulation of e-commerce, documents and digital signatures. The Legislative Assembly is considering a proposal for new legislation to be entitled Special Act against Cybercrime.

Among the main challenges facing the country is the need for a general law on data protection that would

be in line with the Directives for Harmonization of Data Protection in the Ibero-American Community issued by the Ibero-American Data Protection Network. El Salvador also needs to set up a national computer security incident response team.

GUATEMALA

The Electronic Communications and Signature Recognition Act, of 23 September 2008, is the main legislation governing e-commerce. It may also be applied, however, to some aspects of e-commerce in the civil, mercantile, financial, administrative and criminal spheres, as described below.

In addition, discussions are ongoing on a digital agenda that would include strategies for promoting e-commerce.

a) Electronic transactions/electronic signatures

International electronic transactions are covered by the CAFTA-DR Agreement and the Regulations to the Unified Central American Customs Code, while the Electronic Communications and Signature Recognition Act is applicable to all types of electronic communications, transactions or legal acts, either public or private, national or international, with the exceptions envisaged in therein.

The Electronic Communications and Signature Recognition Act stipulates that e-commerce involves matters arising from any commercial relationship, whether contractual or not, that is based on the use of electronic communications or similar media. The Act incorporates several precepts from the UNCITRAL model laws on electronic commerce and on electronic signatures. It also establishes the legal requirements that must be met by electronic communications and the elements that must be present in the formation and conclusion of contracts by electronic means.

The Act also defines the requirements that must be met by electronic signatures and digital certificates, as well as the functions of certification service providers that are supervised by the Ministry of the Economy. It also recognizes the functional equivalency of printed documents with handwritten signatures and electronic documents with advanced electronic signatures backed by a digital certificate. It includes provisions governing specific topics, such as transport of merchandise and measures to protect consumers in online transactions.

The Civil Code, of 14 September 1963, establishes principles governing standard-form contracts and recognizes the functional equivalence of physical signatures and signatures that are electronic, digitized or printed by any electronic means available to the Registrar of the General Property Registry with respect to the items recorded in the electronic records.

The Commercial Code, of 28 January 1970, requires that documentation and information related to mercantile activities be preserved for five years and that certain types of acts be recorded in the Mercantile Registry or related books or systems. In the financial area, the Organic Act of the Bank of Guatemala, of 13 May 2002, authorizes the Bank of Guatemala to take steps to ensure the proper operation of the settlements systems, pursuant to the guidelines issued by the Monetary Board. The Monetary Board issued Regulations on the Real-Time Gross Settlement System, of 30November 2005, which covers, among other things, the use of digital signatures. The Securities and Merchandise Market Act, of 24 June 1996, authorizes oversight and accounting for transactions involving securities represented by accounting entries, to be carried out by normal accounting, documentary or electronic procedures.

As regards electronic transactions with the Government, the State Procurement Act, of 31 January 2009, establishes the operational basis for the online government procurement system (Guatecompras). The Act provides that in quoting and bidding procedures, entities must publish on the Guatecompras system the terms for quoting or bidding, technical specifications, evaluation criteria, questions and answers, a list of bidders, reports on final awards, and procurement contracts. It also authorizes electronic notifications through the Guatecompras system and allows for changes in the terms for price quotations to be published through the system.

The regulations to the State Procurement Act define the powers of the Directorate for Oversight of State Contracts and Procurement, and Ministerial Decision 1-2006 deals with the Management Linkage System, the Integrated Accounting System and the Guatecompras system. In addition, Decision 30-2009 of the Directorate for Oversight of State Contracts and Procurement officially recognizes the web address of the State Contracting and Procurement Information System (www.guatecompras.gt) and specifies, among other things, what types of users may access the system and how the Directorate for Oversight of State Contracts and Procurement is to manage access to the system's accounts.

On tax matters, the Tax Code, of 3 April 1991, empowers the Tax Administration to (i) set up procedures

for processing, transmitting and preserving invoices, books, records and documents by electronic means, and (ii) require taxpayers to pay taxes electronically. It also allows taxpayers to meet their tax obligations by using electronic forms and to submit by electronic means their tax returns (including affidavits), financial statements and the annexes thereto or any information they are required by law to supply, provided they are identified with a confidential electronic password which is equivalent to a handwritten signature, that they ensure the integrity of the information submitted, or that the Tax Administration provides them with a physical or electronic notice of receipt.

Under the Tax Code, both the Value Added Tax Act and the Income Tax Act, along with the regulations thereto, allow the use of electronic means for interaction between taxpayers and the tax authorities, and for taxpayers to fulfil their tax obligations.

Finally, with regard to customs, Guatemala considers the Unified Central American Customs Code and its Regulations, as well as the CAFTA-DR Agreement, applicable to its foreign trade operations.

b) Consumer protection

In the area of consumer protection, the Constitution of Guatemala prohibits excessive practices that lead to a concentration of goods and means of production that would be detrimental to the collective well-being, while protecting consumers and users by ensuring that the quality of products for both domestic consumption and export is maintained. Pursuant to the Constitutional mandate to protect the interests of consumers, the Congress of the Republic issued its Decree No. 6-2003,adopting the Consumer and User Protection Act, of 10 March 2003.

The Promotion of Competition and Effective Consumer Protection Act incorporates the basic principles of consumer relations set forth in United Nations General Assembly resolution 39/248, on guidelines for consumer protection. The Act states that the rights and guarantees it provides for are inalienable and are in the public interest.

It also recognizes, among others, the following rights: (i) the right of consumers to safety; (ii) the right to information; (iii) freedom to conclude contracts; (iv) the right to reparation, compensation, reimbursement or exchange of the goods in case of non-compliance; (v) the right of consumers to be educated, and (vi) the right to opt out without incurring liability, within five days from the date of signing the contract or from the date on which the contract was concluded when this was done remotely, especially by telephone or at the domicile of the consumer or user. None of these laws provide special treatment for online transactions with respect to traditional ones.

c) Protection of personal data

The Constitution of Guatemala protects privacy by enshrining as a fundamental right the inviolability of private correspondence and of telephone, radio, cable and other communications by means of modern technology. It also provides that everyone has the right to be aware of any information concerning them that is kept in archives, files or any other type of state record, and the purpose of such information, as well as to correct, rectify and update such information. In addition, the Tax Code protects the confidentiality of tax information.

In the financial sphere, Decree No. 19-2002, adopting the Banks and Financial Groups Act, of 15 May 2002, governs bank secrecy and provides that, except in the case of obligations and duties established in the legislation on laundering of money or other assets, directors, managers, legal representatives, officials and employees of banks may not reveal any information.

Decree No. 57-2008, enacting the Access to Public Information Act, of 23 October 2008, protects the right of all individuals to know and protect any personal information concerning them that is being kept in state archives, as well as to update such information. It establishes the right of habeas data as a guarantee for all individuals to exercise the right to know what information about them is kept in archives, files, records or any other type of public record, and the purpose for which the information is collected, as well as to protect, correct, rectify or update the information. Those who gather the information may not disseminate, distribute or market the personal data contained in the information systems developed as part of their duties, except with the express written consent of the individuals to whom the information refers. Likewise, sensitive information or sensitive personal information may not be sold through any medium.

d) Industrial and intellectual property

Copyright and patent rights are enshrined in the Constitution. The Copyright and Related Rights Act, of 19 May 1998, most recently amended on 27 September 2000, protects the rights of authors of artistic, scientific and literary works, including computer programs and databases. It also recognizes that any permanent or temporary storage of a work in any type of supporting material, format or medium is considered a reproduction. As regards related rights of artists, per-

formers and radio broadcasters, the Act defines the concepts of phonograms and videograms and recognizes the right to communicate with the public by any medium or procedure, analog or digital.

The Industrial Property Act, of 18 September 2009, does not include economic, advertising or business methods or computer programs in isolation as patentable inventions.

The Criminal Code, of 27 July 1973, punishes the following offences related to industrial property and intellectual property: (i) false attribution of copyright holder, artist, performer, producer of a phonogram or broadcasting organization; (ii) presentation, performance or public playing or transmission, communication, broadcast or distribution of a protected literary or artistic work without the authorization of the copyright holder; (iii) public performance or transmission of a protected phonogram without the authorization of its producer; and (iv) reproduction or rental of copies of protected literary, artistic or scientific works, without the authorization of the copyright holder; (v) disclosure of industrial secrets, and (vi) use of registered trademarks or imitations thereof, among others.

On the international front, Guatemala has ratified the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances (2012)
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Lisbon Agreement for the Protection of Appellations of Origin and their International Registration
- Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting organizations (Rome Convention)
- WIPO Patent Cooperation Treaty
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO.

e) Domain names

The Domain-Name Dispute-Resolution Centre for the top-level domain name .gt - Guatemala, housed at the country's Universidad del Valle, is the entity responsible for issuing and updating policies for operation of the country's top-level domain name, and it has adopted the principles of the Uniform Domain-Name Dispute-Resolution Policy of ICANN.

f) Cybercrime and information security

The Criminal Code of Guatemala provides sanctions for the following: (i) destroying computerized records; (ii) altering computer programs; (iii) illicitly reproducing computer programs; (iv) creating a database or computerized record with data that could jeopardize personal privacy; (v) using computerized records or computer programs to hide, alter or distort information required for a commercial activity or for meeting an obligation to the State, or hiding, falsifying or altering the accounting statements or financial status of an individual or legal entity; and (vi) distributing destructive computer programs.

As regards information security, Guatemala has a national computer security incident response team which was set up without going through legal formalities. It is considered advisable, however, to pass legislation or regulations to endow it with authority and resources.

g) Pending legislation and challenges

One of the main challenges faced by Guatemala is the need to update its criminal legislation, both substantive and procedural, in order to strengthen its ability to combat cybercrime. Guatemala is also preparing regulatory and legal changes that would allow for the creation and operation of the national computer security incident response team within the Ministry of the Interior. In addition, the regulatory framework on protection of data must be updated to bring it in line with the commitments undertaken by Guatemala in the Ibero-American Data Protection Network.

HAITI

Haiti has no legislation on e-commerce; however, the parliament is considering a bill on the matter and is in the process of discussing a digital agenda that includes strategies for promoting e-commerce.

a) Electronic transactions/electronic signatures

Haiti does not currently have a law on electronic transactions or on electronic signatures. This is an important area of opportunity that should be borne in mind in connection with the project on Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR).

b) Consumer protection

Haiti has no legislation on consumer protection; however, a bill on the subject, introduced in 2010, is under review in the legislature.

c) Protection of personal data

The Constitution of the Republic of Haiti, of 10 March 1987, enshrines as fundamental rights the right to privacy and to a private life. There is still no specific law on protection of information. The inclusion of Haiti in the Ibero-American Data Protection Network can help move the legislative process along and expedite passage of a special law on the subject.

d) Industrial and intellectual property

The Constitution of Haiti guarantees protection of intellectual property rights. However, the main legislation on the subject is the Decree of 9 January 1968, on copyright protection for authors of literary, scientific and artistic works, which protects the moral and material rights of authors in respect of literary, musical and artistic works, as well as cinematographic and photographic works. The Decree does not expressly cover all related rights (rights of producers of phonograms or of broadcasting organizations, for example), nor does it cover computer programs or databases which are protected as literary works under the TRIPS Agreement.

The Decree grants copyright holders exclusive rights to publish, reproduce, perform, adapt, disseminate, translate, distribute and arrange their works. It also recognizes intangible, inalienable moral rights and protection from garnishment. Copyright protection is extended throughout the life of the right holder plus 25 years after his or her death. Violations of copyright may entail confiscation of forged copies, and the creator of the forgery may be required to pay compensation for damages to the right holder.

On the international level, Haiti has signed the following instruments:

- Paris Convention for the Protection of Industrial Property
- Berne Convention for the Protection of Literary and Artistic Works
- Inter-American Convention on the Rights of the Author in Literary, Scientific and Artistic Works
- WIPO Patent Cooperation Treaty
- Beijing Treaty on Audiovisual Performances

Haiti has also adopted the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO.

e) Domain names

The Sustainable Development Network of Haiti is responsible for managing the top-level domain name .ht. As regards the resolution of domain-name disputes, the Network has not yet published a policy in keeping with the ICANN Uniform Domain-Name Dispute-Resolution Policy.

f) Cybercrime

The Criminal Code of 1985 does not cover cybercrime, and the Code of Criminal Procedure does not include measures for handling digital evidence on crime or criminal investigation.

g) Pending legislation and challenges

Cyberlegislation in Haiti can be developed extensively through the country's participation in the HIPCAR project on issues of e-commerce (transactions), e-commerce (evidence), privacy and protection of data, interception of communications, cybercrime and access to public information (freedom of information).

Some of the main challenges faced by Haiti are the lack of connectivity and of ICT capacities.

HONDURAS

The 2014-2018 Digital Agenda for Honduras provides for strengthening legislation on e-commerce in order to promote its development. There is a proposal for the creation of a law on e-commerce that would help strengthen the existing legal framework. The main laws currently in force are the Electronic Signatures Act, issued by Decree No. 149-2013, of 11 December 2013, and the Act on Efficient and Transparent Procurement through Electronic Means, issued through Decree No. 36-2013, of 5 August 2014, which governs the public sector. The Civil Code of 8 February 1906, as amended in 2009, also covers the conclusion, formalization, validity and efficacy of contracts.

a) Electronic transactions/electronic signatures

The Government of Honduras has signed the United Nations Convention on the Use of Electronic Communications in International Contracts, which was incorporated into the domestic legislation by Decree No. 13-2009. The Electronic Signatures Act includes the provisions of the UNCITRAL Model Law on Electronic Signatures recognizing and regulating the use of such signatures for data messages and granting them the same validity and legal effect as handwritten signatures expressing the will of signatories.

The Act makes a distinction between electronic signatures and advanced electronic signatures, which therefore have different legal effects, and recognizes the functional equivalency between printed documents and documents contained in data messages, as well as between handwritten signatures and digital signatures that have been certified by an accredited service provider. State authorities in the different branches of government are empowered to carry out administrative procedures through electronic means and to use electronic files and digital signatures in their actions, either among themselves or with private parties.

The Commercial Code of May 1950 permits merchants to conduct their accounting via electronic systems, including accounting records and special books and records, documents, invoices, sent and received mail, background information related to tax obligations and, where relevant, programs, sub-programs and other records processed through electronic or computer systems.

The Act on the Financial System, of 22 September 2004, allows institutions in the system to offer and provide financial products and services via electronic media and recognizes the legal force of electronic signatures, which have the same validity on electronic documents as written signatures on paper documents, provided that the electronic signature is backed by a recognized certificate and a secret code generated by a secure signature-creation device. Such signatures are admissible as evidence in judicial proceedings and are valid as public instruments.

In the administrative realm, the State Contracting Act, of 29 June 2001, provides for information technologies to be used in managing contracting systems. However, the Act on Efficient and Transparent Procurement through Electronic Means, issued by Decree No. 36-2013, of 5 August 2014 (Procurement Act) expands the range of public purchases of goods or services to include purchases made by electronic catalogue, which include framework agreements, joint purchases and reverse auctions carried out by centralized and decentralized public agencies.

The Property Act, of 15 June 2004, which governs acts related to chattels, real estate, commercial and intellectual property, as well as to rights in rem and other rights, lays down measures for streamlining related procedures and authorizes the Uniform Property Registry to use advanced legal, administrative and technological tools to ensure security and transparency, reduce costs and expedite registration transactions and administrative procedures, including through mechanisms for electronic certification of legal instruments, contracts or rights documented in public files, with the same legal force and probative value as documents of public record.

The Tax Code, of 30 May 1997, includes a number of measures designed to facilitate online transactions, including by confirming taxpayer actions. The Regulations on the System for Issuing and Generating Electronic Tax-related Documents, of 23 October 2014, govern procedures, requirements, terms of use and obligations of taxpayers using software to issue or generate tax-related documents, which must be duly authorized by the Executive Directorate of Revenues in respect of different types of tax-related documents.

The General Customs Act, of 14 December 1987, does not mention the use of electronic media for customs clearance and related procedures, but does recognize the applicability of international treaties, e.g., the Unified Central American Customs Code and its Regulations, which do cover electronic media. With the Act on Implementation of the CAFTA-DR Agreement, Honduras incorporated the provisions of that Agreement into its domestic legislation.

b) Consumer protection

The Constitution of the Republic of Honduras, of 11 January 1982, most recently amended on 4 May 2005, requires the State to recognize, guarantee and promote consumer freedom. Under the Constitution and pursuant to United Nations General Assembly resolution 39/248, on Guidelines for consumer protection, the Consumer Protection Act, of 1 April 2008, incorporates into Honduran law the fundamental rights of consumers to information and to have access to safe products (http://www.lexadin.nl/wlg/legis/nofr/oeur/lxwehnd.htm).

The Act regulates “sales by mail and the like”, including in the latter category offers of goods and services made via postal mail, telecommunications and electronic media and accepted by those same media. Online transactions are subject to the rules regarding consumers’ right to clear information – in Spanish and with legible characters – that is truthful, complete and timely (including information on prices and on the quality of and guarantees applying to goods and services). Such transactions are also subject to the prohibition on misleading advertising and abusive clauses in membership contracts.

The Regulations to the Consumer Protection Act were adopted by Decision No. 15-2009, of 15 April 2009. Among other things, the Act describes protective

measures that consumers can take through consumer associations, and arbitration procedures and mechanisms for controlling abusive clauses. However, online consumers are not included.

c) Protection of personal data

The Constitution of the Republic of Honduras enshrines the right to honour, personal and family privacy and personal image, and the inviolability and privacy of communications, and it provides for habeas data. The Public Information Transparency and Access Act establishes mechanisms to ensure the protection, classification and security of public information and respect for restrictions on access to reserved information, confidential information provided by individuals and confidential personal data.

The Act also governs the handling of personal data and makes a distinction between personal data and confidential personal information. It regulates the guarantee of habeas data and prohibits compelling anyone to provide personal data that could cause discrimination or jeopardize the person in material or moral terms. It also requires that personal information be protected. The Act punishes anyone who refuses to give personal information to the legitimate data subject, his or her heirs or a competent authority. It also provides sanctions for gathering, capturing, transmitting or disclosing personal information, or refusing to correct or update it or to remove false information or confidential personal data contained in any file, record or database of an institution that is subject to this law. The sanctions are imposed without prejudice to the civil or criminal liability that may result.

d) Industrial and intellectual property

The Constitution of Honduras provides that all authors, inventors, producers and merchants have exclusive ownership of their works, inventions, trademarks and business names, pursuant to the law.

The Copyright and Related Rights Act, issued by Decree No. 4-99, protects the authors of literary and artistic works and computer programs, as well as artists, performers, producers of phonograms and broadcasting organizations. Computer programs are considered literary or artistic works. The Act includes as a right of ownership the authority to access or grant public access to computer databases via telecommunications media.

The Industrial Property Act, issued by Decree No. 12-99, provides that computer programs considered in isolation are not inventions, and therefore are not patentable.

On the international front, Honduras has ratified the following instruments:

- Paris Convention for the Protection of Industrial Property
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Convention for the Protection of Producers of Phonograms
- Berne Convention for the Protection of Literary and Artistic Works
- WIPO Patent Cooperation Treaty
- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances (2012)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO
- Central American Agreement for the Protection of Industrial Property and
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)

e) Domain names

The Sustainable Development Network of Honduras (NIC Honduras (www.nic.hn)) is the agency responsible for administering the top-level domain .hn. It has adopted the principles of the ICANN Uniform Domain-Name Dispute-Resolution Policy for its dispute-resolution policy and regulations.

The Industrial Property Act deems a distinguishing mark to be in use in business when it is adopted as a domain name, an e-mail address or as a name or designation in electronic or similar media that serve as vehicles for electronic communications or e-commerce.

f) Cybercrime and information security

The Criminal Code provides sanctions for intercepting communications, including those sent through electronic means or computers. It establishes penalties for any act of destroying, altering, rendering unusable, or in any other way damaging the data, programs or electronic documents of another contained in networks, media or computer systems. It also provides penalties for damaging media or channels of communication.

It also sanctions the destruction, concealment or forgery of accounting records, company books, legal documents, certifications, affidavits, personal identity, data, records, financial statements, documents stored

in magnetic or electronic form, or of other information of an individual or legal entity, in order to obtain, maintain or extend a capital or credit facility of a supervised institution, or in order to cover up, distort or maliciously modify credit or debit transactions, direct or contingent obligations, illiquidity, insolvency or other facts that must be recorded in accounting records or other records.

The Act provides prison sentences for illegally accessing data processing systems of supervised institutions for the purpose of altering, deleting, damaging or taking records, files or other information of such institutions or their clients for benefit of self or another. The same sentences apply for using any procedure to access or improperly use an institution's databases to steal money by electronic transfer from one account to another account in the same or another institution.

On security of information, the Property Act requires the physical medium of official instruments, contracts or documents authorized or certified by a notary to include fraud-prevention measures and to permit verification of the parties' statements in forms such as encrypted barcodes, fingerprint identification of parties appearing and other means made possible by technological developments. The Act establishes fines for (i) altering the content of certification entries, record entries and registries; (ii) failing to comply with security standards for digital files and media; (iii) accessing electronic files or databases without authorization; (iv) taking or copying computer applications and technologies without authorization; and (v) installing software without authorization.

g) Pending legislation and challenges

Honduras needs to adopt the proposed legislation envisaged in the 2014 Digital Agenda for Honduras, including the e-commerce bill, of 14 August 2014, and the preliminary bill on adoption of the Council of Europe's Convention on Cybercrime. The regulations to the Electronic Signatures Act need to be drafted the Consumer Protection Act needs to be expanded to protect online consumers. A national computer emergency response team or computer security incident response team is also needed.

MEXICO

As a result of the Constitutional amendments of 11 June 2013, access to ICTs, including to broadband Internet, was recognized as a fundamental right. Thus, the National Digital Strategy and the National Development Plan 2013-2018 seek to facilitate an ecosystem for the digital economy, clearly signalling the Federal Government's commitment to promote e-commerce.

Mexico has no specific e-commerce legislation; rather, a number of civil, mercantile, administrative and tax laws have been amended to provide for the use of data messages and electronic means – specifically, electronic signature, advanced electronic signature and digital certification furnished by governmental or private-sector providers of these services – and to recognize their legal validity in contracts made by companies, consumers or government entities.

a) Electronic transactions/electronic signatures

In the area of civil law, the Federal Civil Code of Mexico allows parties to express their will remotely and makes handwritten and electronic signatures functionally equivalent. Moreover, the Federal Code of Civil Procedure allows data messages to be presented as evidence and sets rules for establishing their evidential value.

In the mercantile area, the Commercial Code includes a special chapter on e-commerce, incorporating much of the content of the UNCITRAL model laws on electronic commerce and on electronic signatures, and it regulates, among other matters, electronic signatures, advanced electronic signatures, certification services and the admissibility of data messages as evidence at trial. The regulations to the Commercial Code on certification service providers, general rules and the agreement amending them go into greater detail on technical, administrative and legal requirements for their operation in order to strengthen the legal framework governing providers of certification services.

Steps have also been taken to implement laws and regulations on the Public Registry of Commerce through electronic means, including inter alia measures governing the Single Registry of Chattel Mortgages, which operates on the website http://www.rug.gob.mx , which enables financial institutions or creditors to record documentation whereby liens, special privileges or retention rights on chattels are set up, transmitted, modified or cancelled.

The Credit Institutions Act allows financial institutions to provide their services via electronic means. As regards online banking and mobile banking, the General Provisions on Credit Institutions issued by the National Banking and Securities Commission, known as the Single Circular on Banks, establish rules for transactions involving electronic payments, including mobile banking services.

In the area of public administration, the Federal Administrative Procedures Act, the Procurement, Leasing and Public Sector Services Act and the Public Works and Related Services Act all provide for the use of electronic media for interaction with the federal Government through systems that use advanced electronic signatures backed by digital certificates, both in administrative procedures and in government contracts.

The Advanced Electronic Signatures Act and the regulations thereto reinforce the legal framework for online communications using digital signatures and certificates between public entities at the three levels of government, i.e., federal, state and municipal.

The federal executive branch has issued a decision aimed at issuing policies and provisions for the National Digital Strategy relating to ICTs and security of information. The idea is also to draw up the general administrative manual on these matters, so as to encourage the use of cloud solutions by federal agencies and promote practices that will ensure information security.

In the area of tax law, the Federal Tax Code, the Customs Act and the Social Security Act allow tax authorities to use electronic means in a variety of procedures, processes and documents (including digital tax receipts). These laws recognize handwritten and electronic signatures as functionally equivalent and set forth rules governing the use of advanced electronic signatures backed by digital certificates. The provisions of these laws are described in greater detail in administrative regulations issued by the federal executive branch.

b) Consumer protection

The Federal Consumer Protection Act includes a special chapter with rules governing consumers' rights when executing transactions electronically. It recognizes ethics codes as valid self-regulatory mechanisms that can serve as a basis for seal of trust systems consistent with international best practices, such as the seal of trust of the Mexican Internet Association. This system is part of the Asia Pacific Trustmark Alliance that operates in the Asia-Pacific region and is consistent with the APEC Privacy Framework.

The seal of trust is also designed to serve as an efficient tool for enforcing obligations in regard to protection of personal information.

c) Protection of personal data

Article 6 of the Constitution recognizes the protection of personal data as a fundamental right, and a number of sectoral laws, such as the Federal Act on Transparency and Access to Public Government Information, the Credit Institutions Act and the Federal Act on Consumer Protection, include measures protecting individuals from false or inaccurate personal information.

The regime for protection of personal data was completed with the adoption of the Federal Act on Protection of Personal Data in the Possession of Individuals and the Regulations thereto. Thus, there is now a general law on the handling of personal data by individuals or legal entities in the private sector who collect and process personal data, independently of the sector or industry involved. This provides a protection system that is consistent with international standards, in particular, the European model, the APEC Privacy Framework, bearing in mind the terms of the North American Free Trade Agreement.

In January 2013, Mexico became the second economy to join the APEC Cross-border Privacy Enforcement Arrangement. The Arrangement operates under the Federal Act on Protection of Personal Data, the regulations thereto and the new parameters for self-regulation in the area of personal data published in the Official Gazette of 29 May 2014.

d) Industrial and intellectual property

In the area of intellectual property rights, Mexico has included in the Federal Copyright Act protection for computer programs, as well as the right to exclusive use of news headlines on the Internet. The Federal Criminal Code defines a number of offences related to unauthorized reproduction and large-scale marketing of works protected by copyright without the permission of the holder of the copyright.

In addition, Mexico has signed the following instruments:

- Beijing Treaty on Audiovisual Performances (2012)
- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Brussels Convention relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite

- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

In regard to domain names, NIC Mexico has adopted the arbitration process envisaged in the ICANN Uniform Domain-Name Dispute-Resolution Policy as part of its own dispute-resolution policy, and it recognizes the WIPO Arbitration and Mediation Centre as a provider of arbitration services.

f) Cybercrime and information security

The Federal Criminal Code defines offences related to the interception of communications, gaining illicit access to computer systems and causing harm to IT systems. The Credit Institutions Act defines a number of offences involving fraud employing electronic means.

The Federal Telecommunications and Broadcasting Act expands the powers of law enforcement and security authorities by establishing certain obligations for providers of telecommunications services, whether they be concessionaires, licensees or providers of applications and content services, to enable authorities to gain access in real time to information regarding communications, users and devices in connection with criminal investigations.

So far, no legal regime has been developed to determine the liability of Internet service providers. This discourages the development of technological platforms and networks for accessing the Internet.

It is hoped that with the entry into force of the National Code of Criminal Procedure,[27] an efficient national cooperation system can be put underway that will unify the different local systems. At the federal level, the Code will enter into force on 18 June 2016. No time frame has yet been set for the process at the state level, but it is hoped that the Code will eliminate the existing procedural contradictions between the federal and the 32 state systems.

Mexico is a member of the Conference of Ministers of Justice of the Ibero-American Countries and has signed the Ibero-American Cooperation Agreement on Research, Underwriting and Obtaining Evidence on Cybercrime, as well as the recommendation of the Conference of Ministers of Justice of Ibero-American Countries on the definition and punishment of cybercrime. It has been invited by the Council of Europe to accede to the Convention on Cybercrime, but has not yet done so.

[27] See: http://www.dof.gob.mx/nota_detalle.php?codigo=5334903&fecha=05/03/2014

g) Pending legislation and challenges

The Congress of the Union is currently considering a number of proposed amendments to the Federal Criminal Code and the National Code of Criminal Procedure, with a view to adopting the substantive and procedural measures envisaged in the Council of Europe's Convention on Cybercrime and harmonizing the relevant federal and state legislations. The Congress is also discussing a general bill on protection of personal data, bearing in mind the amendment to article 6 of the Constitution, of 7 February 2014.

The main challenges facing Mexico have to do with the deployment of connectivity infrastructure and the creation of capacities to improve understanding and use of the legal aspects of ICTs to promote e-commerce.

NICARAGUA

The National Human Development Plan 2012-2016 is aimed, among other things, at strengthening e-commerce, while the Ministry of Development, Industry and Trade promotes the use of electronic signatures through its Programme on Strengthening Security and Confidence in the Use of e-Commerce in Nicaragua. Among the main laws for enabling e-commerce are the Electronic Signatures Act (Act No. 729), of 30 August 2010, and the regulations thereto, which were adopted by Executive Decree No. 57-2011, of 8 November 2011.

a) Electronic transactions/electronic signatures

The Electronic Signatures Act incorporates the provisions of the UNCITRAL Model Law on Electronic Signatures and recognizes the efficacy and legal validity of electronic signatures and digital certificates, as well as intelligible software, independently of related hardware, attributable to individuals or legal entities in the public or private sector, and regulates certification services providers. The Act makes a distinction between electronic signatures and certified electronic signatures, which have different legal effects, and recognizes the functional equivalency of printed documents with respect to documents contained in data messages, and of handwritten signatures with respect to certified electronic signatures backed by a certificate issued by an accredited service provider.

It also empowers authorities in the different branches of government to carry out administrative formalities through electronic means and to use electronic files and digital signatures in their actions, either among themselves or with private parties.

The Regulations to the Digital Signatures Act, Decree No. 57-2011, of 8 November 2011, authorize the

Directorate-General for Technology of the Ministry of Finance and Public Credit to act as the lead agency for the electronic signature accreditation process, and outline the powers of the Certification Authority and the obligations and duties of certification service providers.

In the financial field, the General Act on Banks, Financial Institutions, Non-Banking Institutions and Financial Groups, of 30 November 2005, authorizes banks to use computer and microfilm systems in providing their services. Documents reproduced by these systems have full probative value, provided the mechanisms used for reproduction meet the requirements of the Office of the Superintendent of Banks and that the documents are duly signed by an authorized official.

Special mention should be made of Decision No. CD-SIBOIF-725-1-ABR26-2012, of 26 April 2012, governing electronic transactions carried out by financial institutions, which was issued by the Office of the Superintendent of Banks and Other Financial Institutions.

In regard to online government transactions, Act No. 691, on Simplification of Formalities and Services in Public Administration, of 3 August 2009, lays down the bases and principles for simplifying and rationalizing formalities and services in order to ensure that public institutions follow standards of economy, transparency, celerity, efficacy and helpfulness so as to achieve prompt and effective solutions to problems posed by users. The Act promotes implementation of the Single Window for Formalities and Services, as well as the use of electronic means to expedite procedures.

The Public Sector Administrative Procurement Act (Act No. 737), of 8 and 9 November 2010, governs the substantive and procedural aspects of preparing, awarding, executing and terminating procurement contracts by public agencies. The Act also applies to public enterprises and financial entities when their purchases are related to administrative activities. It authorizes the Directorate-General for State Procurement, as the oversight agency for the public sector procurement system, to monitor the actions of contracting entities. Negligent or corrupt behaviour on the part of public officials must be reported to the Office of the Comptroller General of the Republic. The Directorate-General is empowered to sanction providers/contractors who violate the Act, the General Regulations to the Act or other administrative rules relating to procurement. The Act promotes development of micro-small- and medium-sized enterprises and encourages their participation in contracting processes.

The General Regulations to the Public Sector Administrative Procurement Act (Act No. 737), of 15 and 16 December 2010, expand the powers of the Directorate-General for State Procurement as the oversight agency for the public sector procurement system, authorizing it to set guidelines and establish mechanisms and procedures for the use of electronic or manual formats for recording information on contractors. It also establishes the online providers registry, to be operated by the Directorate-General for State Procurement, for registering all individuals or legal entities, national and foreign, that are not prohibited from entering into contracts with the State. The procedures and forms to be used for including or deleting entries, the areas that need to make purchases and the officials concerned are all listed on the website (www.nicaraguacompra.gob.ni).

In regard to customs, Nicaragua has adopted the Unified Central American Customs Code and its Regulations and the CAFTA-DR Agreement.

b) Consumer protection

The Consumer Protection Act (Act No. 842), of 11 July 2013, provides for the fundamental rights of consumers envisaged in United Nations General Assembly resolution 39/248, on guidelines for consumer protection, including the right to information and the right to safe products. It also provides for the right of consumers to opt out of sales made remotely, the right to privacy and the right to real and effective protection in electronic transactions. Abusive clauses in financial services contracts include those which exonerate financial institutions from liability for viruses, fraudulent programs or unauthorized or illicit exposure of their services by electronic means.

The Act also covers procurement of products and financial services by electronic means and attributes to them the same probative value and legal effect as contracts concluded in person. It recognizes electronic transactions and outlines the information that must be provided to consumers prior to the conclusion of an online transaction, including information on physical domicile, electronic address and other means for submitting complaints and clarification, as well as information on goods and services, avoiding deceptive commercial practices that could encourage fraud or create confusion. It requires providers to use reliable technology and technical devices to ensure the security and confidentiality of the information transmitted

and provided by consumers in online transactions and to inform them about such measures.

As regards online purchases of goods and services within the national territory, suppliers are required to provide electronic invoices and to keep a record of electronic payments, as well as to send the consumer the sales contract with full information on terms and conditions, costs and guarantees.

c) Protection of personal data

The Political Constitution of the Republic of Nicaragua, of 19 November 1986, enshrines the right of all persons to their and their family's private life, the inviolability of their residence, correspondence and communications of all types, as well as access to knowledge of all information regarding them is contained in government records, and the reasons and purpose for the possession of such information.

The Public Information Access Act (Act No. 621), of 22 June 2007, incorporates the right of habeas data to protect private personal data appearing in public or private files, records, databases and other technical media, the disclosure of which is an invasion of personal/family privacy if the information disclosed consists of sensitive personal data or information regarding private or family life and affairs, when such information is in the possession of the relevant governmental entities. Habeas data guarantees that anyone may have access to information concerning him or her that is held by a government entity, as well as the right to know why and for what purpose the entity possesses the information.

The Personal Data Protection Act (Act No. 787), of 29 March 2012, follows the Directives for Harmonization of Data Protection in the Ibero-American Community issued by the Ibero-American Data Protection Network. The Act protects personal data, whether automated or not, of all individuals or legal entities, and the handling of such information in public or private files, in order to guarantee the right to privacy of individuals and the right to make their own decisions regarding the use of their information. The Directorate for the Protection of Personal Data in the Ministry of Finance and Public Credit is responsible for enforcing the Act, which classifies all personal data as simple personal data, electronic personal data, sensitive personal data, health-related personal data and commercial personal data. It also establishes the requirement to register files containing personal data with the Directorate for the Protection of Personal Data and prohibits transfer of personal data to countries or international agencies that do not provide suitable levels of security and protection.

Public or private individuals and entities that use, store or transfer private information of their clients or users are required to (i) ensure that the information is used in a manner that is appropriate, proportional and necessary in respect of the scope and the purposes for which it is collected; (ii) obtain the consent of the data subject to provide the data; (iii) use the data for the purposes for which they were obtained; and (iv) take technical and organizational measures to guarantee the security and confidentiality of personal data.

Violations of the Act are punished with administrative and criminal sanctions. The Act grants the data subject the right to request from the Directorate for the Protection of Personal Data information concerning the existence of files on him or her in personal data files, the purpose for which the data are held and the identity of the parties responsible. It also allows him or her to request that the personal data be corrected, modified, deleted, supplemented, included, updated or cancelled. The Act classifies violations as minor or serious and establishes administrative sanctions, independently of any civil or criminal liability that might also apply.

The regulations to the Personal Data Protection Act (Act No. 787) were adopted by Decree No. 36-2012, of 17 October 2012. The decree describes in detail a number of aspects of the Act, including rights of access, correction, cancellation and objection, as well as security measures and procedures relating to inspections and punishment.

d) Industrial and intellectual property

With regard to intellectual property rights, the Constitution of Nicaragua guarantees free and unrestricted artistic and cultural creation. It also stipulates that cultural workers are free to choose their forms and modes of expression and that the it is the State's duty to facilitate the means necessary for creating and disseminating their works and protecting their copyright.

The Copyright and Related Rights Act (Act No. 312), of 6 July 1999, most recently amended on 16 March 2006, protects computer programs on the same terms as literary works. Such protection is extended to include technical documentation and user manuals. The Act also protects databases; reproduction for personal use excludes reproduction of all or major portions of numerical databases. The Act defines as an offence the act of circumventing technological measures in order to permit unauthorized access to a

work or to an interpretation or performance of a protected phonogram or other protected object.

With regard to industrial property, article 6 of the Act on Patents for Inventions, Utility Models and Industrial Designs (Act No. 354), of 22 and 25 September 2000, stipulates that mathematical methods or computer programs considered in isolation are not patentable inventions. The Trademarks and Other Distinguishing Signs Act (Act No. 380), of 16 April 2001, establishes the requirements for the protection of trademarks, domain names, business names, denominations of origin and other distinguishing signs.

In the area of international intellectual property rights, Nicaragua has ratified the following instruments:

- WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances (2012)
- Protocol to the Central American Agreement for the Protection of Industrial Property
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (Geneva Convention)
- International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention)
- Brussels Convention relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

e) Domain names

With regard to domain names and the matters covered by the Trademarks and Other Distinguishing Signs Act (Act No. 380), NIC NI (http://nic.ni) is the entity responsible for administering the country's top-level domain name .ni. As the country's registering authority, NIC NI has adopted the ICANN Uniform Domain-Name Dispute-Resolution Policy, which conforms to international best practices. It recognizes the dispute-resolution services provided through the WIPO Arbitration and Mediation Centre.

The Trademarks and Other Distinguishing Signs Act (Act No. 380) recognizes as a trademark the use of the distinguishing sign as a domain name, e-mail address, or name or designation in electronic and other similar media used for electronic communications or e-commerce.

f) Cybercrime and information security

The Criminal Code (Act No. 641), of 13 November 2007, provides penalties for illegally opening, intercepting or in any other way learning the content of a letter, sealed bid or telegraphic, telematic, electronic or other message not addressed to the person carrying out such an act. It also punishes anyone who without authorization promotes, facilitates, authorizes, finances, creates or markets a database or computer record containing information that can harm individuals or legal entities.

The Criminal Code also punishes the unauthorized use of computerized records of another or unauthorized entry by any means in another's database or electronic files. It establishes sanctions for any person who without authorization makes use, by any informational means, of information, data, written or electronic documents, computer registries or other media or objects that contain a business secret.

g) Pending legislation and challenges

Among other challenges, Nicaragua needs to address the issue of cybersecurity and establish a national computer security incident response team, along with legislation to further the process. The main legislative measures being reviewed by the National Assembly include the preliminary bill on e-government and the preliminary proposal for a special law on protection against cybercrime.

PANAMA

The most important legislation for the development of e-commerce in Panama is Act No. 51, of 22 July 2008, which defines and regulates electronic documents and electronic signatures and allows the provision of technological storage services for documents, as well as electronic signature certification services. This Act also includes provisions for the development of e-commerce, as follows.

a) Electronic transactions/electronic signatures

The purpose of Act No. 51 is to establish a regulatory framework for the creation, use and storage of electronic documents and electronic signatures, as well as for registration and oversight of providers of technological storage services for documents and

providers of electronic signature certification services in Panama.

The Act incorporates several elements of the UNCITRAL model laws on electronic commerce and on electronic signatures, as well as elements of the European directives on e-commerce, electronic signature and remotely handled direct marketing. The Act establishes regulations on a variety of aspects of electronic transactions between private parties and with public agencies.

Act No. 51 establishes a regulatory framework for certain commercial internet transactions, primarily governing what information is provided prior and subsequent to making electronic contracts and setting forth conditions for the validity and legal force of such contracts. It outlines the obligations and responsibilities of entities providing commercial services via the Internet, including those acting as intermediaries for the transmission of content, storage and temporary copies, along with the limitations on liability; the electronic exchange of commercial information and documentation, including offers, promotions and competitions, and the sanctions applying to providers of commercial services via electronic media.

Act No. 51 recognizes the functional equivalence of signed printed documents and electronic documents with advanced electronic signature backed by a digital certificate issued by a certification service that has been duly accredited before the Public Registry. It also recognizes foreign digital certificates issued by competent authorities of other countries, provided they comply with the standards required by the Public Registry.

It also recognizes that electronic documents are admissible as evidence and have the same probative weight as paper documents. The trustworthiness of the manner in which an electronic document has been generated, filed or communicated is to be taken into account in assessing its probative value, as is the reliability of the way in which the integrity of the information has been safeguarded.

Act No. 51 was amended by Act No. 82, of 9 November 2012, which transfers competence in regard to electronic signatures from the Directorate-General for e-Commerce of the Ministry of Commerce and Industry to the National Directorate for Electronic Signatures of the Public Registry of Panama. The amendment added a chapter II, on rules for electronic communication, which provides further support for the formation of contracts through electronic means, and incorporates several measures from the United Nations Convention on the Use of Electronic Communications in International Contracts, which Panama has signed and which is in the process of being ratified by the National Assembly.

In the area of finance, Decision No. 6 of 2011 of the Office of the Superintendent of Banks lays down guidelines on electronic banking and related risk management, requiring banking institutions in Panama to modernize the electronic systems used to provide their services.

In the context of government, Act No. 51 authorizes the State to use technological document storage internally and in its relations with private parties. Act No. 83, of 9 November 2012, sets rules for the use of electronic media in the government formalities previously authorized by Executive Decree No. 928, of 21 September 2010, known as “Paperless Panama”.

Executive Decree No. 847, of 20 October 2014, established the Electronic Registry System based on the electronic folio technique, incorporating the use of electronic signature that is recognized for all operations and registry procedures in the Public Registry, in order to strengthen security attributes, i.e., authenticity, integrity and non-repudiation of documents for registry operations.

In the area of customs, Decree Law No. 1, of 13 February 2008, created the National Customs Authority and laid down a number of provisions allowing for the use of electronic media for customs procedures.

With regard to taxation, Act No. 51 of 2008 establishes the legal validity of electronic invoices and recognizes the validity for tax purposes of commercial transactions carried out by electronic means. The Tax Code and Decision No. 201-2969, of 15 August 2007, of the Directorate-General of Internal Revenue of the Ministry of Economy and Finance authorize the submission of sworn statements by electronic media.

b) Consumer protection

The Constitution mandates that everyone has the right to obtain goods and services of quality and to have accurate, clear and sufficient information on the characteristics and content of goods and services acquired, as well as freedom of choice and equitable treatment consistent with human dignity.

Act No. 51 includes a number of consumer protection measures covering e-commerce transactions, with stipulations regarding the responsibilities of commercial service providers using the Internet, including providers of intermediation services. The Act includes measures to limit unsolicited commercial

communications, including those sent via the Internet. It also authorizes the use of seals of trust to promote use of the Internet as a secure medium for offering and obtaining commercial goods and services.

c) Protection of personal data

The Constitution of 1972, as amended on 15 November 2004, guarantees the inviolability of private communications, which may not be intercepted or recorded except under judicial order. Failure to respect this prohibition renders the results of such interception or recording inadmissible as evidence, without prejudice to any criminal liability that may be incurred by said interception or recording. It also gives all persons the right to access personal information on themselves contained in public and private databases and to request the correction and protection, as well as the removal, of such information. Such information may only be collected for specific purposes, with the consent of the data subject or by authorization of a government agency pursuant to the law.

The Constitution also gives all persons the right to file habeas data actions to guarantee their right to access personal information regarding them in government databases, or in private databases when such databases or records belong to firms that provide services to the public or are information providers. Habeas data action can be used to confidentially request correction, updating, rectification, removal or preservation of personal information or data.

Act No. 51 establishes a special regime to guarantee the inviolability of the information deposited in databases as backup for offshore operations of private or public enterprises, including state and international organizations. Act No. 24 of 2002, of 22 May 2002, as amended and added to by Act No. 14 of 2006, of 18 May 2006, contains several measures relating to the management of information concerning consumers' credit history.

d) Industrial and intellectual property

Following ratification of the United States-Panama Trade Promotion Agreement, Act No. 35, of 10 May 1996, was amended by Act No. 61, of 5 October 2012, to allow for the use of electronic media in submitting applications for trademarks, patents and industrial models to the Directorate-General of the Industrial Property Registry.

Panama has signed the following treaties:

- international treaties administered by WIPO, including the Patent Cooperation Treaty and the Trademark Law Treaty
- WIPO Copyright Treaty and the Performances and Phonograms Treaty
- It has ratified the following instruments:
- Protocol to the Central American Agreement for the Protection of Industrial Property
- Dominican Republic-Central America-United States Free Trade Agreement (CAFTA-DR)
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by WTO

In the area of copyright and related rights, Act No. 64, of 10 October 2012, was passed to abrogate Act No. 15, of 8 August 1994, in order to bring it in line with the digital environment of the information society. The scope of the Act was expanded to include protection for software and databases and to elaborate on concepts such as information on management of rights and effective technology for protecting one's own online identity. With regard to the related rights of artists, performers and broadcasting organizations, it defines the concepts of phonogram and videogram and recognizes the right of publication via any medium. Regulations to the Act are being developed.

e) Domain names

In regard to domain names, NIC-Panama (http://nic.pa), which is housed at the Technological University of Panama, is the entity responsible for administering the country's top-level domain name, .pa. As the Internet registry authority, NIC-Panama has adopted the ICANN Uniform Domain-Name Dispute-Resolution Policy, which conforms to international best practices, and it recognizes the dispute-resolution services provided through the WIPO Arbitration and Mediation Centre.

f) Cybercrime and information security

Act No. 51 defines as an offence the alteration or adulteration of technologically stored documents, as well as the improper disclosure of the technological information stored. The Criminal Code (Act No. 14) defines a number of offences involving illicit access to computer systems, as well as the interception of electronic communications, with harsher penalties in cases involving data contained in databases or computer systems of (i) government offices, (ii) public, private or mixed institutions that provide a public service, and (iii) banks, insurance companies or other financial or securities institutions. It also sanctions illicit disclosure of industrial secrets and unauthorized reproduction of works that are protected by copyright and related rights.

Under Act No. 79, of 22 October 2013, Panama ratified the Council of Europe's Convention on Cybercrime. Panama is a member of the Conference of Ministers of Justice of Ibero-American Countries.

In regard to security of information, the National Authority for Government Innovation administers the National Computer Security Incident Response Centre of Panama, which was created by Executive Decree No. 709 (2011). This Centre coordinates all activities aimed at preventing and responding to cyberattacks against government IT systems and critical infrastructure.

g) Pending legislation and challenges

The National Assembly is discussing a bill on cybercrime (Act No. 105), of 16 October 2014, in fulfilment of the country's obligations under the Council of Europe's Convention on Cybercrime.

The Directorate-General for e-Commerce of the Ministry of Commerce and Industry is preparing a new executive decree to draw up regulations to Act No. 51 of 2008, as amended by Act No. 82 of 2012, as well as regulations on technological storage of documents and e-commerce. Work is also under way on new executive decrees to regulate the new legislation on industrial property and copyright and related rights.

The National Authority for Government Innovation is holding public consultations on preparation of a comprehensive law on protection of personal data.

One of the main challenges faced by Panama is the need to close the digital gap; this will entail promoting strategies for facilitating access of micro- and small businesses to e-commerce and implementing self-regulation schemes such as seals of trust. It also needs to train judges, prosecutors, attorneys and merchants, in both small and large businesses, to promote the use of the Internet in a safe environment and encourage e-commerce.

PARAGUAY

The ICT Master Plan was adopted pursuant to Decree No. 7706, of 15 November 2011, issued by the Office of the President of the Republic of Paraguay. One of the measures proposed in the Master Plan for closing the digital gap is a strategy for promoting e-commerce among different actors in the economy. Bearing in mind the Master Plan, the National Congress adopted the e-Commerce Act (Act No. 4868/13), of 1 March 2013, which is the main legislation on the subject, along with the Act on the Legal Validity of Electronic Signatures, Digital Signatures, Data Messages and Electronic Files (Act No. 4017/10), of 24 December 2010, which was amended by Act No. 4610, of 9 May 2012. These laws include several measures from the UNCITRAL model laws on electronic commerce and electronic signatures.

a) Electronic transactions/electronic signatures

The e-Commerce Act (Act No. 4868/13) governs commerce and contracts carried out through electronic or technologically equivalent media between online suppliers of goods and services (businesses established both within and outside of Paraguay), intermediaries involved in transmitting content through telecommunications networks, electronic commercial communications and consumers or users. The Act provides for providers of intermediation services, data storage, links and temporary copies to be exempt from liability. It establishes information requirements that must be met by websites and recognizes the legal validity of contracts concluded by electronic means and of electronic invoices. It also lays down a list of violations and sanctions.

The regulations to the e-Commerce Act (Act No. 4868), of 26 February 2013, were issued by the President of Paraguay by means of Decree No. 1165, of 27 January 2014. The regulations empower the Ministry of Industry and Commerce to serve as the implementation authority, acting through the Directorate-General for Digital Signatures and e-Commerce, to interpret and enforce the Act in areas pertaining to (i) remote online contracting with suppliers of goods and services, (ii) organizing and managing auctions by electronic means or in virtual markets and shopping centres; (iii) managing online purchases by groups of people; (iv) distributing content over the network, in response to an individual request resulting in economic activity for the provider; (v) sending commercial communications; (vi) intermediation services (access, data transmission, storage, temporary copies, searches); and (vii) supplying information by telematic means.

Act No. 4017/10 is especially important because it recognizes the legal validity of electronic signatures, digital signatures, data messages and electronic files, and regulates their use. It also regulates certification companies and authorizes their operations and the provision of certification services. It makes a distinction between electronic signatures and digital signatures, conferring on them different legal effects, and recognizes the functional equivalence of printed documents with respect to documents contained in data messages, as well as between handwritten signatures and digital signatures, provided the latter have

been certified by a provider of services that is licensed by the Ministry of Industry and Commerce. It also empowers the Government to carry out administrative procedures through electronic means and to use electronic files and digital signatures in its actions.

The regulations to the Act were issued by Executive Decree No. 7369/2011. The scope of the Act was extended by Act No. 4610/12, of 9 May 2012, which partially amends it in regard to the scope of application of electronic files, and by the designation of the Ministry of Industry and Commerce as the implementation authority.

In the administrative sphere, the Public Procurement Act (Act No. 2051/03, of 12 December 2002, as amended by Act No. 3439/07, of 31 December 2007, established the Public Sector Procurement System to regulate planning, programming, budgeting, contracting, execution, spending and monitoring of contracting and subcontracting for all types of goods, contracting of services in general, consultant services and public works and related services, in addition to regulating the certification of electronic means of identification for public sector contracting.

As regards the use of electronic means in government administration, the Administrative Reorganization and Tax Reform Act (Act No. 2421/04), of 25 June 2005, requires the Office of the Deputy Secretary of Taxation to maintain and regularly update a web page to inform taxpayers about its services and about their tax obligations. The Tax Administration currently allows taxpayers to submit sworn statements online or to print the form for the Single Registry of Taxpayers. The Customs Code (Act No. 2422/04), of 30 June 2004, incorporates the use of computer systems, information technologies and automation in customs transactions, in order to simplify procedures. It also allows the handwritten signatures required by the National Customs Service to be replaced by proper passwords or sign-ons, or by electronic signatures, as a means of substantiating administrative procedures carried out digitally. The Customs Code recognizes passwords and electronic signatures as being equivalent to handwritten signatures for all legal purposes and regulates the use of electronic files.

The Republic of Paraguay has signed, but not yet ratified, the United Nations Convention on the Use of Electronic Communications in International Contracts (2005). Paraguay has signed MERCOSUR resolution 34/06, adopting the Guidelines for Agreements on Mutual Recognition of Advanced Electronic Signatures; this resolution does not need to be incorporated into the legislation of States parties in order to be applicable to the relevant aspects of the organization or operation of MERCOSUR. Paraguay has also signed MERCOSUR resolution 37/06, recognizing the legal validity of electronic documents, electronic signatures and advanced electronic signatures; however, this resolution has not been incorporated into the country's substantive law.

b) Consumer protection

In the area of consumer protection, the Consumer and User Protection Act (Act No. 1334/98), of 30 October 1998, establishes rules to protect consumers' dignity, health, safety and economic interests. The rights defined in this law are not subject to waiver, transaction or conventional limitation by consumers and override any legal provision, usage, custom, practice or stipulation to the contrary. The Act governs all transactions between providers and consumers for the distribution, sale, purchase or other form of commercial transaction involving goods and services. In the telecommunications realm, Act 2340/03 expands the scope of Act 1334/98, adding a special chapter on telecommunications services, the principal elements of which include the obligation to provide information that permits consumers to identify providers and the obligation to furnish transparent billing information.

The eCommerce Act (Act No. 4868/13), of 26 February 2013, also establishes the following rights for consumers: (i) to object to the use of their data for promotional purposes; (ii) to opt out of commercial transactions within five days after receiving the product or service, simply by electronic notification of their decision; (iii) to obtain complete and truthful information on products and services; (iv) to receive the product or service purchased within the time, of the quality and in the quantity agreed upon; and (v) to receive reimbursement when merchandise is returned. The regulations to the e-Commerce Act require online providers of goods and services to provide consumers or users, in a transparent, clear and simple manner, information about the security of the means of payment used and the technology used to protect transmissions, processing or storage of their financial data.

Of note at the international level is the Santa María Protocol, ratified by Paraguay via Act No. 1081, of July 1997, which recognizes the jurisdiction of the courts of the State in which a consumer is domiciled. Also worth mentioning are MERCOSUR resolution 21/04, on consumers' right to information in commercial transactions made via the Internet, and MERCOSUR resolution 45/06, on consumer protection and

misleading advertising. Paraguay has signed both resolutions, but has not yet incorporated them into its domestic substantive law.

c) Protection of personal data

The Paraguayan Constitution recognizes privacy and protection of personal data as fundamental rights, in accordance with the San José Pact, which guarantees the right to personal and family confidentiality, respect for individual privacy and dignity, and to a person's private image. The Constitution also recognizes habeas data as a fundamental right entitling all persons to have access to any information and data on themselves or their assets contained in government records or in private records of a public nature and establishing the right to be apprised of the use and purpose of such information.

Habeas data gives the data subject the right to request updating, correction or removal of erroneous data or of data that illegitimately jeopardize his or her rights. In addition, Act No. 1682/2001, regulating information of a private nature, which was adopted on 28 December 2000 and amended by Act No. 1969/02, of 6 September 2002, lays down rules on the storage, collection, processing and publication of data of a private nature. The Act is general in scope and not limited to electronic databases. It authorizes the publication and dissemination of data consisting of a person's first and last names, identity document, domicile, age, date and place of birth, marital status, occupation or profession, place of work and work telephone number, which are considered to be public personal data.

Act No. 4868/13 stipulates that providers may not jeopardize the protection of personal data and the right to personal and family privacy of the parties or of third parties who are involved. It also requires that when providers of goods and services use data storage and recovery devices on terminals, they must inform consumers or users fully and clearly about the use and purpose of such devices and offer them the option of refusing the use of their data; this option is to be made available free of charge, using a simple procedure.

The Act stipulates that providers who offer goods and services online must inform consumers or users of the purpose and treatment of their personal data, in accordance with the relevant legislation that is in force at the time. They must also provide this information to the recipients of the data supplied and to those responsible for keeping or storing the information provided. Providers of goods and services must use secure systems to prevent loss, alteration and access by unauthorized third parties to the data supplied by consumers or users, and they must obtain the express consent of consumers to process their personal data.

d) Industrial and intellectual property

In the area of intellectual property rights, the Paraguayan Constitution guarantees authors, inventors, producers and merchants exclusive ownership of their works and inventions under the law. some of the main laws on the matter are the Copyright and Related Rights Act (Act No. 1328/98), of 27 August 1998; the Trademarks Act (Act No. 1294/98), of 24 June 1998; the Patent Act (Act No. 1630/00), of 29 November 2000, as amended by Act No. 2047/02, of 19 December 2002; Act No. 2593/05, of 17 June 2005; the Industrial Designs and Models Act (Act No. 868/81), of 2 November 1981; Act No. 1582/00, approving the WIPO Copyright Treaty, adopted on 6 October 2000, and Act No. 1583, approving the WIPO Performances and Phonograms Treaty, adopted on 6 October 2000. Paraguay has also ratified the Paris Convention and the Berne Convention.

e) Domain names

As regards domain names, NIC-PY is the entity responsible for administering domain names; it is operated by the Catholic University's Digital Electronics Laboratory and the National Computer Centre at the National University of Asunción. There is no legislation on the legal nature of domain names, which are subject to the administrative regulations of NIC-PY. NIC-PY serves as coordinator of the domain names system but has no jurisdictional authority and does not act as a mediator or arbitrator or intervene in disputes over domain names. Disputes that are settled out of court are subject to the Arbitration and Mediation Act (Act No. 1878/02).

f) Cybercrime and information security

Act No. 4439 of 3 October 2011, which amends and expands several articles of the Criminal Code (Act No. 1160/97), added the following cybercrimes: (i) child pornography; (ii) improper access to data; (iii) interception of data; (iv) preparation for improper access to and interception of data; (v) improper access to IT systems; (vi) sabotage of IT systems; (vii) misappropriation of funds via IT systems; and (viii) forgery of debit or credit cards and other electronic means of payment.

In 2012, the CERT-PY computer emergency responses team was set up within the National Secretariat for Information and Communication Technology to facilitate and coordinate protection of ICT systems that support the national and government infrastructure and to

guarantee effective and timely responses to computer security incidents.

g) Pending legislation and challenges

Paraguay faces the challenge of catching up to other countries in the region. To address the digital gap, it needs to improve access to the Internet so as to ensure that it will be more inclusive and development-oriented. The criminal procedural legislation needs to be brought up to date in order to strengthen the State's capacities to combat cybercrime. The legal framework for data protection also needs to be updated in order to comply with the commitments undertaken by Paraguay in the Ibero-American Data Protection Network.

PERU

The Development Plan for the Information Society in Peru – Digital Agenda 2.0, issued by Supreme Decree No. 066-2011-PCM, of July 2001, includes a strategy for the development of e-commerce under objective 5, i.e., "to increase productivity and competitiveness through innovation in the production of goods and services, by developing and applying ICTs." In addition, the National e-Government Policy 2013-2017, adopted through Supreme Decree No. 081-2013; the Act on Promotion of Broadband and Construction of the National Fibre Optic Backbone (Act No. 29904), of 20 July 2012, and the regulations thereto, of 4 November 2013, as well as Legislative Decree No. 604, adopting the Act on Organization and Duties of the National Institute of Statistics and Informatics, of 30 April 1990, are all measures designed to strengthen the environment for making e-commerce viable.

Some of the main laws governing e-commerce are Act No. 27291, of 24 June 2000, amending the Civil Code; the Digital Signatures and Certificates Act (Act No. 27269), of 26 May 2000, as amended by Act No. 27310, and the regulations to the Digital Signatures and Certificates Act, contained in Supreme Decree No. 052-2008/PCM, of 18 July 2008.

The Office of the President of the Council of Ministers, working through the National Office for e-Government and Informatics encourages public agencies to use ICTs in providing their services and to hold seminars on the subject of e-government and the information society. The idea is to train public officials in areas such as the legal framework for e-government, open government, ICT statistics in the State, the information society and inclusion, and digital citizenship for modernization of the State and improvement of public management.

a) Electronic transactions/electronic signatures

Act No. 27291, amending the Civil Code, provides that when the law requires a particular procedure or signature to establish a party's will, the requirement may be satisfied via electronic, optical or any similar means, and that for the purpose of contracts executed remotely, offers, withdrawals, acceptances and all other contractual statements are considered to have been communicated when they arrive at the addressee's address. If they are transmitted by electronic, optical or other similar means, they are presumed to have been received upon receipt of a confirmation of delivery.

The Digital Signatures and Certificates Act (Act No. 27269) of 2000, article 11 of which was amended by Act No. 27310, establishes general guidelines regarding digital signatures and digital certificates, as well as establishing the authority of the relevant government entities and the types of action to be taken by certification, registration and verification entities. Under this legislation, digital signatures have the same force and legal validity as handwritten signatures or similar expressions of a party's will. It also recognizes certificates of digital signature issued by foreign entities, provided such certificates are recognized by the competent administrative authority.

The regulations to the Digital Signatures and Certificates Act (Supreme Decree No. 052-2008/PCM), issued by the Office of the President of the Council of Ministers, reflects some of the provisions of the UNCITRAL Model Law on Electronic Signatures. The Act was designed to regulate the use of electronic signatures and the regime governing the Official Electronic Signature Infrastructure in both the public and private sectors. The regulations designate the National Institute for the Protection of Competition and Intellectual Property Rights as the lead administrative agency, and assign to the National Registry of Identification and Civil Status the roles of National Certification Entity for the Peruvian State, Certification Entity for the Peruvian State and Registry or Verification Entity for the Peruvian State.

The regulations give digital signatures generated within the Official Electronic Signature Infrastructure the same validity and legal force as handwritten signatures. They also make digitally signed electronic documents in that framework admissible as evidence in judicial or administrative proceedings. The Official Electronic Signature Infrastructure is a reliable accredited system regulated and supervised by the relevant administrative entity and has the necessary legal and

technical tools for generating digital signatures and providing various levels of security to ensure the integrity of electronic documents and the identity of their authors.

Supreme Decree No. 070-2011-PCM, of 27 July 2011, amending the regulations to the Digital Signatures and Certificates Act (Act No. 27269) and laying down rules for registry procedures carried out under Legislative Decree No. 681 and supplemental provisions, modifies the requirements relating to the content and duration of digital certificates for individuals and legal entities and recognizes the authority of the National Institute for the Protection of Competition and Intellectual Property Rights to act as competent administrative authority for the Official Electronic Signature Infrastructure.

Supreme Decree No. 105-2012-PCM, of 21 October 2012, establishes provisions for facilitating implementation of digital signatures and amends Supreme Decree No. 052-2008-PCM, on regulations to the Digital Signatures and Certificates Act. The 2012 decree allows for individuals and legal entities to use a digital certificate issued by providers holding a Web Trust international certification until such time as they obtain the digital certificate from the National Institute for the Protection of Competition and Intellectual Property Rights.

The National Supervisory Commission for Companies and Securities issued its Decision No. 008-2003, of 7 February 2003, approving the regulations to the Peruvian Securities Market Network, governing the transmission and exchange of documents and information through the Peruvian Securities Market Network using public key infrastructure technology. Individuals and legal entities that are subject to the Commission's supervision and control must use this network for providing any information and documentation required of them.

In the area of online government transactions, regulations provided by the General Administrative Procedures Act (Act No. 27444), of 10 April 2001, include notification by electronic and other means that establish reliable confirmation of receipt and identification of the receiving party, provided that the user has expressly requested return receipt. It also authorizes the use of electronic means for communications within government.

Under this Act, users may request that information or documentation pertaining to administrative processes be sent to them by remote means.

At present, the State Electronic Contracting System (www.seace.gob.pe) allows for the exchange and dissemination of information on government procurement and contracting, as well as for electronic transactions.

Under the regulations to the Digital Signatures and Certificates Act, the National Office for e-Government and Informatics has the authority to supervise government agencies' plans for the implementation of administrative procedures and formalities by secure electronic means.

In regard to taxes, the Tax Code (Supreme Decree No. 135-99 of 19 August 1999), as amended by Legislative Decree No. 953, of 5 February 2004, provides for the Tax Administration to authorize the submission of tax returns through magnetic media, fax, electronic transfer or any medium that meets the conditions established by the Office of the National Superintendent of Customs and Tax Administration. On that basis, the Office of the National Superintendent of Customs and Tax Administration has developed telematic programs for filing tax returns.

The General Customs Act (Decree No. 809, of 19 April 1996), and the regulations thereto, adopted by Supreme Decree No. 011-2005-EF, of 26 January 2005, governs customs activities involving persons, goods and modes of transport crossing borders at customs points, and gives the Customs Service the authority to issue rules and establish procedures for the issuing, transferring, using and monitoring information through documentary, magnetic or electronic means, in order to promote development and facilitate customs activities. The Ministry of Foreign Trade and Tourism is responsible for developing the Single Window for Foreign Trade created by Supreme Decree No. 165-2006-MEF, of 3 November 2006, which was given the rank of law through the first supplemental provision of Legislative Decree No. 1036, of 24 June 2008.

The Single Window for Foreign Trade enables the parties involved in international trade and transport to electronically process the paperwork required by the competent agencies, in accordance with the regulations currently in force, or requested by the parties in connection with the transit, entry to or exit of goods from the national territory, and to implement e-commerce provisions of the free trade agreements with the United States and Canada, as well as the commitments of the APEC Electronic Commerce Steering Group regarding paperless commerce.

b) Consumer protection

The Consumer Protection Code (Act No. 29571, of 1 September 2010) includes a number of provisions

for protecting online consumers. Among other things, it enables consumers to opt out of contracts using the same mechanisms of form, place and means employed to conclude the contract, including electronic media. It also stipulates that providers must show that they have furnished users, in timely fashion, a copy of the contract, including the general terms and conditions, and they must provide information on their identification, domicile, e-mail and other contact information.

The Code also prohibits unsolicited and persistent advertising by e-mail, disregarding a consumer's request that such activities be ceased. It prohibits sending mass e-mails to promote products and services, as well as telemarketing to e-mail addresses that have been included in the registry established by the National Institute for the Protection of Competition and Intellectual Property Rights to keep a record of consumers who do not wish to receive such advertising. It also provides that commercial establishments must keep a Logbook of Complaints in either physical or virtual form.

The regulations to the Logbook of Complaints provided for under the Consumer Protection Code were issued by means of Supreme Decree No. 011-2011-PCM, of 28 February 2011, as amended by Supreme Decree No. 006-2014-PCM, of 23 January 2014. The Code stipulates that all establishments that are open to the public must keep a Logbook of Complaints and that online providers must keep a Virtual Logbook of Complaints and provide consumers with the necessary support to enable them to record their complaints in the Logbook of Complaints.

The Suppression of Unfair Competition Act, adopted by Legislative Decree No. 1044, of 25 June 2008, governs online advertising and empowers the National Institute for the Protection of Competition and Intellectual Property Rights to sanction parties using the Internet or other electronic means to disseminate information detrimental to the competitive process by misleading or confusing consumers.

c) Protection of personal data

The Protection of Personal Data Act (Act No. 29733), of 3 July 2011, is in line with the Directives for Harmonization of Data Protection in the Ibero-American Community issued by the Ibero-American Data Protection Network. The Act protects personal data, whether automated or not, of all individuals or legal entities, and the handling of such information in public or private databanks, in order to guarantee the right to personal privacy. The National Personal Data Protection Authority of the National Directorate of Justice of the Ministry of Justice and Human Rights is responsible for overseeing implementation of the Act. The Act makes a distinction between personal data and sensitive data. It also mandates registration of public or private databanks with the National Registry for Protection of Personal Data and prohibits the transfer of personal data to countries that do not provide suitable levels of security and protection.

Individuals, private entities and public entities that use, store or transfer private information of a data subject are required (i) to ensure that the information is used in a manner that is suitable, proportional and necessary for the scope and purpose for which it is collected; (ii) to obtain the consent of data subject before providing the data; (iii) to use the data for the purposes for which it was obtained; and (iv) to take technical, organizational and legal measures to guarantee the security and confidentiality of personal data.

Violations of the Act are subject to administrative and criminal sanctions. Under the Act, the data subject has the right to be informed; the right of access; the right to have the data updated, included, corrected or deleted; the right to express objection; the right to prevent the data from being supplied; the right to objective treatment and the right to compensation. The Act classifies violations as minor, serious and very serious, and establishes administrative sanctions, independently of any civil or criminal liability that might be in order.

The legal framework for protection of personal data is completed with the Regulations to the Protection of Personal Data Act (Act No. 29733), issued by Supreme Decree No. 003-2013-JUS, of 22 March 2013, and the Directive on Security of Information Administered by Personal Databanks issued by the National Personal Data Protection Authority in October 2013.

d) Industrial and intellectual property

In the area of intellectual property rights, the Copyright Act (Legislative Decree No. 822), of 23 April 1996, incorporates into Peruvian law a number of measures contained in the Berne Convention, the TRIPS Agreement and Decision 351 of the Commission of the Cartagena Agreement, approving the Common Copyright and Related Rights Regime. The Act protects authors of literary and artistic works, as well as their rights holders and those holding copyright-related rights. It also regulates collective bargaining organizations and protects the authors of databases in terms similar to those set forth in the TRIPS Agreement. Legislative Decree No. 1076, amending Legislative Decree No. 822, of 27 June 2008, incorporates the

use of technological measures to protect works and information systems designed to manage rights.

In the international arena, Peru has signed the following instruments:

- WIPO treaties, including the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty
- Beijing Treaty on Audiovisual Performances

In the area of industrial property, the Industrial Property Act (Legislative Decree No. 823), of 23 April 1996, incorporates a number of measures from Decision 344 of the Commission of the Cartagena Agreement, the Common Industrial Property Regime for the Andean Countries, the Paris Convention for the Protection of Industrial Property and the TRIPS Agreement. The Act includes regulations on patents for inventions, certificates of protection, utility models, industrial designs, industrial secrets, trademarks, business names, commercial logos and denominations of origin. Among measures taken to combat piracy, Peru adopted Legislative Decree No. 1092, of 27 June 2008, approving measures to be taken at the border to protect copyright and related rights and trademarks.

e) Domain names

The Peruvian Scientific Network is responsible for administering the Peruvian domain .pe. It has adopted the ICANN Uniform Domain-Name Dispute-Resolution Policies in its own dispute-resolution policy. The WIPO Arbitration and Mediation Centre and the Peruvian Cybertribunal are recognized as dispute-resolution venues.

f) Cybercrime and information security

In the area of criminal law, Act No. 30171, of 10 March 2014, amending the Cybercrime Act (Act No. 30096), added definitions of several criminal offences, including the following: (i) illicit access to IT systems; (ii) attacks against the integrity of IT data; (iii) attacks against the integrity of IT systems; (iv) child pornography via technological media; (v) interception of IT data; (vi) fraud through IT systems; (vii) abuse of IT mechanisms and devices; and (viii) illegal trafficking.

In addition, mechanisms were set up for interagency coordination between the National Police, the Public Prosecution Service and other specialized agencies. Measures were put in place to exempt providers of telecommunications services from criminal liability. Steps were also taken to intervene or record telephone communications or other types of communication and geolocation apps on mobile phones.

To improve information security, PeCERT, the Peruvian computer security incident response team, was set up in 2009. It has played an important role in dealing with computer security incidents.

g) Pending legislation and challenges

Peru needs to accede to the Council of Europe's Convention on Cybercrime in order to strengthen international cooperation in the investigation and prosecution of cybercrime. It also needs to set up an agency to properly coordinate policies and regulations on the information society so as to ensure joint action towards enhancing transparency and access to information by the commission on space data, PeCERT, the personal data authority, the digital signatures system, digital literacy policies and tools for e-government and e-commerce.

URUGUAY

The Digital Agenda 2011-2015 of Uruguay includes among its objectives that of developing e-commerce and initiatives to promote the financial inclusion of its citizens. The main laws on e-commerce are the Act on the Admissibility, Validity and Legal Efficacy of Electronic Documents and Electronic Signatures (Act No. 18,600), of 21 September 2009, the Consumer Protection Act (Act No. 17,250), of 17 August 2000, Act No. 18,331, on Protection of Personal Data and Habeas Data Actions, of 11 August 2008, and the Financial Inclusion Act (Act No. 19,210), of 9 May 2014. These laws are discussed below.

a) Electronic transactions/electronic signatures

Act No. 16,879, of 3 November 1997, endorsed the United Nations Convention on Contracts for the International Sale of Goods, which accepts telephone, telex or other means of instantaneous communication as methods of indicating consent to contractual provisions. In addition, under Decree No. 174/005, of 6 June 2005, MERCOSUR resolution No. 17/04, on standards for computerization of international freight manifests and customs declarations, is incorporated in the country's domestic law.

The Electronic Documents and Electronic Signatures Act, establishing the admissibility, validity and legal efficacy of electronic documents and electronic signatures (Act No. 18,600), of 21 September 2009, draws a distinction between electronic signatures and advanced electronic signatures, giving them different legal effects, and recognizes the functional equiva-

lence of print documents with respect to documents sent in data messages, as well as of handwritten signatures with respect to digital signatures that have been certified by an accredited service provider. It also authorizes authorities in the different branches of government to carry out administrative procedures through electronic means and to use electronic files and digital signatures in their actions, either among themselves or with private parties.

The Act governs electronic certification services, designates the Agency for e-Government and Information Society as the national root certification authority and confers on the Electronic Certification Unit, a deconcentrated body of the Agency for e-Government and the Information Society, authority to (i) accredit certification service providers; (ii) monitor the quality and reliability of accredited certification services; (iii) receive and evaluate complaints of certificate holders; (iv) regulate; and (v) sanction service providers who do not comply with the law.

The Decree of 8 December 2011 lays down regulations for the Electronic Documents and Electronic Signatures Act (Act No. 18,600), which governs the national electronic certification infrastructure and establishes the ranking system, headed by the Agency for e-Government and the Information Society, as the national root certification authority. Thus, the Agency for e-Government and the Information Society is the highest authority in the certification chain that is responsible for issuing, distributing, revoking and administering certificates of accredited providers of certification services.

The Act on Accountability and Budget Execution for Fiscal Year 2006 (Act No. 18,172), of 7 September 2007, created the Registry of Certification Service Providers within the Communications Services Regulatory Unit. Its responsibilities include that of monitoring the quality and reliability of the services of certification service providers.

The Act on Public and Private Services, Public Security and Conditions in which Productive Activities Take Place (Act No. 17,243), of 6 July 2000, regulates the use of electronic signatures, digital signatures, certification services and electronic procedures in the administrative context. It recognizes the use of digital signatures and their legal validity as instruments to provide security in electronic transactions by making it possible to identify the participating parties. The Electronic Files Act (Act No. 18,237), of 9 January 2008, authorizes the use of electronic procedures and documents, simple computer passwords, electronic signatures, digital signatures, electronic communications and established electronic domains in all judicial branch proceedings (both administrative proceedings and actual court proceedings).

The Financial Inclusion Act (Act No. 19,210), of 9 May 2014, allows for wages, retirement pensions and professional fees to be paid through deposits in bank accounts or in electronic currency instruments. It also regulates electronic money in the Uruguayan financial system and bank accounts with financial intermediation institutes. It sets a two-year time frame for implementation of the Act and imposes restriction on the use of cash. It also creates tax incentives for the use of debit and credit cards, reducing the rate of the value added tax.

A number of rules have been issued in the area of taxes and customs, including the Tax System Act (Act No. 18,083), of 18 January 2007, which provides exemptions from the income tax on economic activities and the income tax on physical persons for profits generated by the production of software and other developments in biotechnology and bioinformatics. Decree No. 208/007, of 18 June 2007, regulates exemptions from the income tax on physical persons in the area of new technologies. Decree No. 150/007, of 26 April 2007, reiterates the declaration of national interest for the software-production sector in regard to international competition and exempts profits from software production from the income tax on economic activities through 31 December 2009.

Decree 341/003, of 26 August 2003, established the system for enabling certain taxpayers to submit their tax returns online, and Decree No. 148/002, of 30 April 2002, regulates predictions of the outcomes of international sporting events and games of chance via the Internet. Decree No. 506/001, of 4 January 2002, establishes a new regime governing international mail parcels resulting from e-commerce transactions.

There have also been a number of decrees establishing exemptions from the industrial and commercial income tax and the value added tax in the area of new technologies, particularly for software (Decrees Nos. 323/007, 207/007, 150/007 and 148/007).

In addition, Decree No. 174/05 incorporates into the domestic legislation MERCOSUR resolution No. 174/05, which sets standards for computerization of international freight manifests and customs declarations.

b) Consumer protection

In regard to consumer protection, the Consumer Protection Act (Act No. 17,250) provides general rules on certain aspects of online commerce. It makes offers

directed to either specific or unspecified consumers – by any means of communication, if containing sufficiently precise information on the products and services offered – binding on the party marking the offer and on the consumer expressly taking advantage of it, for the period of time during which the offer remains in effect. Under this law, an offer of products or services made outside the provider's place of business by mail, telephone, television, IT media or similar means gives the consumer who accepts it the right to withdraw his or her acceptance or annul the contract on his or her own initiative within five business days from execution of the contract or delivery of the product without incurring any liability.

The regulations to Act No. 17,250 are laid down in Decree No. 244/000, of 23 August 2000, which, among other things, establishes the procedure for substantiating consumer complaints. Act No. 18,507, of 26 June 2009, establishes a special procedure for consumer relations governed by Act No. 17,250, for dealing with complaints for amounts of under 100 Uruguayan pesos (approximately US$ 3.10). The procedure is substantiated before the justices of the peace.

Under Decree No. 246/005, of 8 August 2005, MERCOSUR resolution No. 21/004, on consumers' right to information in online commercial transactions, was incorporated into the domestic legislation.

c) Protection of personal data

In addition to the protection afforded by the Constitution, the Act on the Protection of Personal Data and *Habeas Data* Actions (Act No. 18,331), of 11 August 2008, was enacted. This Act applies the model set forth in Directive 95/46/EC of the European Parliament and the Council of Europe, on protection for the privacy of individuals in respect of the handling of their personal data and the free movement of such data, a level of protection that has been endorsed by the European authorities. The Act recognizes the right to protection of personal data as a right that is inherent to all persons; hence, its subjective sphere of application covers individuals but also extends to protection of legal entities as appropriate. The Act applies to personal data recorded on any medium allowing for data processing and to any subsequent use of the data in the public or private spheres.

The Act gives data subjects the right to information, to access, to correction, updating, inclusion or deletion of their personal data, as well as the right to challenge a personal evaluation based on the handling, whether automated or not, of data, and the right to limit communication of their data by bringing an action of data protection or habeas data before the judicial authority in a summary proceeding. The Act develops a number of principles that should govern the handling of data, including the following: (i) legality, (ii) accuracy, (iii) purpose, (iv) prior informed consent, (v) security of data, (vi) confidentiality and (vii) responsibility.

The agency responsible for supervising compliance with the Act is the Unit on Regulation and Control of Personal Data, a deconcentrated body of the Agency for e-Government and the Information Society, which is empowered to enforce the Act.

The Act prohibits the transfer of personal data of any kind to countries or international agencies that do not provide adequate levels of protection consistent with the standards of international or regional law on the matter. It also stipulates that all public or private databases must be registered with the Registry set up by the Unit on Regulation and Control of Personal Data. No data user may possess personal data other than those that have been declared in the Registry. The Unit on Regulation and Control of Personal Data has the power to sanction violations of the Act by issuing warnings, fines of up to 500,000 indexed units, or suspension of the database. In the area of criminal sanctions, the Act stipulates that anyone who by virtue of his or her job or some other type of relationship with the person in charge of a database has access to or intervenes at any stage in the processing of personal data is required to maintain strict professional secrecy regarding the data.

The regulations to the Act are set forth in Regulatory Decree No. 414/09, of August 2009, which describes in greater detail the security measures that must be implemented to protect personal data and the requirements for the different procedures envisaged in the Act.

d) Industrial and intellectual property

The Literary and Artistic Property Act (Act No. 9,739), of 17 December 1937, as amended by the Copyright and Related Rights Act (Act No. 17,616), of 17 January 2003, protects the rights of artists, performers, producers of phonograms and broadcasting organizations with respect to their works and related rights, including the right to sell, reproduce, distribute, publish, translate, adapt, transform, communicate or make them publicly available in any form or by any procedure.

Also of note are Act No. 18,253, of 5 March 2008, approving the WIPO Performance and Phonograms Treaty and the Agreed Statements Concerning the WIPO Performance and Phonograms Treaty, and

Act No. 18,036, of 31 October 2006, approving the WIPO Copyright Treaty and the Agreed Statements Concerning the WIPO Copyright Treaty. In the area of trademarks, Uruguay has adopted the Regulations Regarding Trademarks (Act No. 17,011), of 7 October 1998, and Act No. 912/1996, of 27 June 1996, approving the Protocol for the Harmonization of Intellectual Property Norms in Relation to Trademarks, Geographical Indications and Denominations of Origin, currently in force in the MERCOSUR countries.

e) Domain names

The Uruguayan NIC is administered by the Central Service for University Informatics, part of the University of the Republic, to which IANA has delegated this responsibility.

The Central Service for University Informatics has assigned the administration of the .com.uy domain to the National Telecommunications Administration. Domain-name disputes concerning .uy domain names are dealt with according to the Arbitration Rules of the Conciliation and Arbitration Centre, the International Arbitration Court for MERCOSUR and the Commodity Exchange of Uruguay, which include a number of the provisions of the ICANN Uniform Domain-Name Dispute-Resolution Policy.

It should be noted that the Agency for e-Government and the Information Society is working with the Central Service for University Informatics on the process of registering and renewing the government domain names .gub.uy and .mil.uy.

f) Cybercrime and security of information

While there is no specific law on computer crime, there is legislation covering a number of crimes in this category. The National Budget Act (Act No. 16,736), of 12 January 1996, makes using digital and telematic media to intentionally transmit an inaccurate text, or to alter or destroy a document stored in magnetic form (or its backup) legally equivalent to forgery of public documents, which is defined in the Criminal Code. Furthermore, the Act on Sexual Violence Against Children, Adolescents or Disabled Individuals for Profit or for Other Purposes (Act No. 17,815), of 14 September 2004, criminalizes the marketing and dissemination of pornographic material in any format that includes an image or other representation of minors or disabled or elderly persons, as well as facilitating, in whatever way, the marketing and dissemination of pornographic material containing an image or other representation of one or more minors or disabled persons.

The Act on Attempts to Interfere with the Regular Functioning of Telecommunications (Act No. 18,383), of 31 October 2008, amending article 217 of the Criminal Code, provides prison sentences for anyone interfering with the regular functioning of wired or wireless telecommunications. The courts have issued rulings on crimes related to fraud or deception conducted via the Internet, software piracy and cybersquatting, among others.

Act No. 18,362, of 15 October 2008, created the National Computer Security Incident Response Centre (CERTuy), which reports to the Agency for e-Government and the Information Society. The purpose of the Centre is to regulate the protection of critical State information assets, based on the criteria suggested by the Honorary Advisory Council on Cybersecurity. Its work and organization is governed by Decree No. 451/009, of 28 September 2009, issued by the Agency for eGovernment and the Information Society. Also worthy of note is Decree No. 452/009, of 28 September 2009, issued by the Agency for e-Government and the Information Society, governs the adoption of a computer security policy for public agencies.

g) Pending legislation and challenges

The pending legislation includes a bill on e-commerce proposed by the Agency for eGovernment and the Information Society. The issue of cybercrime is one of the main challenges faced by Uruguay. Significant changes need to be made to include the substantive and procedural provisions envisaged in the Council of Europe's Convention on Cybercrime (independently of whether or not the country accedes to it) in order to strengthen international cooperation on the investigation and prosecution of cybercrime. The Agency for eGovernment and the Information Society has submitted to the parliament a bill on cybercrime, which will be discussed.

BOLIVARIAN REPUBLIC OF VENEZUELA

Based on its National Plan on Science, Technology and Innovation 2005-2010: Building a Sustainable Future, the Bolivarian Republic of Venezuela plans to develop ICTs, especially in the area of e-government, without expressly including a strategy for promoting e-commerce. The Data Messages and Electronic Signatures Act, of 13 December 2000, the Infogovernment Act, of 17 October 2013, and the laws on the financial sector discussed below provide a legal basis for e-commerce transactions.

a) Electronic transactions/electronic signatures

In the area of electronic transactions, the Data Messages and Electronic Signatures Act includes several provisions of the UNCITRAL Model Law on Electronic Commerce and recognizes the validity and legal value of electronic signatures, data messages and all intelligible information in electronic formats, independently of the physical medium and whether it comes from individuals or legal entities in the public or private sector. It also regulates the operation of certification service providers and the legal status of electronic certificates.

The Partial Regulations to the Data Messages and Electronic Signatures Act, of 14 December 2004, go into greater detail on certain aspects of the Act, particularly in relation to the accreditation of certification service providers and the powers of the Office of the Superintendent of Electronic Certification Services. They also establish rules that must be observed in handling the data involved in generating electronic signatures, which, once created by a certification service provider, must be delivered personally and immediately to the signer. They also define security standards, plans and procedures to be followed by certification service providers.

Also of note is the Decree of 10 May 2000, declaring access to and use of the Internet to be a priority policy for the cultural, economic, social and political development of the Bolivarian Republic of Venezuela.

As regards financial transactions, the General Act on Banking and Other Financial Institutions, of 3 November 2001, governs virtual banking, dematerialized services, electronic delivery services, electronic accounting systems and virtual financial services, defined as the group of products and services offered by banks, savings and loan and other financial institutions, to carry out, through electronic, magnetic or similar media, directly and in real time, transactions that would traditionally entail making telephone calls or require users to go to the offices, branches or agencies of the institution concerned. The Act also recognizes the probative value of the aforementioned services.

The Act on Credit, Debit and Prepaid Cards and Other Financial and Electronic Payment Cards, of 22 September 2008, regulates all matters pertaining to the system and to operators of credit, debit, prepaid and other financial and electronic payment cards, the financing of such cards and relations between issuers, cardholders and businesses affiliated to the system, in order to guarantee respect for and protection of the rights of users of those instruments of payment. Issuers of those instruments are required to provide adequate and non-deceptive information to cardholders.

By its Decision No. 641.10, of 19 January 2011, the Office of the Superintendent of Banking Sector Institutions issued rules governing the use of electronic banking services carried out through automatic teller machines, mobile banking, points of sale, Internet banking and telephone banking to support different financial transactions, including domiciling services, payments and transfers to third parties, in a secure environment under the responsibility of the banking institutions concerned, so as to protect users against electronic fraud. Among other security measures, the decision calls for the implementation of multiple authentication measures to protect data in the course of electronic transactions.

In the area of e-government transactions, the Organic Act on the Public Administration requires government entities to use electronic, computer and telematic media, including web pages, for their organization, operations and relations with persons. Under this Act, documents reproduced by electronic, computer, optical or telematic media have the same validity and effect as original documents, provided that they meet the requirements established by law and that the authenticity, integrity and inalterability of the information they contain are guaranteed.

The Public Procurement Act, of 6 September 2010, governs State procurement of goods, provision of services and construction of works, in order to preserve public assets, strengthen sovereignty, develop production capacity and ensure transparency in the action of public agencies. Contractors may be selected through open calls for bids, closed calls for bids, invitations to tender and direct contracting. The Act covers technical specifications in electronic contracting and requires the use of data messages and electronic signatures.

The Act on Electronic Access and Exchange of Data, Information and Documentation among State Agencies, of 15 June 2012, lays down the bases and principles governing electronic access and exchange of data, information and documents among State agencies and entities, in order to ensure implementation of a standard of interoperability that will enable citizens to exercise their right to information and submit requests for interoperable services.

The Act also requires government agencies and entities to develop interoperable information systems and information services using open-standard free software and to use certification and electronic signa-

tures. It authorizes those entities to substantiate their administrative actions by electronic means, use electronic files and digitize their archives, which must be signed electronically by the official authorized to make certified digital copies. The Act requires government staff to set up a digital repository.

The Infogovernment Act, of 17 October 2013, establishes rules, principles and guidelines governing the use of free information technologies in State procedures at the national, state and municipal levels, in order to improve public management and facilitate citizens' access to information in their roles as controllers and users, as well as to promote national development to guarantee technological sovereignty. It promotes the elimination, simplification and automation of government procedures.

The Act regulates different subjects such as forensic informatics, critical infrastructures, interoperability, security of information and free software. It authorizes individuals to (i) send any kind of request through the use of ICTs; (ii) make payments, declare and pay taxes through the use of ICTs; (iii) receive notifications by electronic media; (iv) access public information through secure electronic means; and (v) electronically access files, among other rights. It also establishes that electronic files and documents of government entities with electronic certificates and signatures have the same legal validity and probative efficacy as printed files and documents with handwritten signatures.

The Public Registrars and Notaries Act, of 22 December 2006, encourages the use of technological media in these areas as being in the public interest, so as to streamline procedures for receiving, registering and publicizing documents without jeopardizing legal security, and gives registry entries and registry information from electronic means the full legal force of public documents. The Act provides for digitization of all physical media used in the registry and notarial system and for transfer of this information to databases. The registry and notarial process is to be conducted entirely on the basis of electronic documents, and the electronic signature of registrars and notaries is to have the same evidential validity as the law gives to handwritten signatures.

b) Consumer protection

The Organic Act on Fair Prices, of 23 January 2014, is intended to ensure the harmonious, fair, equitable, productive and sovereign development of the national economy by establishing fair prices for goods and services through an analysis of cost structures; setting maximum profit margins and effectively overseeing economic and commercial activity; allowing access by persons to goods and services to meet their needs; establishing unlawful administrative acts, related procedures and sanctions, economic crimes, their criminalization and compensation for damage suffered, for the consolidation of the socialist economic system of production.

The Act governs economic activities in Venezuela, including those carried out through electronic media, by public or private individuals and legal entities, both nationals and foreigners. However, it does not clearly establish the obligations of providers nor does it expressly define the rights of online consumers, as was the case with the Act on Protection of Persons in Accessing Goods and Services, of 1 February 2010, which was abrogated by this Act.

The Organic Act on Telecommunications, of 1 June 2000, requires operators of telecommunications services to respect users' rights, including the right to appropriate and non-deceptive information on the content and characteristics of Internet services, as well as the right to freely select service providers, and mandates equitable treatment of consumers. Failure to observe these obligations is punished with a fine and, for certain offences, can even lead to revocation of the administratively granted authority to provide telecommunications services.

The Organic Act for the Protection of Children and Adolescents, of 31 December 2001, establishes preventive measures to insure against the production and sale of computerized, electronic or multimedia games considered harmful to the health or integral development of children and adolescents. It also prohibits using multimedia or networks to allow children and adolescents to view material with pornographic content, or content that condones violence, crime or use of tobacco, alcohol or drugs.

(c) Protection of personal data

As regards the protection of privacy and personal data, the Constitution of Venezuela, of 30 December 1999, enshrines the right of all persons to have access to the information and data on themselves or their assets that appear in government or private records, except in cases specified by law, as well as their right to know how such information is used and for what purpose, and to request the appropriate court to order the updating, correction or destruction of said information (habeas data) if it is erroneous or is unduly detrimental to their rights. It also enshrines the right of all persons to protection of their honour, private life, privacy, image, confidentiality and reputation, and pro-

vides constraints on the use of information technology, in order to protect the honour and personal and family privacy of citizens and the full exercise of their rights.

The Act on the Protection of Persons in Accessing Goods and Services, of 1 February 2010, provides that in electronic negotiations, providers must guarantee the privacy and confidentiality of data used in transactions, so as to limit access exclusively to authorized persons.

The Infogovernment Act provides that information contained in government archives and records is public in nature, except in the case of information on the honour, private life, privacy, image, confidentiality and reputation of persons and on the defence of the nation. The Act also authorizes government entities to collect data relating to the rights and guarantees of children and adolescents, upon the request of the person legally authorized for that purpose. The information may not be publicized, assigned, transferred or shared with any individual or legal entity without the prior consent of the child's legal representative, except in cases specified by law.

The Act also provides that government entities, through the use of ICTs, are required to notify persons that their information will be collected in automated form, stating the purpose and use that will be made of the information and with whom it will be shared. They must state the options available to data subjects for exercising their right to access, ratify, delete or oppose the use of their information and the security measures applied to protect the information, records and archives in the databases of the entities concerned.

In the administrative realm, the Administrative Procedure Establishing the General Conditions of Administrative Powers, of 2006, issued by the National Telecommunications Commission, requires Internet service providers to ensure the confidentiality and inviolability of private communications and to adopt the measures needed to guarantee the protection and confidentiality of users' personal data. They must not use said data for purposes other than for providing the service, except upon receiving requests for information from the State's security agencies or other authorized entities. Failure to observe these provisions incurs a fine and leads to the revocation of the authorities granted.

d) Industrial and intellectual property

In the area of intellectual property rights, the Bolivarian Republic of Venezuela has become a party to Decision 486 (Common Industrial Property Regime) and Decision 351 (Common Copyright and Related Rights Regime) of the Commission of the Andean Community. It has also signed the Berne Convention and the Rome Convention, as well as the WIPO Copyright Treaty and the WIPO Performance and Phonograms Treaty.

In the legislative realm, the Industrial Property Act, of 14 October 1955, regulates the rights to industrial creations, inventions or discoveries of those who invent, discover or introduce products, and ensures the rights of producers, manufacturers or merchants to phrases or special signs that they use to distinguish their products or activities from those of others. The Act gives these rights holders the right to register trademarks, logos and business names, as well as patents, models and industrial drawings.

The Copyright Act, of 14 August 1993, protects creative works of the imagination, whether literary. scientific or artistic, in any genre or form of expression, and of any merit or for any purpose. The Act also protects databases and computer programs, along with technical documentation and user manuals.

e) Domain names

The National Telecommunications Commission administers and manages the Network Information Centre of the Bolivarian Republic of Venezuela (NIC.ve), which is responsible for assigning .ve domain names. It has adopted the Uniform Domain-Name Dispute-Resolution Policy, under which disputes can be settled through the WIPO Mediation and Arbitration Centre.

f) Cybercrime

Of note in the criminal area is the Special Act Against Computer Crime, of 30 October 2001, the purpose of which is to provide comprehensive protection of systems that use information technologies and to prevent and punish crimes against such systems or any of their components, or actions carried out with the use of said technologies. Among the crimes defined are improper access to IT systems, sabotage or damage to them, computer espionage and forgery of electronic documents. The Act also defines sanctions for various crimes against property, in particular, crimes that involve obtaining information belonging to third parties in order to steal their property or assets. The Act defines the crimes of fraud using information technologies, fraudulent use of smart cards, improper provision of goods or services and the possession of equipment for forgery.

The General Act on Banks and Other Financial Institutions, of 3 November 2001, includes in the chapter on criminal sanctions a number of computer crimes, including disclosure of confidential information contained in IT media, electronic fraud, appropriation of information on clients, and appropriation of information by electronic means.

The Special Act Against Computer Crime provides sanctions for crimes against children and adolescents consisting of furnishing them access to pornographic material or displaying pornographic images of children or adolescents. As crimes against the economic order, it punishes violations of intellectual property rights and violations of consumers' rights through misleading offers.

The Act makes crimes committed outside the Bolivarian Republic of Venezuela punishable on Venezuelan soil when they have had effects in Venezuela and when the responsible party has not been tried for the action or has evaded trial or sentencing by foreign courts.

In regard to security of information, the Infogovernment Act requires that electronic actions carried out by government entities must guarantee the integrity, confidentiality, authenticity and availability of electronic information, documents and communications. It authorizes the Office of the Superintendent of Electronic Certification Services to implement the National System of Information Technology Protection and Security, which is made up of four national subsystems, namely, cryptography, computer security incident response (VenCERT), forensic informatics and data protection.

g) Pending legislation and challenges

One of the main challenges faced by Venezuela is the need to adopt general legislation on personal data, in order to comply with its commitments as part of the Ibero-American Data Protection Network. It also needs to review and update its substantive and procedural legislation, bearing in mind the Council of Europe's Convention on Cybercrime, the Ibero-American Cooperation Agreement on Research Underwriting and Obtaining Evidence on Cybercrime and the recommendation of the Conference of Ministers of Justice of Ibero-American Countries on the Definition and Punishment of Cybercrime, of which Venezuela is a member.

Layout and Printing at United Nations, Geneva – 1529154 **(E)** – September 2016 – 313 – **UNCTAD/DTL/STICT/2015/4**